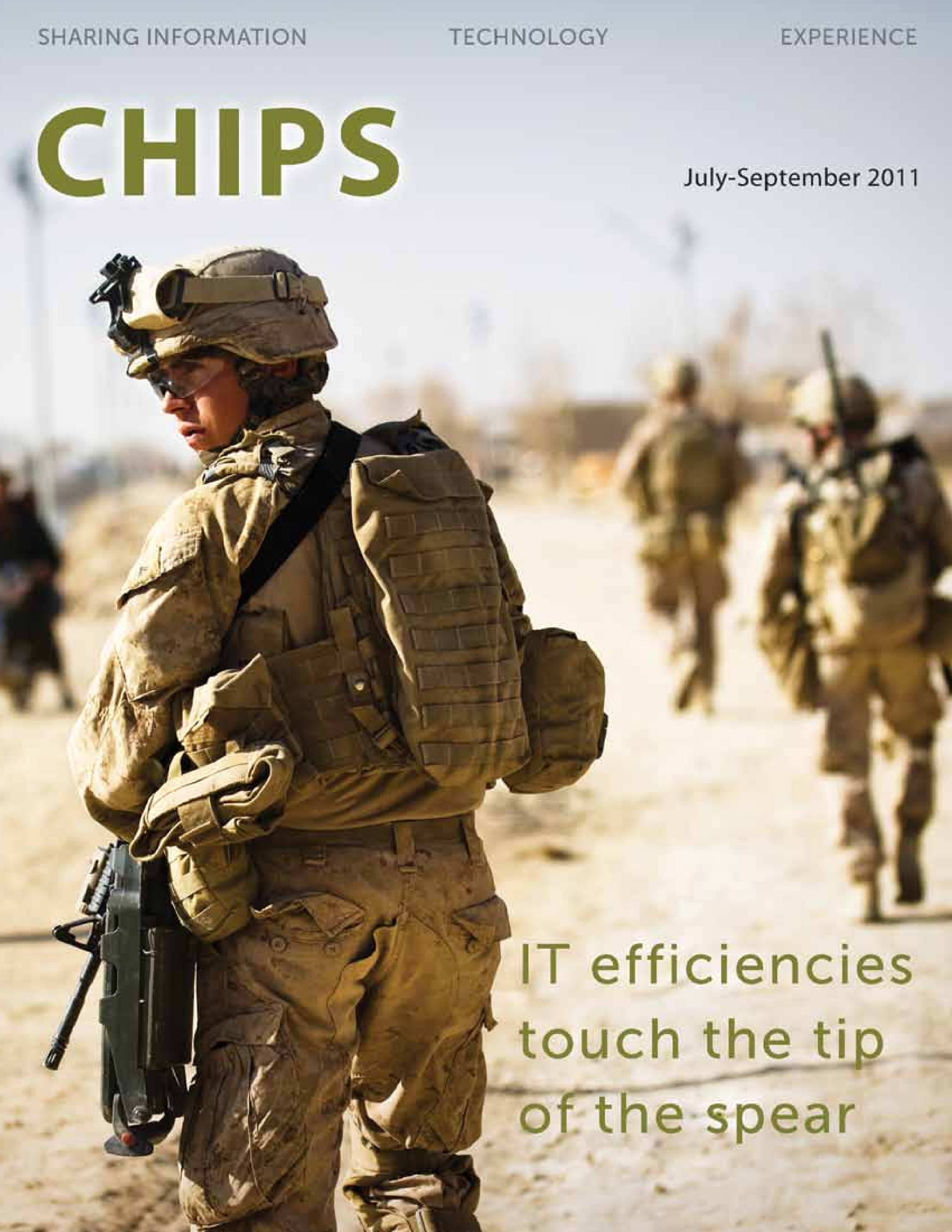
SHARING INFORMATION TECHNOLOGY EXPERIENCE

CHIPS

July-September 2011



IT efficiencies touch the tip of the spear

CHIPS July – September 2011 | Vol. XXIX Issue III

Department of the Navy Chief Information Officer
Mr. Terry A. Halvorsen

Department of the Navy
Deputy Chief Information Officer (Navy)
Vice Adm. Kendall L. Card

Department of the Navy
Deputy Chief Information Officer (Marine Corps)
Brig. Gen. Kevin J. Nally

Space & Naval Warfare Systems Command
Commander Rear Adm. Patrick H. Brady

Space & Naval Warfare Systems Center Atlantic
Commanding Officer Cmdr. Mark Glover

Space & Naval Warfare Systems Center Pacific
Commanding Officer Capt. Joseph J. Beel

Senior Editor and Layout and Design
Sharon Anderson

Webmaster
Department of the Navy Chief Information Officer

Columnists
Sharon Anderson, Terry Halvorsen,
Tom Kidd, Mark Rossow

Contributors
Lynda Pierce, DON CIO Enterprise IT Communications
Holly Quick, SPAWARSYSCEN Atlantic

CHIPS is sponsored by the Department of the Navy Chief Information Officer (DON CIO), the DoD Enterprise Software Initiative and the DON's ESI software product manager team at SPAWARSYSCEN Pacific. CHIPS is published quarterly by SPAWARSYSCEN Atlantic. USPS 757-910 Periodical postage paid at Norfolk, VA and at an additional mailing office. POSTMASTER: Send changes to CHIPS, SSC Atlantic, 1837 Morris St. Suite 3311, Norfolk, VA 23511-3432.

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, 1837 Morris St. Suite 3311, Norfolk, VA 23511-3432, or call (757) 443-1775; DSN 646. Email: chips@navy.mil; Web: www.chips.navy.mil.

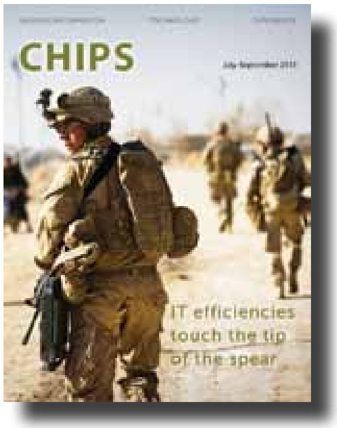
Disclaimer: The views and opinions contained in CHIPS are not necessarily the official views of the Department of Defense or the Department of the Navy. These views do not constitute endorsement or approval by the DON CIO, Enterprise Software Initiative or SPAWAR Systems Centers Atlantic and Pacific. 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.

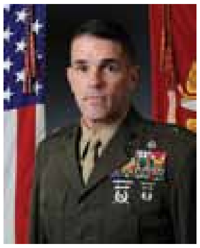
Online ISSN 2154-1779: www.chips.navy.mil.

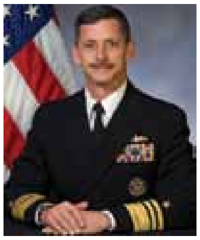
Cover

The Marine Corps is a lethal, agile middleweight fighting force enabled by efficient and effective information technology and mobile renewable energy solutions to power the battlefield, vehicles and for shelter.



Interviews





Navigation

From the DON CIO

From Around the Fleet and Program Offices

More Interviews

Highlights

In Every Issue

ALEXANDRIA, Va. (June 16, 2011) Chief of Naval Operations Adm. Gary Roughead, left, and Rear Adm. Nevin Carr, Chief of Naval Research, observe a commercially available drone while touring the exhibit portion of the Office of Naval Research-hosted Naval Science, Technology, Engineering and Mathematics (STEM) Forum. The drone is just one example used by the Space and Naval Warfare Systems Command (SPAWAR) to teach students how technology is used in the real world. U.S. Navy photo by John F. Williams.

Editor's Notebook

Be Enterprise, Be Effective and Be Efficient

Members of the DoD Enterprise Software Initiative team: Jim Cecil, and ESI working group co-chairs, Jim Clausen, from the office of the DoD CIO, and Floyd Groce, director of enterprise IT strategy in the office of the DON CIO, in May at the DON IT Conference at the Virginia Beach Convention Center.

In response to spiraling costs and the economic downturn, the Defense Department and each of the services are examining ways to save money while not sacrificing mission effectiveness. The departments found many efficiencies in reducing overhead costs and are now focused on finding efficiencies in the way they deliver IT and cyber services.

In this issue, we feature interviews with top IT/cyber leaders in the Navy and Marine Corps, beginning with Marine Corps Brig. Gen. Kevin J. Nally, Director for C4, DON Deputy CIO (Marine Corps) and Deputy Commanding General of Marine Forces Cyber Command, and Vice Adm. Bernard J. "Barry" McCullough III, Commander, Fleet Cyber Command/10th Fleet. Each leader discusses more efficient ways of doing business, from a realignment of forces, to server consolidation, to reducing energy consumption on the battlefield. And, Vice Adm. Kendall L. Card, Deputy Chief of Naval Operations for Information Dominance/ Director of Naval Intelligence (N2/N6), makes his debut in CHIPS in his role as the DON Deputy Chief Information Officer (Navy).

Lt. Col. Rick "Silky" Schilke, a requirements analyst, in the Marine Corps Expeditionary Energy Office, carries the efficiencies momentum further in a discussion about mobile renewable energy and the successes of the Experimental Forward Operating Base.

Also weighing in on the energy discussion are OPNAV Director, Energy and Environmental Readiness Division and Director of Task Force Energy Rear Adm. Philip Hart Cullom and Commander, Navy Installations Command, Vice Adm. Michael C. Vitale.

In an interview, Rear Adm. Sinclair Harris, director of the Navy Irregular Warfare Office, talks about his experiences as commander of Expeditionary Strike Group 5 and the ongoing work to implement the Navy's vision for irregular warfare. In another interview, the commanding officer of the Naval Research Laboratory, Capt. Paul Stewart, speaks passionately about NRL's remarkable 85-year history and inspiring scientific work.

In May, we had the pleasure of exhibiting CHIPS with two of our sponsors, the Department of the Navy Chief Information Officer and the DoD Enterprise Software Initiative, at the DON IT Conference in Virginia Beach, Va. The ESI is a catalyst for savings through its enterprise contracts. You will want to read the article by ESI working group co-chair, Floyd Groce, and Marine Corps Systems Command director for Product Group 10, Karen M. Davis, who write about the "DON's Approach to Buying and Managing IT Resources."

CHIPS assistant editor Nancy Reasor manning the ESI exhibit at the DON IT Conference in May. Go to page 62 for ESI contracts news.

DON CIO Terry Halvorsen asked that the DON Information Management/Information Technology/Cyberspace Campaign Plan for Fiscal Years 2011-2013 be published in this issue to draw your attention to the imperative to "Be Enterprise, Be Effective and Be Efficient." To achieve the proposed IT efficiencies across the DON is not just a matter of cost savings; it is a national security priority, and one that we must work together to accomplish.

In July, a new and improved CHIPS website launches with many exciting features, including searchable content, better maneuverability and greater functionality. Through the coming months, we will be adding CHIPS back issues for your convenience. The website is moving to a DON enterprise solution, but you can still find CHIPS at *www.chips.navy.mil.*

Lastly, I wish to extend "Fair winds and following seas" to the CHIPS assistant editor, Nancy Reasor, who retired July 2 with 31 years of Navy civilian service. Nancy's hard work and cheerful demeanor will be sorely missed by everyone who had the pleasure to work with her.

Welcome new subscribers!

Sharon Anderson

A MESSAGE FROM THE DON CIO

Changing the IT Business Model

The Department of the Navy must change the way it manages its business information technology (IT) systems. It is the reality of these fiscally constrained times; and frankly, it is the right thing to do as good stewards of taxpayer money.

As we examine and evaluate our business IT, we are going to follow the money — because where we spend the most money — is where we will find the biggest opportunities to save. Everything, short of our combat systems, is on the table.

Under Secretary of the Navy Robert Work directed the department to cut its IT budget by 25 percent over the next five years. We will not hit that target by doing the same things we do today more efficiently. A cut of this magnitude requires a fundamental shift in our IT business model. It will require taking risks and doing things that would have been considered too risky or too controversial in the past.

While this process will be a difficult one, it will ultimately move the department toward greater effectiveness and efficiency. We will not pursue anything that will negatively impact the department's ability to achieve its primary mission of protecting this nation in the name of being more efficient. But as we become more effective, the efficiencies will follow.

Today we are running more than 2,000 applications on the NMCI network, which includes multiple versions of the same software, and software that is used by a small number of people. We have 140 to 150 data centers in operation that are not optimally located. The result is an extremely complex and duplicative network structure, which generates greater purchase and manpower support costs, in addition to test, certification, operation and maintenance expenses. Some of the areas we are examining include the following.

Application Redundancy. The department has a number of applications that basically perform the same function, and some that are used by a small number of people. We must look at these applications and question whether a unique requirement is worth the cost of multiple applications performing the same function, or whether an application is worth keeping if it's not widely used. We are doing the math and considering what value we are actually getting for our investments. We will decide which applications are worth keeping and which will be eliminated.

Data Storage and Management. The trend in industry is to consolidate data centers to reduce costs; the department must do this as well. We are already making progress; we have closed seven data centers so far this year. We are considering current and future needs, as well as operational costs, when determining which data centers to close. We cannot afford to provide immediate access to all data so we must standardize and prioritize data. If we have fewer data centers with better connectivity, we can send high priority data faster. This is difficult to do now with data stored in different standards and in many data centers.

Enterprise licensing. We must require purchasing via enterprise licenses with no waivers granted. Allowing waivers led us to where we are today with multiple versions of software, including customized software. We cannot continue to customize off-the-shelf software at the rate we currently do because once we customize we are required to pay for testing and updating. We must centralize decision making to determine if and when customization will be allowed. In the future, this may mean changing a process rather than customizing software to fit that process.

Governance. We must improve governance across all IT functions, which will enable the department to act more like an enterprise. I am working with Marine Corps and Navy leadership to address this. Not everyone will like the result, which will be more centralized governance. However, this does not mean all execution will be at the department level; it means centralized governance through the two services.

Addressing these issues will reduce the complexity of the network and associated costs, which will allow the department to accomplish its mission more effectively and more efficiently. As we consider the options before us, we are asking industry for suggestions on how to achieve meaningful savings. Some changes under consideration include moving to commercially provided email, operating data centers in a public/private venture similar to how the military manages housing, and delivering common applications via cloud computing.

It is a balancing act. In moving to new business models, we must balance risk, total cost and the mission with an enterprise perspective. We also must get better at analyzing IT costs and taking risks in our business IT operations that will not impact the mission. Security is a key consideration in this process, but we need to understand the actual value we are getting for our security dollars. While it is necessary to meet requirements, we must understand the value of going beyond those requirements. What level of security and at what cost?

We must begin realizing savings in fiscal year 2013. Reducing the IT budget by 25 percent won't be easy. But it must be done, and it must be done smartly. We must act more like an enterprise to become more effective and efficient, which ultimately enables us to better support the Sailors and Marines working around the world to achieve our mission. CHIPS

Terry Halvorsen

Interview with Marine Corps Brig. Gen. Kevin J. Nally

Director for Command, Control, Communications and Computers (C4)
Deputy Commanding General for Marine Forces Cyber Command
Department of the Navy Deputy Chief Information Officer (Marine Corps)

Brig. Gen. Kevin J. Nally

Brig. Gen. Kevin J. Nally, as the Director for C4, Deputy Commanding General for MARFORCYBER and the DDCIO for the United States Marine Corps, leads many of the IT and cyber efficiency efforts for the Marine Corps. CHIPS asked the general to discuss these efforts in June.

CHIPS: The DON CIO Terry Halvorson said at the DON IT Conference in January that he is going to look at information technology policy to make sure it is viable and enforceable, and that he will be looking at the second, third and fourth order effects of policy decisions. Are there any specific policies that the Marine Corps is looking at in this regard since Marine forces are expeditionary by nature?

Nally: We work closely with the Department of the Navy and Terry Halvorsen's office. However, first and foremost, what I always concentrate on is our workforce (Marines, GS (civil service personnel) and contractors) and then our network, the MCEN, the Marine Corps Enterprise Network; we have to meet the intent of my Commandant's planning guidance.

This is my first tour of duty in D.C., in 31 years. I work backwards from the forward operating bases in Afghanistan back to the Pentagon to see if whatever we are going to put into the network, can be put into the network seamlessly. This helps create a knowledge-based force that makes good, knowledgeable decisions in a timely manner that meet the commander's requirements.

I always concentrate on [the question], 'Is it going to take away the effectiveness of our fighting forces?' Just because it is an efficiency, doesn't necessarily mean it is the right thing to do if it is going to degrade our combat effectiveness.

I brag about this, but we are the only service that can actually touch our individual computers out in Afghanistan from our Marine Corps Network Operations and Security Center in Quantico, Va. We do that for security reasons. We are pretty proud of that and that's another concern that I keep in the back of my mind. I do not want to lose that ability.

CHIPS: The Marine Corps was named the lead for assessing and buying enterprise hardware and software solutions for making the right investment choices for the DON. The lead integrator is Marine Corps Systems Command, but will you have a role to play in the assessment?

Nally: We offered that up to them [Office of the Chief of Naval Operations]. The one for the hardware is called MCHS, Marine Corps Common Hardware Suite, and the one for software is called the Marine Corps Software Enterprise License Management System (MCSELMS).

We told the N2/N6 (Deputy Chief of Naval Operations for Information Dominance), the Department of the Navy Deputy CIO, 'We are willing to help you create these kinds of programs for the Department of the Navy and the OPNAV.' Terry's office said, 'Great.' So between MARCORSYSCOM, my office, Terry's office and the N2/N6 office, we can help create a Department of the Navy program for each one of those efforts.

The programs are used for non-NMCI (Navy Marine Corps Intranet) hardware and software. Since we are still under HP's network for NMCI, for anything NMCI related we go through HP for hardware and software pieces.

Currently under the Common Hardware Suite program, those computers that are not NMCI related, not tied to that network, that is how we buy those computers. If my computer on my desk breaks, HPES (Hewlett-Packard Enterprise Services) replaces that. We end up paying for it, of course, but HP handles that. If it is a computer that we have to put in Afghanistan, the Marine Corps solely takes care of that transaction. It is not easy to understand, but I deal with it all of the time.

With MARCORSYSCOM and the Department of the Navy, my role as the CIO for the Marine Corps is defining and developing appropriate terms and conditions for the hardware and software because it will be connected to the Marine Corps Enterprise Network. In my role as the DAA (Designated Accrediting/Approval Authority) for the Marine Corps, I want to make sure that I can assure my boss, the Commandant, that our hardware and software share common certification and accreditation. And in my role as the Deputy Commander for the Marine Forces Cyber Command, that also plays into the role in terms of cybersecurity and making sure that what we are hooking up to the network, we are going to be able to provide, operate and defend the network.

CHIPS: Will these new licensing agreements make it easier for the Navy and Marine Corps to interoperate? For example, I attended the Bold Alligator exercise in December 2010 and the IT operators told me that the communications equipment between the Navy and Marine Corps did not always interoperate well.

Nally: The ships don't always upgrade their IT equipment on a regular basis like we do. For example, on the ship [maintenance] cycles they don't necessarily upgrade their IT equipment for 18 to 24 months until it [the ship] comes back into port for reset and refurbish. On the other hand, the Marine expeditionary units are deploying seven, eight, nine months at a time, coming back, and then one of the MEUs refits and goes out again.

We have the ability to upgrade our IT at a lot faster rate than they [fleet] do. When we go aboard ship, we have certain spaces dedicated to the Marines, and we bring our own IT, so we do our best to bring the latest and greatest IT aboard ship. In conjunction with OPNAV, we have stood up a C4 amphib working group, to better improve the C4 aboard the ships for the Navy and the Marine Corps. We are working closely with the N2/N6 on that as well.

CHIPS: IT efficiencies and data center/server consolidation are big news topics right now, and a mandate per the Under Secretary's "DON IT/Cyberspace Effiency Initiatives and Realignment" memo. What progress has the Marine Corps made?

Nally: We have a Marine Corps Enterprise IT Services Center in Kansas City, Mo., that will be initially operationally capable 6 July. That is the centerpiece of the Marine Corps data center service consolidation strategy, and it will provide world-class capability for hosting Marine Corps critical applications and systems, as well as data assets. We have already established some guidelines for later this year; of the 162 programs in the Marine Corps that we are going to start migrating, some of those, around 50, [will migrate] to the MCEITS (Marine Corps Enterprise IT Services) program. Near-term, MCEITS is going to serve as a COOP (continuity of operations) site, and it will serve as part of our cloud computing efforts. It is a really nice facility, and we are really excited about it.

I have talked with Terry Halvorsen, and we have offered up pieces of the building there, so the Navy can move into that facility, the data center, so they can potentially do some consolidation as well.

> "We are expeditionary in nature, and we are, as the Commandant says, a middleweight fighting force, so we are strong enough and powerful enough to affect combat operations when we get there, and we are also strong enough to sustain our operations. We need to be able to be responsive, scalable, flexible and available 24/7 from anywhere and anytime; we need that as part of our networks."

CHIPS: Naval leadership has said that the department needs to stop building one-of-a-kind systems and figure out how to reuse data because building and maintaining new systems is just unsustainable. Do you have a strategy to make data more accessible and ideas on how to take advantage of the systems that are already in place? Will MCEITS help you make data more accessible?

Nally: Yes, so we can share authoritative data at an easier rate. Our objective is to reduce the number of data dependencies between systems. We created an environment where the systems go to the authoritative source for the data they need. In addition to that, whatever we do with MCEITS out in Kansas City, Mo., we need to make sure that we can take pieces of that and deploy it for our operating forces, either aboard ship or on shore, or wherever they go, and that's what we are going to be able to do with that. It [the capability] is not going to be just in Kansas City, to reduce latency for reachback we are going to take pieces of it and be able to deploy it.

Director for Command, Control, Communications and Computers (C4), Deputy Commanding General for Marine Forces Cyber Command and the Department of the Navy Deputy Chief Information Officer for the United States Marine Corps Brig. Gen. Kevin J. Nally, and from the office of the Deputy Chief of Naval Operations for Information Dominance, director of communications, networks and CIO division (N2/N6F1) and deputy DDCIO (Navy) Janice Haith, discuss Navy and Marine Corps IT efficiency efforts at the DON IT Conference in Virginia Beach, Va., in May.

> "You can have what someone says is the best IT, and it is going to solve solutions A through Z, but if I don't have the Marines qualified to operate the IT, the IT is useless."

What we have done, I call it regionalization. Our MCNOSC (Marine Corps Network Operations and Security Command), located in Quantico, Va., can reach out and touch any computer in the entire network. We are working closely with HPES moving toward a government-owned, government-operated NIPRNET. We do own and operate our own SIPRNET, and we have been doing that for several years. We [also] own and operate our own tactical and operational networks.

We are expeditionary in nature, and we are, as the Commandant says, a middleweight fighting force, so we are strong enough and powerful enough to affect combat operations when we get there, and we are also strong enough to sustain our operations. We need to be able to be responsive, scalable, flexible and available 24/7 from anywhere and anytime; we need that as part of our networks. We fight with our networks, and we need that flexibility, scalability and responsiveness with our networks as well.

CHIPS: You said at the DON IT Conference that the "best IT is a well-trained Marine." What do you mean by that?

Nally: That's a quote by my predecessor, the gentleman I took over from, Maj. Gen. (George J.) Allen. It stands true, and it's timeless with respect to IT. Foundationally, the training and education is a critical link in making our Marines intellectually smart enough to operate the equipment. You can have what someone says is the best IT, and it is going to solve solutions A through Z, but if I don't have the Marines qualified to operate the IT, the IT is useless.

Our Marine Corps Communication-Electronics School, headquartered in Twentynine Palms, Calif., teaches all of the entry-level through career-level enlisted courses in communications, cyber and maintenance of the equipment for all of our enlisted, and then our officers are taught in Quantico, Va. There are some other satellite schools spread throughout the United States.

We have partnered with industry, numerous companies, and they have become satellite academies, where entry level Marines get commercial certifications, for example, A+, Net+, Security+, and CISSP (Certified Information Systems Security Professional). We train them in CCNA (Cisco Certified Network Associate) levels one through four. We train them in Microsoft certifications, Cisco certifications and storage application certifications. We partner with industry and academia so we get the really, really good well-trained Marine that can go out there and operate the equipment.

We are never complacent either, so if things change, we get the changes through industry, and we get the changes from our operating forces. They give us feedback and after action reports about how we can potentially make some better changes to the way we operate the equipment. We feed that back to the schoolhouse where it teaches the Marines to be able to operate it.

CHIPS: At Sea Air Space in April, Assistant Commandant Gen. Joseph Dunford told the audience that the Marine Corps has three challenges in purchasing new equipment: reducing weight and cost and increasing energy efficiency. How does that affect IT planning and purchases and existing equipment?

Nally: In terms of strategic planning, the Marine Corps stood up the Expeditionary Energy Office that works directly for the Commandant, and they've made really significant inroads. I will speak just for the IT piece of it to reduce weight, cost and increase energy efficiency. Since 9/11, Marine Corps IT requirements have increased by 700 percent. The weight of the IT because of the increase has increased 400 percent, and the battery requirements for that have increased 1,294 percent because Marines are operating in distributed ops, which means that there are smaller units of Marines operating in different locations spread out [around the world].

Because we are fighting a counterinsurgency operation, and we are looking for terrorists and bad guys, the requirement is that you have to be further distributed instead of in one consolidated mass. It has obviously increased IT requirements.

CHIPS: At the conference, you mentioned increasing or maximizing bandwidth for expeditionary forces, can you discuss what has been done?

Nally: The Marine Corps has recognized the need to provide higher bandwidth to our expeditionary forces but also to use this bandwidth more efficiently. In order to accomplish this we have acquired portable commercial satellite bandwidth, augmenting military satellite bandwidth, providing bandwidth when and where needed.

Upgrading Marine Corps SATCOM terminals to take advantage of the most efficient modes of operation has allowed us to exploit this bandwidth more efficiently. Utilizing time division multiple access (TDMA) technologies have enabled the implementation of mesh communication architectures [minimizes the total amount of power consumed in communications] allowing operators to share the finite bandwidth resources. We strive to ensure Marine Corps communications are secure, reliable and agile to meet the needs of our operating forces.

CHIPS: Do you have anything else to add?

Nally: We are actively engaged in DoD and DON IT efficiency initiatives. As we are working with DoD and [the] DON, we will continue to execute our efforts that align with their goals and objectives — many of which were initiated well before IT efficiencies began — adjusting as we go based on higher headquarters direction, and as DoD and DON enterprise solutions become available and are found to be acceptable both operationally and from a cost perspective.

For more information about HQMC C4, go to https://hqdod.hqmc.usmc.mil/default.asp.

Marine Corps Information Technology Efficiencies

Brig. Gen. Nally issued a message April 13, 2011, titled, "Marine Corps Information Technology Efficiencies, which identifies savings and cost opportunities related to Information Management (IM), IT/Cyberspace, and Information Resources Management (IRM).

In the message, the general discusses the power of consolidation in select areas and has actively pursued Marine Corps wide enterprise solutions. The Marine Corps will participate in the DON CIO focus area IPTs and DoD efficiency activities to continue refining efforts and develop new courses of action aligned with the Secretary of the Navy s goals and objectives.

The Marine Corps Enterprise Information Technology Services (MCEITS) program and IT service regionalization programs are Marine Corps enterprise solutions that will consolidate enterprise IT efforts and contribute to the DON efficiency effort. These two initiatives will meet the primary objectives of the federal data center consolidation initiative, DoD data center consolidation intent, and the DON CIO data center consolidation focus area IPT.

The Marine Corps Common Hardware Suite (MCHS) and Marine Corps Software Enterprise License Management System (MCSELMS) initiatives institutionalize commodity buying and management of software licenses at the enterprise level to achieve economies of scale pricing and cost saving/avoidance. Both initiatives meet the primary objectives of the DON CIO focus area IPT for Enterprise Software Licensing (ESL)/hardware and software commodity purchases/IT services and align with DoD efforts.

The Marine Corps rationalized its application portfolio several years ago, reducing down to the current levels of applications and systems registered in the DoD IT Portfolio Repository (DITPR) and the DON Application and Database Management System (DADMS).

Other efforts are discussed in the message, to access go to: www.marines.mil/news/messages/Pages/MARADMIN234 11.aspx.

A Message from the DDCIO (Navy)

Vice Adm Kendall L. Card

As the Deputy Chief of Naval Operations (DCNO) for Information Dominance (N2/N6), I also wear another hat — that of the Deputy Department of the Navy Chief Information Officer (DDCIO) - Navy. In this role, I work very closely with the Department of the Navy CIO, Mr. Terry Halvorsen, on those issues that directly affect the U.S. Navy. Alongside my U.S. Marine Corps counterpart, Brig. Gen. Kevin Nally, DDCIO - Marine Corps, I also work with DON CIO on those issues that affect the department as a whole.

Recently, to my surprise, I found out this title as DDCIO-N is why my name is now on the masthead of CHIPS.

Providing great assistance to me in all these efforts is Ms. Janice Haith, who serves as both the director of our Communications, Networks and CIO Division (N2/N6F1) and as my deputy for DDCIO-N issues. I could not juggle all these separate responsibilities without the assistance of Ms. Haith and her remarkable team of professionals.

Having just assumed the DCNO/DDCIO-N mantle on 1 June, this is my first opportunity to address the readership of CHIPS on what we have been doing in the Navy, as well as where we will be focusing our efforts in the months ahead.

I can basically sum our path ahead in three words: Efficiencies, Collaboration and Convergence.

First, we must be smarter in the way we do business. We can no longer approach our jobs by doing things the same way, simply because that is how we have always done it. The rapidly changing technology environment and the need to husband our decreasing resources will not allow this inefficient approach. We started in this campaign for effective IT back in January when we announced a Navy information management/information technology (IM/IT) efficiencies effort focused on enterprise software licensing, data center consolidation and thin client initiatives (NAVADMIN 008/11). I feel we have already made some gains in efficiencies in that we focused in on a few key performance parameters and set a few objectives. For example, with the data center consolidation, the NAVADMIN stated our goal is to reduce data centers by 25 percent, increase server utilization by 40 percent (or more), and increase server virtualization by 50 percent.

The NAVADMIN output will serve to feed the recently established DON integrated product teams (IPTs) to address individual focus areas in the DON CIO-led IT/IM/Cyberspace Efficiency Initiatives and Realignment effort. Members of the N2/N6 staff are actively involved with these IPTs and are serving as the Navy leads for several of the IPTs. N2/N6 is also engaged with the Office of Management and Budget and Department of Defense Federal Data Center Consolidation Initiative, which intends to reduce the number of data centers across the federal government.

Moving beyond the goals addressed in that message, we are also leading an effort for the Chief of Naval Operations focused on developing and implementing a "Navy IT Way Ahead." This Way Ahead will improve Navy's IT capabilities, increase efficiencies, streamline processes and gain greater control over Navy's information/networked capabilities. Fleet Cyber Command and Space and Naval Warfare Systems Command leaders and staff will also be directly involved in our IT Way Ahead implementation. Our IT Way Ahead is still in the early stages, but more details will be provided soon.

We must also address collaboration and convergence across all our IT systems. This means we must leverage the talents of those in the intelligence community and work closely with our other service and joint counterparts to maximize the capabilities of all our forces. For example, one challenge is to decide where we put the people and processors such that we take raw data, transport it (or not), process it, and then transport it to the (Navy/joint) decision maker and trigger puller…all inside the adversary's decision cycle.

This is but one of the many efficiencies I will be discussing in the months ahead. As this note is designed to be just a brief initial communications from me, I will stop here. However, I look forward to regularly engaging with you through this great magazine!

Thank you for the hard work you do every day and Keep Smiling! CHIPS

V/R, VADM Kendall Card

NAVADMIN 008/11 is available at www.public.navy.mil/bupers-npc/reference/messages/Documents/NAVADMINS/NAV2011/NAV11008.txt.

Interview with Vice Adm. Bernard J. "Barry" McCullough III Commander, U.S. Fleet Cyber Command/ Commander, U.S. 10th Fleet

Vice Adm. Bernard J. McCullough III

Since U.S. Fleet Cyber Command/U.S. 10th Fleet was established Jan. 29, 2010, Vice Adm. Barry McCullough led the Navy's newest fleet through a reorganization of Navy cyber assets to optimize combat capabilities in the information/cyber domain with the ultimate goal of achieving the integration and innovation necessary for warfighting superiority across the full spectrum of military operations at sea, under the sea, in the air, in the littorals, and in the cyberspace and information domains.

April 18, 2011, U.S. Fleet Cyber Command and U.S. Fleet Forces Command announced an administrative realignment of the Navy's cyber organizational structure designed to enhance the Navy's ability to remain a leader in cyberspace operations and provide the necessary command and control structure to achieve decision superiority in the information domain. This change realigned administrative control (ADCON) of Navy cyber, network operations, information operations, cryptologic, and space forces to Fleet Cyber Command to allow for unity of command and optimal resource management.

CHIPS asked Vice Adm. McCullough to discuss the realignment and Fleet Cyber Command's progress in achieving the Chief of Naval Operations vision for information dominance — a little more than a year since we last talked at the stand up of U.S. Fleet Cyber Command and U.S. 10th Fleet.

CHIPS: When we spoke last year, you discussed some of your near-term goals for Fleet Cyber Command, particularly with regard to the Navy's ability to command and control forces globally. Can you provide an update on the progress you've made?

McCullough: Over the past year we have made significant progress toward revolutionizing cyber warfare to deliver operational, maritime-focused cyberspace capabilities to the fleet with the command and control necessary for warfighting superiority across the full spectrum of naval operations. A major part of operationalizing cyber command and control was establishing a subordinate standing task force organizational structure.

Naval Network Warfare Command was designated Task Force 1010 and is responsible for network operations; as subordinate task groups to NETWARCOM, Naval Computer and Telecommunications Area Master Station Atlantic and Pacific provide network direction, maintenance and shore-based relay to the fleet; network defense is conducted by Navy Cyber Defense Operations Command as Task Force 1020; NIOC (Navy Information Operations Command) Norfolk coordinates network assessment and information operations as Task Force 1030; NIOC Colorado is Task Force 1080 responsible for supporting worldwide defense operations and multi-agency collection, analysis, reporting and dissemination of intelligence information; and Navy Cyber Warfare Development Group is Task Force 1090, which is our research and development organization.

Then we aligned our global NIOCs as standing task forces associated with the numbered fleets and Navy component commanders they support. NIOC Texas is Task Force 1040 and is aligned with 4th Fleet and U.S. Naval Forces Southern Command; NIOC Georgia is Task Force 1050, which is aligned with U. S. Naval Forces Central Command/5th Fleet; Task Force 1060 in Maryland is aligned with 6th Fleet and U.S. Naval Forces Europe; and Task Force 1070, which is located in Hawaii, is aligned with 7th Fleet and U.S. Pacific Fleet.

The commanders of those task forces provide us weekly updates, so I have real-time input from my subordinate commanders to enable command and control of the organization globally but with regional focus. This allows for a diverse dissemination of intelligence, technology and responsibilities and provides us with the ability to respond quickly to tasking in support of Navy and joint commanders' operations.

To further mature our operational relationships, Task Forces 1010 through 1070 were designated as assigned forces to a combatant commander, U.S. Strategic Command. The combatant commander then delegated operational control of those forces to my operational boss, U.S. Cyber Command, who in turn delegated operational control back to us. So now we have a structured operational command and control authority that goes back to a combatant commander, and I think that is important as we look at how operational authority for military forces is delegated from the president to the secretary (Secretary of Defense) with the advice of the chairman (of the Joint Chiefs of Staff) to the combatant commanders.

Additionally, we now have administrative control over our subordinate forces, which enables us to maintain the operational readiness, define the training requirements, and have execution of the funding that supports those forces.

"Over the past year we have made significant progress toward revolutionizing cyber warfare to deliver operational, maritime-focused cyberspace capabilities to the fleet with the command and control necessary for warfighting superiority across the full spectrum of naval operations."

CHIPS: Are you referring to the realignment that was announced April 18 regarding your subordinate commands?

McCullough: Yes, the recent realignment announced in the press release [U.S. Fleet Cyber Command, U.S. Fleet Forces Command Announce Navy Cyber Administrative Realignment] was the administrative control realignment. It was important that we have the administrative authority, as well as the operational authority, because if you are charged with the operational responsibility to conduct a mission, it's my belief that you ought to be charged with the operational readiness so the units can conduct that mission. That's why I believe that the ADCON realignment was so important. Additionally, if you are going to be responsible for the operational readiness of the units to conduct the mission, you need to be accountable for the funding that enables that operational readiness, and that came as part of the administrative realignment.

CHIPS: How does the realignment help Fleet Cyber Command's mission effectiveness?

McCullough: The operational authority comes from U.S. Cyber Command to us, and if I have a convoluted administrative chain of command, I could be responsible for conducting the operational missions and be held accountable by U.S. Cyber Command, and if I didn't have the administrative responsibility for operational readiness, the potential existed that the forces would not be operationally ready to conduct the mission as I understood it from my operational commander. This new structure streamlined the ability to conduct this new mission set that we have been given by providing unambiguous lines of authority, accountability and resource prioritization necessary to deal with challenges in the cyber domain.

CHIPS: What are U.S. Cyber Command's expectations from 10th Fleet?

McCullough: As one of his service components, we are responsible for conducting operations that he (U.S. Cyber Command Commander Army Gen. Keith Alexander) delegates to us. We do that through various combatant commander exercises and the development of the ability to operate in our three lines of operation, which are net operations, net defense and full spectrum cyber operations, in support of combatant commanders.

That's our responsibility to U.S. Cyber Command, and as part of that defense of the net operations piece, we are responsible to CNO (Chief of Naval Operations) to maintain those networks in support of regional naval component commanders so they can command and control their kinetic forces.

CHIPS: How are you working with U.S. Cyber Command? Do you collaborate with the other services' cyber commands?

McCullough: Our folks routinely discuss operations and planning efforts with Maj. Gen. (Suzanne) Vuatrinot's folks at the 24st Air Force, Lt. Gen. (Rhett) Hernandez's folks at Army Cyber Forces, and Lt. Gen. (George) Flynn at Marine Corps Cyber Forces. When we are given tasking, the four commands get together and work through how to best execute the plan that U.S. Cyber Command has given to any one of us. I think that the relationship between the service components is strong.

CHIPS: What else has Fleet Cyber Command and 10th Fleet achieved?

McCullough: One of the things that I am really happy with is how we integrated with the other numbered fleet commanders and the other Navy component commanders. We have done this both from a cryptology standpoint, as well as a network standpoint.

We signed a memorandum of agreement for network operations with all the numbered fleet commanders. The agreement codified the supporting relationships that we each have to each other. All seven numbered fleet commanders signed this one document — and that was a huge accomplishment.

Pacific Fleet Commander, Adm. (Patrick) Walsh, Fleet Forces Commander, Adm. (John) Harvey and I also signed a memorandum of understanding on operational support at the Navy component command level. This codified a lot of unofficial agreements, but it also lays out how we need to operate the Navy in this domain. These memorandums of agreement will be incorporated into the next set of published missions, functions and tasks that the numbered fleet commanders and component commanders put out. This is a huge win for all of us.

We have also worked on something we have called the 'Navy Unified Cryptologic Operations Strategy.' It is a memorandum of agreement signed by the numbered fleet commanders on how we are going to do global cryptologic operations. Our NUCO strategy places emphasis on how our forces operating afloat and ashore can better function as an integrated team by fully leveraging all Navy cryptologic capabilities and our operational partnership with national agencies through a distributed and collaborative operational environment.

Another thing that we've put a lot of effort into over the past year is dynamic situational awareness and how we monitor operations on our global network in near real-time. We've built a fleet operations center inside of our headquarters here at Fort Meade with a watchfloor broken down into different areas of responsibility.

There's a watch that does dynamic network defense and has displays representative of what our sensors tell us is occurring on the network from an attack vector standpoint. We have a NETOPS station that looks at the overall health of the transport — the fiber cables and the radio frequency transport both line-of-sight and satellite that we have — so we understand the health of the network and what the attack vectors are. We also have the ability to monitor our collections capability. We have developed a very good planning capability where we can collaboratively plan with our subordinate task forces, and if required, the other services.

A lot of these capabilities existed in stovepipes across the services and in the combat support agencies. We have been able to pull that together so those data feeds are displayed in our operations center. We are at about 75 percent of what we need from a data display standpoint, and we are continuing to evolve that. A lot of what we put in our ops center we learned from a PACOM exercise that we executed in May 2010. We evolved that into this ops center, and we turned it on right before the first of the calendar year.

I believe we have the information, now our challenge is how you integrate it. We are able to display a lot of information in this space, so much that a human being can't integrate it in real time. We are working on our ability to develop tactical decision aids to enable integration of the information in real time to alert the operators to take action if and when necessary.

Another significant achievement has been our partnership with the Defense Information Systems Agency, DISA, and Lt. Gen. Carroll Pollett, in developing a robust network inspection and certification program for the Navy. This is how we assess all Navy commands on a periodic basis from a network security and physical security standpoint to enforce accountability and shift fundamental behaviors of how our force operates, maintains and interacts with our networks.

We are working work with DISA to qualify our folks and meet their standards, as well as the additional standards that we have imposed for the Navy. Our teams will be qualified to start conducting certifications for the Navy by the end of June. This is something I wanted to achieve sooner, but this is a big effort and involved a lot of folks. We've modeled it [certification program] after propulsion inspections and combat systems inspections that we do routinely at our commands.

Computer networks capability is part of a core warfighting capability we have, and we believe that the cyber certification and inspection program is absolutely necessary to maintaining our warfighting edge. Global standardization of network assets and configuration control are key to assuring command and control of our forces and warfighting systems. They are also required if our Navy is to evolve from static, reactive network operations and defense, to a capability that provides proactive, predictive and dynamic operations.

While the network inspection and certification program deals with how commands operate their networks, we are continuing to work on something that I think is very important, which is a Navy-wide cyber knowledge training continuum, that will help folks understand how networks operate and why certain things are prohibited on Navy networks, so they can better help us defend our command and control capability.

We intend to integrate cyber and network responsibilities and vulnerability training into our accession programs and then on a routine basis, as well as a higher level of training for those folks in leadership positions like department heads, COs and XOs. The training will be targeted to folks across the entire Navy for active and Reserve component uniformed folks, as well as our government service civilians and the contractors we have working for us. Our prototype training course was launched at Naval Training Center Great Lakes at one of the "A" Schools in June.

> "The Navy has been pretty gracious with the resources. When I have needed both human capital and physical resources, OPNAV has provided, and I am happy with that."

CNO talked to me about modeling it [network training] after damage control training, and Adm. Harvey and I have had this discussion also. How do you do damage control training on a periodic basis so that when there is damage on a ship, everybody on the ship is part of the damage control party, from the captain all the way down? How do you implement that same rigor of service-wide training in this area to minimize our vulnerabilities?

We believe that if you do the proper housekeeping, education and training that a large majority of the threats are eliminated allowing us just to focus on the high end of this. If we can get to that point, it frees up our folks' time and energy to focus on the high end instead of putting out brush fires across the entire service. I think that getting this training Navywide is extremely important.

CHIPS: What responsibilities does Fleet Cyber Command have as the Service Cryptologic Component to the National Security Agency?

McCullough: The only U.S. Cyber Command component that is the Service Cryptologic Component Commander is the Navy. The other services didn't make the alignment that way. These are the national mission set folks we have that support the National Security Agency globally. This gives us visibility into collections that help enable both full spectrum cyber operations, as well as proactive defense. I think we did it right, and I think that the synergy we have as the Service Cryptologic Component to the National Security Agency, as well as the service component to Cyber Command, gives us better integration and capabilities than the other service components have.

CHIPS: Has recruiting the right workforce been difficult?

McCullough: It's a challenge. You have a certain populace in the United States that has the aptitude and the capability to do these types of activities. The other services are competing for that population, other agencies are competing for that population, and commercial [organizations] and academia are competing for that population. Thus far we have been able to attain the goals we have to attract people into the Navy that we need to execute this mission set for us.

But as all the services' demand goes up for these people, and as the economy continues to improve, I think we are going to have a more challenging situation. The skill level of the people that work for us is equal to or better than anybody else in the Department of Defense, both our national mission set folks and our service mission set folks.

CHIPS: Have resources been sufficient to accomplish your goals?

McCullough: The Navy has been pretty gracious with the resources. When I have needed both human capital and physical resources, OPNAV has provided, and I am happy with that. When you stand up anything new, things take longer to achieve than you anticipate they will. While I am extremely satisfied with where we are, as are Gen. Alexander and the CNO, Adm. Roughead, my ambitions were a little greater than what we achieved.

CHIPS: Is there anything else you would like to add?

McCullough: It was a good year's worth of work with everything Fleet Cyber Command and 10th Fleet accomplished in the last year, but that about wore me out. I say me, it's not me, it's the folks that work for me that do all of this. It has been my honor and privilege to be the commander of this organization.

I can't express enough gratitude for the people that work for us and do the things we need them to do. CHIPS

For more information about U.S. Fleet Forces Command go to www.cffc.navy.mil/. For more information about U.S. Fleet Cyber Command go to www.fcc.navy.mil/.

DON Manages Increasing Spectrum Encroachment

By Tom Kidd and Mark Rossow

Naval installations have long been good neighbors with their surrounding communities. In fact, in many cases, Navy and Marine Corps bases, posts and training ranges limit some operations to preserve friendly relationships.

When many military installations were initially built, they were literally in the middle of nowhere. Cheap land and wide open spaces meant that Sailors and Marines could train in relative seclusion. But this isolation could not last forever in a rapidly growing nation. And as people moved closer to military installations and airfields, what were once non-issues, such as aircraft noise, became points of contention within communities. Likewise, amphibious landing exercises on once secluded beaches became disruptive to tourism because modern highways made remote locations more easily accessible.

As a result, many restrictions were enacted within the past two to three decades in consideration of the growing populations living near military installations. Operational restrictions curtail aircraft and machinery noise, protect wildlife and limit carbon emissions into the atmosphere.

The continued encroachment on Navy and Marine Corps real estate even affects the type of training and operations that can be conducted on installations. Many restrictions are permanent, but some are limited to specific times of the day, month or year.

The Department of the Navy's electromagnetic spectrum, or radio frequency, use is similarly affected by encroachment. During the past decades naval spectrum use grew proportionally to public and commercial use. For most of the 20th century, the Navy and Marine Corps had ample spectrum to support communications, radar and other spectrum-enabled capabilities. Spectrum use, though always regulated, was relatively unimpeded.

But near the end of the 20th century, the emergence of a plethora of wireless capabilities, made possible by the use of radio frequencies, began to affect the amount of spectrum available to naval forces. While public and commercial spectrum use, as well as federal government use, increased dramatically in recent decades, so too has the military's reliance on spectrum.

To help ensure harmony with public and commercial spectrum requirements, restrictions limiting naval spectrum use, such as time, location, altitude and propagation, are often placed on DON installations just as training and operational restrictions are imposed.

Some spectrum restrictions intend to prevent radio frequency interference to public and commercial spectrum use; while others are self-imposed to prevent interference between Navy, Marine Corps, Army and Air Force equipment.

As spectrum use increases, spectrum encroachment will continue to challenge the Navy and Marine Corps when conducting realistic training and day-to-day operations. The DON maintains a unique and diverse cadre of spectrum professionals who understand the department's spectrum requirements, ensure they are met and comply with international, federal, Department of Defense and DON regulations.

The department's globally dispersed spectrum team of civilian and military personnel are located at installations, training ranges, major commands and operational organizations throughout the nation and the world. This team coordinates and negotiates the department's usage of spectrum with host nation governments and non-government entities.

Access to and use of spectrum continues to be vital to the nation's naval services. The DON, in its continuing efforts to ensure spectrum is available, will also continue to ensure that its use is in concert with commercial and public spectrum use — as a good neighbor should.

To locate a spectrum manager in your area, whatever your spectrum requirement, email: navyspectrum.fct@navy.mil.

Tom Kidd is the director for strategic spectrum policy for the Department of the Navy. Mark Rossow provides strategic spectrum policy support for the DON spectrum team. Contact Mr. Kidd at DONSpectrumTeam@navy.mil.

Reshaping the DON’s Approach to Buying and Managing IT Resources

By Floyd Groce and Karen M. Davis

As all personnel within the Department of Defense and across the federal government are well aware, this is an era of increased budget scrutiny. However, with this scrutiny comes a new opportunity to assess and advance how DoD operates and to improve efficiency across a wide variety of business units and operations. As a significant budget item, the massive information technology infrastructure is no exception and offers a number of areas for improvement, while not compromising product and service quality.

Since December 2010, the Department of the Navy is reevaluating how it approaches IT initiatives and working to centralize and consolidate efforts where it makes sense. These efforts are being made while ensuring operational integrity, maintaining sufficient levels of defense-in-depth and fail-over capabilities, and supporting DoD IT Enterprise Strategy and Roadmap consolidation and efficiency initiatives. These efforts are also designed to recognize and address the costs and risks associated with proposed changes, and will be based on solid business case analyses.

DON IT Integrated Product Teams

In a memo dated Dec. 20, 2010, **“DON Information Technology/Cyberspace Efficiency Initiatives and Realignment Tasking,”** the DON Chief Information Officer Terry Halvorsen announced the establishment of a new department IT policy and governance board, the Information Enterprise Governance Board (IGB), as well as eight new integrated product teams (IPTs) designed to reshape the way the DON approaches its information management (IM), IT/cyberspace and information resources management (IRM) initiatives. The IPTs formed under this initiative are:

- Data Center Consolidation;
- Application Rationalization;
- Enterprise Software Licensing/Hardware and Software Commodity Purchases/IT Services;
- Navy and Marine Corps Portal Environment;
- Near-, Mid- and Long-Term Initiatives;
- Current and Planned IT Acquisition Programs;
- DON Telecommunications Environment; and
- IT/Cyberspace Workforce and Training.

Through the chartering of the DON IGB, the DON established a single, senior management policy and governance forum to decide on IM, IT/cyberspace and IRM matters. Moreover, the DON is now leveraging existing resources and functional processes used by the Navy and Marine Corps to enable improved collaboration and resolve these challenges more rapidly. The newly created IPTs benefitted greatly from the formation of this streamlined approval process, providing a focused, mission-oriented team that is empowered to operate across the more traditional intra-DON organizational structures.

“Be Enterprise, Be Effective, and Be Efficient”

In a follow-on memo dated May 5, 2011, **“DON IM/IT/Cyberspace Campaign Plan,”** Halvorsen expands the plan by outlining the DON IM, IT/cyberspace and IRM priorities for the next 24 months, based on the following concepts:

- An enterprise approach;
- Centralized and consolidated efforts;
- Maximized security;
- Protected personally identifiable information; and
- Effective and cost-efficient implementation.

He also laid out his vision for the DON IM/IT/Cyberspace Campaign Plan for FY2011-2013 under the theme: “Be Enterprise, Be Effective, and Be Efficient.” This memo provides a framework built on four goals:

Goal 1: Sustain an operationally effective, integrated, secure, and efficient IM/IT/cyberspace and IRM capability.

Goal 2: Ensure protection of sensitive information, including personally identifiable information, and timely access to trusted authoritative information to enable effective decision making and mission support.

Goal 3: Attract, develop and retain a highly competent IM/IT/cyberspace and IRM Total Force.

Goal 4: Ensure all IM/IT/cyberspace and IRM investments are effective, efficient, planned, aligned and acquired to support DON enterprise strategies.

IPT-3 Overview & Key Actions

The Enterprise Software Licensing/Hardware and Software Commodity Purchases/IT Services IPT (identified as IPT-3) is tasked with improving the DON's IT/cyberspace investment decisions by assessing and procuring enterprise solutions. This initiative, which supports Goal 4 of the Campaign Plan, is predicated on the idea that by consolidating and centralizing the acquisition of IT hardware, software and services, the DON will lower its investment in IT infrastructure over time. Each IPT has a designated lead to integrate the various tasks the team is assigned. The IPT-3 lead is assigned to the Marine Corps, and is under the guidance of lead integrator Karen M. Davis, Marine Corps Systems Command, director of Product Group 10 (Information Systems and Infrastructure).

IPT-3 is comprised of a distributed team of subject matter experts from across the DON's acquisition, business and financial management, and CIO communities. Specific licensing efforts undertaken within the DON will join SMEs from across the DON to create multifunction teams to support establishment and management of each enterprise software license. The IPT will align with DoD efficiency efforts and with the DoD Enterprise Software Initiative (www.esi.mil) program, which is leading the higher level software and hardware strategies for use by DoD components. The DoD ESI is tasked with establishing and managing enterprise commercial off-the-shelf IT agreements, assets and policies for the purpose of lowering total cost of ownership across the DoD, Coast Guard and intelligence communities. The ESI's mission extends across the entire commercial IT life cycle leveraging the DoD's combined buying power with commercial software publishers, hardware vendors and service providers.

IPT-3's initial efforts include focus on consolidation of multiple software contracts across the DON into enterprise-wide contract vehicles or enterprise software licenses to improve buying power. This enables lower volume pricing, secure and more favorable terms and conditions, improved IT asset visibility, and faster time to delivery of commercial software through streamlined processes. IPT-3 delivers regular status reports to the IGB on its current and emerging efforts and raises any issues that need to be addressed by the board.

IPT-3 developed a unified software investment management process for the DON based on recommendations from Navy and Marine Corps leaders in financial management and incorporates solutions and processes that proved to be beneficial for other budget and investment areas. DON budget guidance will now incorporate data requirements of this new process, which will improve visibility into current budget planning and execution, as well as future budgets.

While developing the new processes, the IPT also began work to establish enterprise software licenses. This includes collecting DON requirements, meeting with industry, and identifying products commonly used within the department. The product research includes focus on the software publishers for which there is sizable spending within the DON and tackling the licensing of products that are widely deployed — but may not represent the higher level of spending. Through the work of IPT-3, the DON's IT asset management capabilities will be greatly enhanced through more robust software assurance and maintenance, less costly and more timely access to future upgrades, maximized volume price discounts and optimized licensing terms.

Conclusion

By forming the new IPTs, as well as the Information Enterprise Governance Board, the DON is reshaping how it acquires and manages its software, hardware and IT support services. These initiatives are nothing short of transformational in their scope, and will be instrumental in maintaining an efficient and innovative organization for years to come. CHIPS

Floyd Groce is director of enterprise commercial IT strategy in the office of the Department of the Navy Chief Information Officer. Karen M. Davis is the Marine Corps Systems Command director for Product Group 10 (Information Systems and Infrastructure).

Interview with Vice Adm. Michael C. Vitale Commander, Navy Installations Command

Vice Adm. Michael C. Vitale

Vice Adm. Vitale, as Commander of Navy Installations Command (CNIC), is the commander for 11 regions and 72 naval bases worldwide. CNIC's mission is to deliver effective and efficient readiness from the shore. CNIC's job as an "enabler" is to thread a needle across Navy enterprises, with the needle and thread equating to all the services installations provide on a daily basis in support of the enterprises. These services include ports, airfields, security, morale, welfare and recreation facilities, child care and housing, to name just a few.

In response to the Secretary of the Navy's energy goals to produce at least half the shore-based energy requirements from renewable sources, such as solar, wind and ocean generated by the base; and by 2020, ensuring at least 40 percent of the Navy's total energy consumption comes from alternative sources, CNIC, partnering with Naval Facilities Engineering Command, is working to reduce energy consumption while moving to renewable energy sources for naval installations worldwide.

At the 2011 Sea Air Space Exposition Vitale explained that CNIC and NAVFAC will develop an adaptable assessment tool to standardize energy investment decisions and develop a project list on an annual basis. He said the Navy is building a Smart Grid across the naval bases that will help validate how CNIC's energy project list is progressing.

CHIPS asked Vice Adm. Vitale to discuss CNIC's shore energy initiatives in June.

CHIPS: What has CNIC learned since the launch of the Navy's Advanced Metering Infrastructure (AMI) program in 2009 as a means of monitoring electrical use and tracking reduction progress?

Vitale: We are still installing meters across Navy installations and that is a rollout plan that will take several years. Once we have the meters in place connected with the backbone to collect all the data, then we can begin analyzing the data, and can answer that question. I can tell you, without waiting two or three years to get the AMI data, we believe we will find that we are expending a lot of energy in places we didn't expect.

Today, all of our energy usage is modeled. Once we get our Smart Grid online with our meters, we may find out that a particular building, which has been historically modeled, is really leaking like a sieve. Its energy consumption is not anywhere near what we thought it was. Now we know that this is where we should be making an investment to improve the insulation in the building, the insulation in the windows, insulation in the roof, improve chillers, coolers and energy-saving devices, like [automation for] turning off the lights. Then we are going to be able to start targeting exactly what places are expending a lot more energy than we actually thought.

We believe we are going to find lots of opportunities to save more money.

CHIPS: AMI is one of the critical components of the Smart Grid. Can you explain the Smart Grid implementation plan?

Vitale: We are installing meters by region, and we are awarding contracts as we speak. Since 2009, there are six regions that have had AMI contracts. We are not metering everything. It is unaffordable, and it is not necessary. A smart meter is an expensive meter, it is basically a miniature computer that connects to the power grid, and we can use [the smart meter] to help understand what's going on.

We can use it for monitoring, and we can use it for control, we can turn things off, we can turn things on, much like people do in their homes today. Most power companies have installed devices to allow them to turn off your water heater, for example, so they can save money. You don't even realize they are turning off your water heater, and you get a savings or a discount from your bill.

Smart Grid means different things to different parties in the energy and utility businesses. For the Navy's Smart Grid, I envision more of an energy management role and less of a utility management role. For instance, initially, at the installation level, we will be able to monitor the status and energy performance of systems in a facility and eventually control lighting and temperature settings. The facility level performance can be rolled up to an installation's overall performance and all the way up to a Navywide picture. As the energy management picture is perfected and refined with Smart Grid, we will be able to provide every echelon of our energy management and leadership team with actionable information to make better energy management decisions.

CHIPS: Increasing the energy efficiency of new and existing infrastructure is the most cost-effective way to reduce energy consumption, protect critical assets and enable renewable technology development. Can you talk about some of the initiatives in these areas that CNIC is pursuing?

Vitale: Probably the most significant program we have today to improve and conserve energy is our REM program — regional energy monitors. The monitors were established through our NAVFAC partnership. They conduct systematic surveys of facilities on installations and make many recommendations using energy efficiency technologies.

CHIPS: Is there an incentive for your tenant commands to report broken windows or "leaky" buildings?

Vitale: There is a system that allows for the tenant to do that [report needs], but there is not a reason for them to call us, other than to say, 'I know that we're wasting energy.' In terms of overall consumption, the way we do business today is … I'm responsible for paying the electric bill, which is roughly $900 million a year for the Navy ($873 million in FY 2010), and our overall utility bill is about $1.2 billion. That's because we don't have the meters and a way to bill our tenants.

If I wanted to bill SPAWAR (Space and Naval Warfare Systems Command), or other tenants in a building for their consumer usage, I have to meter all of their spaces too. We are putting a meter on a building; we don't put a meter on a room. That would require a significantly higher level of instrumentation. We will get there eventually, and I will be able to give a tenant a bill, but I can't do that right now, even with our current AMI plan.

CHIPS: Do you see a difference in how personnel use energy on naval installations? Is there an incentive for installations and facilities to reduce energy consumption?

Vitale: Probably the biggest way I see change occurring is in the way we are improving consumption in our new construction program. We are now required to build to a LEED (Leadership in Energy and Environmental Design) standard, which is an energy-efficient standard, and it includes all aspects of energy efficiency. As I briefed at Sea Air Space, another tool that we are now using, the eROI (energy return on investment) tool, allows us to look at those energy maps at the base and combine that with energy technologies that are available in that geographic area, to then develop a list of projects that will allow us to further improve and meet SECNAV, legislative and executive orders that have been mandated. However, until we have a smart-like grid with AMI that puts an energy 'bug' on every computer screen to show them [users] what they are consuming, we'll only see marginal consumption reduction.

CHIPS: Do alternatives, like solar and wind turbines, prove to be as reliable as traditional energy sources?

Vitale: Yes. We have them today. We have photovoltaic cells, what everyone calls PV, on a lot of our bases. We have geothermal [electricity generated from geothermal energy] on our base in China Lake. We have wind at a variety of places, and we are doing a lot of studies right now for wind to see where we can add more. They (PV, wind turbines) are reliable, but what they don't do is satisfy the full demand. What they do is provide an offset. If your base is drawing X megawatts a day, for example, in Pearl Harbor it is about 60 megawatts a day, and you put in photovoltaic cells, you might be able to take five, six or 12 [megawatts], depending on how big the array is, off that load. If you can offset the demand completely, that would be what we call net zero installation, which is one of the SECNAV's goals in 2020.

CHIPS: I heard that you advocate telecommuting as another means to reduce an installation's energy consumption, number of buildings and real estate needs.

Vitale: I am not a big believer that telecommuting or telework is another methodology for saving energy. There is marginal savings in telework — there is much more significant savings in what we call mobile work. The difference is that telework tends to be an ad hoc approach to the current employment model. If you want to telework today, you spend one or two days a week at your house. The space you occupy at the office still exists, the telephone is still there, the computer is still there and all of the things that use energy are typically still there. I don't see a lot of savings with that methodology.

Mobile work is a completely different approach. A lot of businesses today do not provide administrative space for their workers; they literally live without [an] office. They have a laptop and a telephone that connects them directly with their work, which they can do from anywhere. That allows management to take that space and consolidate its facilities, which does save money, or turn some of that space into hoteling space, which is where you create generic cubicles that people can come in and use temporarily.

That is what business is doing universally today, and that's the approach that the Navy is looking at, but we'll need to make significant changes in the way IT support is provided today to make it work. I can see the savings in transportation costs, time and quality of life benefits.

CHIPS: Surely, personnel are excited by a mobile work arrangement.

Vitale: The answer is mixed. In surveys that have been done in headquarters like our own, the response is interesting. The first thing you have to do is look at your work, and decide if that work is mobile and doesn't require a space. In our case, the average is about 25 percent, and it depends on where you are. If you are at the headquarters, a large number of our people are in 'admin' space, they might be analysts, and a lot of their work is done on the computer, so they could be eligible for mobile work. If you are on an installation, and you are out and about all over the base doing your job, you probably don't need an office. It is different for each job, and you have to study it at each level.

At the headquarters level, perhaps 25 to 30 percent could be mobile. Of that 25 to 30 percent, about 50 percent say they would like it, and 50 percent say they would not [like mobile work]. When you query the people who say they would not, you get some very personal answers like, 'I want to get away from my mother-in-law or my wife,' or 'I don't want to work in my house every day.'

Until I read that, I really didn't appreciate it [many different viewpoints] at all.

There are some cultural implications here that we will have to work through before we arbitrarily change the conditions of employment and say, 'Congratulations, today is your big day, you are now a mobile worker.' [Then they say], 'Great! That's super! What does that mean?'

Then you say, 'You don't have a desk anymore, you don't have an office. Here is your laptop. Here is your telephone. You get to stay home almost every day from now on,' and the guy goes, 'I don't want to do that.'

Initially, businesses have gone through a very steep learning curve and systematically had to figure out who would be accepting of it — and who wouldn't be accepting of it.

You find that the type of work is critical to effective mobile work, whether it is analytical work or sales work, and that there will be people who don't like it. You have to be very scientific about this, which we will do when we decide to do it.

The Navy is driving to take advantage of every energy opportunity available to reduce its consumption, as well as driving itself to become truly more efficient while it remains effective. CHIPS

Q&A with Rear Adm. Philip Hart Cullom
Director, Energy and Environmental Readiness Division
Director, Task Force Energy

"Partnering for a Greener Future"

Rear Adm. Philip Hart Cullom

An energy secure nation is a matter of national security, Secretary of the Navy Ray Mabus often says. To this end, the Secretary outlined five energy goals. Rear Adm. Cullom is leading efforts to meet several of these goals, foremost of which is an overall change to reduce reliance on fossil fuels in a volatile petroleum market and move the Navy to renewable energy sources. Other energy advances include improved coatings for hulls and propellers and solid state lighting for ships, as well as many environmental conservation efforts.

CHIPS talked to Cullom last summer about the Navy's tactical energy plans and he provided a written update in June.

CHIPS: At the 2011 Sea Air Space Exposition in April, you said that energy efficiency should play an earlier role in the acquisition process. Are you seeing evidence of this in the purchases the Navy is making now?

Cullom: We are working hard to incorporate energy factors earlier into the acquisition process, but it's not easy. A lot of people within the Navy, from all levels of the chain of command, as well as industry, need to be involved. I like to compare optimizing the Navy's acquisition process to NASA's space program.

NASA is able to successfully launch satellites, space shuttles, and even people into space, all monumental and complex tasks, by bringing together all of the players — policy makers, engineers, scientists, and industry — early into the acquisition process to make a corporate decision about which requirements, in terms of mission capabilities, payload, support systems, safety redundancies, and needed thrust, will be prioritized for the mission. I am confident that the Navy can bring that same approach to our acquisition process.

CHIPS: I read about the MIT Sloan School energy study for the Navy and the Leadership Lab project to stimulate the renewable biofuels market by coordinating with producers, suppliers and consumers to identify possible alternatives for accelerating the availability of energy products, examine issues associated with the scalability of emerging technologies, and to analyze prospects for lowering prices for consumers. There are many skeptics regarding the cost effectiveness of biofuels and renewable energy as long-term reliable sources of power, as well as concern that there will not be a sufficient number of providers to ensure a competitive market. Since the Secretary laid out his energy agenda, do you have a better understanding of the ability of the commercial market to meet the Navy's demands? Can you forecast a date where renewable energy alternatives reach parity or cost savings compare to traditional energy sources?

Cullom: As you probably remember, Secretary Mabus laid out his energy agenda in fall of 2009, of which biofuels played a significant part of that agenda. Since then, the SECNAV and OPNAV staffs have been working together to understand all aspects of the commercial biofuels market. We have engaged numerous venture capitalists, private investors and biofuels companies to understand how they feel about the viability of scale up, production, and expected cost in the near and long-term. We've also spoken with end users, such as commercial air carriers and shippers, e.g., UPS, FedEx, about their expectations.

Those discussions were much more encouraging than I would have thought based upon literature available in 2009 when we first looked at this issue. To validate those discussions, my staff worked with MIT's Sloan School of Management to better understand whether the development and production of viable, competitive markets for biofuel is possible. According to the study, which included conservative estimates for increases in conventional petroleum-based fuel prices, the cost competitive point for biofuels, without incentives, would be around 2020. I've had discussions with companies that are likely to be among the first to help facilitate scale up regarding this study, and they agree that the cost competitive point can be achieved far earlier than 2020, particularly if targeted incentives are available to facilitate this scale up.

CHIPS: It is intriguing to think that mundane initiatives, such as improving hull and propeller coatings and hybrid engine improvements, could reduce the Navy's fuel consumption significantly. What other innovations is the Navy working on to power aircraft, weapons systems and ships?

Cullom: The math is the math: the U.S. Navy uses 29 million barrels of oil a year. So if we save only 1 percent a year, from improving hull coatings and stern flaps, we are able to save 300,000 barrels a year — an impressive amount of petroleum saved. Ultimately, 1 percent saved here and there adds up to real barrels and real money. By 2020, these initiatives will add up to 5 million barrels of oil saved per year.

Those barrels saved translate directly to enhanced combat capability on or to the battlefield — either afloat or for naval forces, Marine or Navy, as 'boots on ground.' In fact, I would argue that energy efficiency is combat capability.

Examples of innovative technologies that will be the driving force for improving combat capability include: (1) testing, and ultimately implementation of, hybrid electric drive technology for our DDG 51 class, which will essentially turn those destroyers into the afloat version of a Prius, providing estimated fuel savings of 8,500 barrels per year; (2) development of variable cycle technology, which combines high performance of a military jet engine and fuel efficiency of a next generation commercial core into a single propulsion system, improving energy efficiency by more than 20 percent; and (3) greater consideration of the role of unmanned vehicles, for which ONR (Office of Naval Research), DARPA (Defense Advanced Research Projects Agency), and others, are exploring numerous opportunities to power those vehicles in the air, on the surface of the ocean, or beneath the waves. Innovations in the C5I (command, control, communications, computers, combat systems and intelligence) arena may hold other intriguing opportunities, and we are at the beginning stages of looking at this as well.

CHIPS: There is another dimension to conserving energy and switching to renewable energy — environmental stewardship and reduction of greenhouse gases. Is there a way to measure the effects of the Navy's conservancy efforts?

Cullom: Certainly. The most direct way to measure the effects of the Navy's energy efficiency efforts is to consider every energy savings initiative that we employ and evaluate it to determine the number of barrels of oil saved. If we are not burning a barrel of oil, we are not putting greenhouse gases in the air, and so we can calculate by how much our greenhouse gas emissions have been reduced.

We know that these calculations will demonstrate significant reductions. For our ships and aircraft, the Navy intends to purchase 8 million barrels of 50/50 blend biofuel and petroleum-based fuel by 2020. We know that greenhouse gas emissions will be less from biofuels that are compliant with Section 526 of the Energy Independence and Security Act 2007, which prohibits federal agencies from procuring biofuels unless its lifecycle greenhouse gas emissions are less than those for conventional petroleum sources.

On shore, anywhere we increase efficiency, through use of electric vehicles that receive their charge from renewable energy like solar, wind, ocean and geothermal, we can expect greenhouse gas reductions. Sailors and Marines may start to notice more electric golf carts transiting their respective bases. These golf carts are not just energy efficient but functional. Many have been modified to meet installation requirements, such as including baskets for carrying supplies.

> "As we've looked at energy futures and the worlds of 2020 and 2030, we realized that if we do not incorporate our energy initiatives now, ultimately, there will be billions of dollars of additional costs to the Navy. We will end up with a great Navy that we cannot afford to operate."

CHIPS: At Sea Air Space, you mentioned the Navy is undergoing a cultural change to meet the Secretary's energy goals. Have you seen an increased effort in the fleet to move to more energy efficient technologies?

Cullom: Culture change is more about operating differently, whether ashore or afloat. More efficient technologies are a piece of this, but it's also the mindset and conduct to be more frugal with energy use. We want our Sailors and Marines to be Spartan warriors — warriors who adopt an energy frugal mindset into their mission planning and training, which will minimize their logistics Achilles' heel, best leverage the significant investments we are making in energy technology improvements, and increase their chances of mission success.

We are changing our energy culture by linking energy consumption to behavior through awareness and accountability at the individual, command and functional level. For example, afloat we are expanding our use of shipboard energy surveys.

Ashore, we are investing in facility management experts and advanced metering infrastructure. These measures provide greater visibility of energy consumption. If we can identify the biggest 'energy offenders' afloat and ashore, we can implement measures to reduce such energy consumption.

CHIPS: You also mentioned the Jevons paradox at Sea Air Space. This theory proposes that technological progress that increases efficiency tends to increase rather than decrease the rate of consumption. Pundits use this theory to argue that energy conservation is useless since more and more technology products are introduced daily and that as developing countries begin to increase use of technologies, quality of life will improve, but the demand for energy will keep growing.

Cullom: The Jevons paradox was proposed in the 19th century and is still alive in the 21st century. However, we can break this paradox. This goes back to my assertion that we must adopt a Spartan warrior ethos — a warfighting mindset to use less, which makes us more agile, more self-sufficient, and less vulnerable.

CHIPS: Do you think the Navy's energy strategy is sustainable over time given changes in leadership and priorities — and a shrinking research and development budget?

Cullom: Our energy strategy is decidedly sustainable, from two different aspects. First, it is sustainable so that we can continue to do our mission over the long haul. If we use energy right, we'll be able to fly farther and sail longer without looking for our tanker or oiler; our energy supply will be more secure; and we'll accomplish our mission without being tied solely to a dwindling finite resource.

Second, we cannot afford not to do these things from a financial perspective. As we've looked at energy futures and the worlds of 2020 and 2030, we realized that if we do not incorporate our energy initiatives now, ultimately, there will be billions of dollars of additional costs to the Navy. We will end up with a great Navy that we cannot afford to operate.

Our energy strategy provides a 'long view' that can ultimately help our Navy and our nation remain strong in perpetuity. Because all Sailors — and the nation I think — want the Navy to remain the most capable Navy, able to answer the call as a 'Global Force for Good.' I firmly believe these efforts will continue.

Department of the Navy Task Force Energy:
www.facebook.com/NavalEnergy

Currents, the Navy's Environmental Magazine (quarterly): www.enviro-navair.navy.mil/index.cfm?pg=currents

Department of Defense Energy Support Center: www.desc.dla.mil/

Q&A with Lt. Col. Rick “Silky” Schilke
Requirements Analyst, U.S. Marine Corps Expeditionary Energy Office

On Aug. 13, 2009, the Commandant of the Marine Corps declared energy a top priority and within six weeks created the U.S. Marine Corps Expeditionary Energy Office (E^2O), with the mission to analyze, develop and direct the Marine Corps’ energy strategy to optimize expeditionary capabilities across all warfighting functions.

E^2O is the Marine Corps’ functional advocate and service representative for expeditionary (aka operational) energy and works in partnership with the Deputy Commandant for Installations and Logistics, the functional advocate for energy aboard Marine Corps installations.

Lt. Col. Rick Schilke, right, and Robert Turner, project support, Experimentation Center, Marine Corps Forces Pacific, listen to feedback from Lance Cpl. Jean Sanchez, Water Support Technician, Communication Company, Headquarters Battalion, 3rd Marine Division, III Marine Expeditionary Force, on an experimental water-purification pump during Exercise Cobra Gold Feb. 11, 2011. Photo by Lance Cpl. Mark Stroud.

The Marine Corps Expeditionary Energy Strategy, signed by the Commandant of the Marine Corps in February 2011, communicates the Commandant’s vision, mission, goals and objectives for expeditionary and installations energy. Specifically, it directs the Corps to increase the energy efficiency of its battlefield weapon systems, platforms, vehicles and equipment and cut in half the fuel used per Marine, per day by the year 2025. The strategy also directs that by 2020, 50 percent of Marine bases and stations will be net zero energy consumers. Setting the course to move from paper to action, the strategy also includes an implementation plan which identifies specific tasks and responsibilities.

CHIPS asked Lt. Col. Rick Schilke to talk about the work of the E^2O.

CHIPS: What are some of the major accomplishments of the E^2O?

Schilke: First and foremost I’d say the success has been actually getting gear that’s available into the hands of Marines to reduce our energy burden on the battlefield. A multifunctional team, led by the E^2O and consisting of Marine Corps requirements, acquisition and technology stakeholders was able to define requirements, identify commercially available solutions, and provide equipment to deploying units while making in-stream improvements. The catalyst for this effort was the Experimental Forward Operating Base (ExFOB), chartered by the Deputy Commandant for Combat Development and Integration.

Equipment was initially provided to one company of Marines — India Company, 3rd Battalion, 5th Marine (Regiment) — who successfully trained and then deployed to Afghanistan with some of the energy efficient equipment as part of a user evaluation. That gear included several solutions: shelter liners to reduce soft-shelter cooling and heating demand; less power-hungry LED lighting for shelters; man-packable solar systems known as the SPACES (Solar Portable Alternative Communications Energy System) to recharge batteries and run tactical radios and laptops, and other low power systems; and, a portable hybrid solar power and battery system called GREENS (Ground Renewable Expeditionary Energy System) that can power slightly larger and more static applications, such as company-level command operations centers.

The SPACES, which is part of a program of record, has been in high demand and been provided to other units in theater and units preparing to deploy. This gear has proven successful in reducing the number of batteries being carried by foot — mobile Marine patrols and the need for battery resupply — it’s truly making a difference on the battlefield. So that is probably the biggest success — moving from a cold start to having solutions that reduce fuel and battery logistics deployed to combat in less than a year.

Additional accomplishments include the development and release of a comprehensive bases-to-battlefield Expeditionary Energy Strategy and Implementation Plan and the completion of a capabilities-based assessment for expeditionary energy, water and waste. The results of that assessment are documented in an initial capabilities document that is in its final review.

CHIPS: Can you talk about the energy strategy?

Schilke: The mission is to be able to deploy a Marine Expeditionary Force by the year 2025 that can maneuver from the sea and sustain its C4I (command, control, communications, computers and intelligence) and life support systems in place, using liquid fuel only for mobility systems, which will be more fuel efficient than mobility systems are today. That is a very challenging mission statement from the Commandant.

The strategy is focused on executing this mission by increasing efficiency in our weapons systems, increasing the use of renewable energy on the battlefield, and finally, the element that underpins the entire strategy: changing our ethos, changing the way we value and employ energy on the battlefield. We recognize that behavior change is key to every aspect of this endeavor. In fact, estimates based on assessments from 2009 tell us that through better energy planning, training, general awareness, and smart employment of our existing systems on the battlefield, we can make about a 25 percent dent in our current battlefield fuel consumption. Today we are burning eight gallons [of fuel] per Marine per day in theater, and we want to get down to four gallons per Marine per day by 2025, for the equivalent force engaged in similar activities and under similar conditions.

Additionally, we want to reduce battery consumption and increase water self-sufficiency in order to lighten the individual load and free up our dismounted Marines from battery and water resupply to the maximum extent we can. So there is a dual operational benefit, increased individual endurance and maneuverability, and increased unit freedom of maneuver and endurance.

CHIPS: Can you talk about the Expeditionary Energy, Water and Waste (E2W2) Initial Capabilities Document?

Schilke: The E2W2 Initial Capabilities Document provides the intellectual, combat development foundation for moving us forward on energy, water and waste capabilities that support the Expeditionary Energy Strategy and Marine Corps future operating concepts. It also is the first step in the JCIDS (Joint Capabilities Integration and Development System) process — defining your needed capabilities and ultimately your solutions. It [ICD] frames the problem, identifies your gaps, identifies non-materiel and materiel approaches you might take to solving those gaps, and then it leads to follow-on effort.

On the materiel side, it leads to other capabilities documents that are more detailed and that initiate future, or modify current, programs of record by defining the desired solution attributes and performance parameters; in other words, the system specifications. Acquisition program developers will ultimately refine the requirements into field-able solutions.

“Today we are burning eight gallons [of fuel] per Marine per day in theater, and we want to get down to four gallons per Marine per day by 2025, for the equivalent force engaged in similar activities and under similar conditions.”

Across all of our systems we want to inject energy as a consideration and get it into the trade space with cost, schedule and performance in acquisition alternatives and source selection. How do we make our systems more efficient to enable things like renewables on the battlefield? How do we make systems more efficient and increase performance at the same time? For example, systems that don’t need as much cooling, or don’t need any cooling or heating. Cooling is a huge [energy] consumer for us right now on the battlefield for systems as well as for individuals. These are some of the questions we’re asking as we look to apply the strategy and ICD approaches to materiel development.

PATROL BASE GUMBATTY (Dec. 31, 2010) Lance Cpl. Dakota Hicks of 2nd Platoon, India Company, 3rd Battalion, 5th Marine Regiment, connects a radio battery to a Solar Portable Alternative Communications Energy System in Sangin District, Afghanistan. SPACES is a flexible solar panel that can be carried by a Marine and is used for recharging radio batteries. With more room in their packs from fewer batteries, coalition forces can pack more essentials, like ammunition. Photo courtesy of 1st Marine Division.

The ICD is already proving useful as a means to identify our needs to the S&T (science and technology) community so we can get them working on the most challenging problems that will require advances in technology. This document will drive S&T efforts that have application across the warfighting functions and will serve as a reference point for all of our future warfighting capabilities.

CHIPS: As the leading edge of the larger Marine Corps Expeditionary Energy effort, ExFOB is identifying and evaluating energy efficient capabilities that can reduce risks to Marines and increase combat effectiveness. Can you talk about the technology that is being developed to achieve this?

Schilke: The first iterations of the ExFOB were essentially an opportunity to find solutions that could have an immediate impact on our energy and water logistics in Afghanistan. Over the next six months, we are expanding and accelerating delivery of those solutions that proved to be successful with the India Company, 3rd Battalion, 5th Marines, to cover 10 battalions in Afghanistan. In May and June 2011, we are coordinating an effort at the Twentynine Palms-based MCTOG (Marine Corps Tactics

35th Commandant of the Marine Corps' Guidance

"The future security environment requires a mindset geared toward *increased energy efficiency and reduced consumption*, thus allowing us *to operate lighter and faster*. We will aggressively continue our pioneering efforts in energy through our Expeditionary Energy Office, with goals of *reduced energy demand in our platforms and systems*, *self-sufficiency* in our battlefield sustainment, and a *reduced expeditionary footprint* on the battlefield…"

and Operations Group), to demonstrate the capability to scale up some of the successful company-level solutions to support a battalion-level command operations center. We are going to run a side-by-side comparison between a conventional battalion COC and one employing energy efficient technologies, such as the thermal liners, LED lights and DC air conditioners, that are capable of being powered by solar systems.

The COC equipment suite will be powered by two hybrid solar-generator-battery systems that were discovered through the previous ExFOB events and developed further to be able to integrate with Marine Corps systems. We will determine if this hybrid system can adequately meet the demands of the battalion COC at a greatly reduced consumption level. We anticipate fuel savings to be in the 30 to 70 percent range. We also hope to collect a lot of data and learn more about hybrid systems.

If that particular solution set is successful, it will deploy with a battalion, currently being identified, to conduct a user evaluation in Afghanistan. A liaison officer from our office is leading the demonstration and will be in theater to support the system deployment and our ongoing energy efforts in Afghanistan. This is similar to the model we used with India Company, 3rd Battalion, 5th Marines.

ExFOB is really a process that includes an annual event. It serves as a catalyst to accelerate commercial or research and development systems into programs and procedures. Through ExFOB we inform our requirements, mitigate investment risks, and build confidence in new technologies. We will use an annual ExFOB event as a means to bring focus to a set of materiel gaps identified in our ICD, beginning with the highest priorities that also have near-term opportunities. This event also informs industry as to the nature of expeditionary operations and the necessary attributes of military expeditionary energy capabilities. In fact, a request for information just closed out, and the responses are being reviewed to determine invitees to the ExFOB 2011 in August.

This year's ExFOB is focused on four key technology areas that support priority gaps and materiel solution approaches identified in our ICD. One is concentrated solar harvesting. We are looking at more innovative and efficient ways to collect, store, and employ solar energy in an expeditionary environment and in the minimum footprint. The other three areas of interest are passive solar water heating, vehicle efficiency technologies and efficient exportable vehicle power. We've asked for industry to come show us what they can do. We will do a side-by-side comparison and evaluation and see what opportunities might be worth pursuing further.

There are a lot of innovative technologies that we are watching that are being developed in the labs, or being improved by industry. Certainly, efforts to more efficiently harvest solar [energy] are big for us because right now that is where we have the best opportunity to harvest renewable energy. There are some ongoing efforts that we now have an oversight role in, including an MTVR (Medium Tactical Vehicle Replacement) fuel efficiency project that will identify opportunities to increase vehicle energy performance and will look at return on investment.

This effort is just kicking off this year and will likely inform all of our vehicle programs, both future and any legacy vehicles that are recapitalized. The project intends to use the MTVR to look at many vehicle technologies ranging from aerodynamic improvements, to driver behavior modification, to hybrid systems.

We've introduced this idea of harvesting energy from vehicles, for example, kinetic energy, or thermal energy, or solar energy, into our S&T objectives for power and energy. We are also looking at this approach on the individual Marine and aboard FOBs. Our vehicles are going to be a key component of our energy [harvesting] on the battlefield as we move toward the vision for the 2025 Marine Corps and getting generators off the battlefield. More efficient vehicles that will harvest, store and share energy for both on-board and off-board systems is a vision we have right now. Vehicles may share energy as part of an expeditionary base grid or form ad hoc power networks. Feasibility of this vision is something we need to assess as we look for ways to achieve the strategy goals.

CHIPS: During your brief at Sea Air Space in April, you discussed how maneuvers are constrained by battery and water needs; how weapon system power limits mobility and wastes fuel; and how the lack of generator maintenance reduces reliability. Can you explain what these challenges mean to an expeditionary force and what the E^2O is doing to help?

Schilke: We are hearing from battalions returning from Afghanistan that batteries are adding significantly to an already burdensome load as they conduct extended dismounted operations over large areas and in difficult conditions. On these dismounted patrols, which range from days to weeks, they are carrying two to three days worth of batteries and water, and are dependent on resupply of these mission critical items. That obviously takes a toll on the Marine in terms of the weight, pushing upward of 120 pounds, when they are moving in a tough environment.

PATROL BASE SPARKS (Dec. 29, 2010) Marines and Sailors of India Company, 3rd Battalion, 5th Marine Regiment, and their Afghan national army counterparts, pose in front of a modified ZeroBase Regenerator in Sangin District, Afghanistan. The ZeroBased Regenerator, nicknamed "the Raptor," after the type of power cells in its six solar panels, can keep more than 17 computers and 15 lighting units running throughout the night. Photo courtesy of 1st Marine Division.

Additionally, they can only get so far off the lines of communication if they're receiving ground resupply. If they are getting air drops, they often have to adjust their maneuver to recover the supplies, or air [supply] sometimes doesn't show up when or where they expect it. It was really becoming a driver of their maneuver and operational timeline. What we see is an opportunity to improve operational effectiveness by reducing that battery burden on the Marines, both at the individual and unit level.

There are some larger scale issues with batteries also. We have weapon systems that are dependent on battery power; some are vehicle mounted and operated on the vehicle, either on the move or at the halt, or can be dismounted from the vehicle, such as jammers, persistent surveillance sensors, and anti-armor systems, and some which are off-board systems, such as artillery fire control systems. These systems require power from the vehicle engine even when stationary. So, idling vehicles that are actively operating systems or charging batteries is proving to be tremendously inefficient for quite a few applications.

You start to see examples of these systems where we are overmatched in terms of our power production to our consumption needs, and really, it comes down to a lack of scalability in our power supplies and energy storage, and the fact that we don't yet have enough access to renewables. There is a phenomenon known as wet stacking — when you're not drawing enough power off what the generator is producing, it actually increases the wear on the generator, and that is a big cause of maintenance problems right now in theater.

Water is another challenge. Marines are carrying several days of water, their water, water for their IED (improvised explosive device) detector dogs. We want to be able to help them do that better and more safely so it enables them to get off the water resupply tether and perhaps lighten the load. In the future, we hope to have a robust individual or squad-level water purification system that is also renewable, powered by solar or some other renewable source. We are still drinking bottled water because that is what the large sustainment contracts are providing.

One of the lessons heard very recently from our combat logistics battalions stated that they could probably reduce their convoys by about 40 percent just by getting off bottled water transportation. This is consistent with previous estimates that about 70 percent of our on-the-road convoy logistics is liquid logistics, and about 70 percent of that liquid logistics is water.

"One of the lessons heard very recently from our combat logistics battalions stated that they could probably reduce their convoys by about 40 percent just by getting off of bottled water transportation. This is consistent with previous estimates that about 70 percent of our on-the-road convoy logistics is liquid logistics, and about 70 percent of that liquid logistics is water."

That is pretty significant because now you are taking trucks off the road, you are reducing the IED threat to Marines, and that has the second order effect of burning less fuel as you reduce the tonnage being transported on, and miles being covered by, very fuel-hungry vehicles. So water self-sufficiency really has a multiplicative benefit across the battlefield. CHIPS

For more information about the U.S. Marine Corps Expeditionary Energy Office (E^{2}O), go to www.marines.mil/community/Pages/ExpeditionaryEnergy.aspx.

Interview with Rear Adm. Sinclair M. Harris
Director, Navy Irregular Warfare Office

Rear Adm. Sinclair M. Harris

Rear Adm. Harris held numerous leadership positions ashore and afloat. His most recent assignments include tours in the Washington, D.C., area at the Institute for National Strategic Studies in the National Defense University; the Navy staff in the Assessment Division (OPNAV N81) Campaign Analysis, Modeling and Simulation branch; and the Joint Chiefs of Staff (J-5) Strategic Plans and Policy Directorate as the Global Security Affairs Division chief for Security Assistance. He was a senior fellow in the Chief of Naval Operations Strategic Studies Group (SSG XXVI). In May 2008, Harris returned to the Office of the Chief of Naval Operations as the deputy director, Expeditionary Warfare Division (OPNAV N85B). The admiral was the commander, Expeditionary Strike Group 5. Harris now serves on the Chief of Naval Operations staff as the director, Navy Irregular Warfare Office (NIWO). The admiral responded to CHIPS questions in writing in June.

CHIPS: As commander of ESG 5, you commanded U.S. Task Forces 51, 52, 55 and 59, overseeing a wide range of missions including maritime security operations and crisis response. When we talked at the Sea Air Space Exposition in April, you referenced the "whole of government" approach for responding to a variety of missions. Can you explain what you mean?

Harris: This is an evolving dialogue. Once we called it 'interagency' and lately, I have heard it referred to as a 'Comprehensive Government Approach.' There are even those that want to enlist private agencies, businesses and the NGO (non-governmental organization) community by referring to a 'Whole of Nation or Society' approach. No matter what you call it, it is clear that many of the challenges the Navy confronts cannot be addressed by military means alone.

Increasingly, we are discovering that the most effective way to deal with our world's complex menu of security challenges, like piracy, or responding to a humanitarian disaster, requires the participation and expertise of multiple departments and agencies across the U.S. government — and international organizations like the United Nations. Terms like this address a growing recognition that the opportunities and challenges we face are so complex, and so interconnected, that no single agency possesses the depth of expertise, requisite authorities and specialized skill sets required to successfully execute these missions.

For example, in counterpiracy [operations] the Navy works with U.S. Coast Guard law enforcement teams, coalition partners, the Department of State, Justice, other intelligence agencies, and even private firms to detect, track and interdict the proliferation of piracy.

ESG-5's support to aid flood victims in Pakistan last year was also based on this concept. In addition to Navy-Marine Corps forces, Army and Air Force specialists were vital to our success. Mostly, the military worked in support of Department of State and in coordination with USAID (U.S. Agency for International Development) and [the] World Food Program to deliver food, water and other supplies. And, all this was in support of and in concert with the Government of Pakistan.

CHIPS: You said while you were leading the antipiracy task force, you were inspired by the participation of navies from a wide range of countries including China and Iran. Can you talk about how the coalition of navies work together?

Harris: I did not lead in the antipiracy effort, but was one of many commanders supporting that effort. The task forces confronting piracy off the Horn of Africa and Gulf of Aden are an excellent example of maritime cooperation in action. There are multiple task forces executing this mission — Combined Maritime Force, NATO, EU (European Union) and others. These groups work in coordination, and de-confliction of zones of responsibility and operation is a continuing issue.

Overall, the international effort is largely a story of successful partnering among a coalition of the willing. There are multiple efforts, albeit with differing rules of engagement and responsibilities, but all are focused on counterpiracy. Combined Task Force 151 is the U.S. Navy component to this effort. There is a European Union Naval Force working this mission, along with CTF 152, which is an international force deployed to counter piracy. CTF-152 is also a success story — that command rotates among different nations, including Bahrain, India, Singapore and others. Then there are those who we refer to as the 'independent operators' to include Russia, China, and even Iran, who have ships deployed in the region to protect their own cargo vessels.

While not formally part of any of the international counterpiracy efforts, U.S. Navy forces have in the past engaged with the naval forces of these nations. There are always communications taking place between ships to understand missions, intent, position and other information. These so called 'bridge to bridge' contacts can often prove valuable and knock down barriers in terms of language and better understanding in how different navies operate.

CHIPS: State Department representatives say that solving the piracy situation off the coast of Somalia is difficult and complicated by many factors including Somalia's weak government and dire poverty. In addition to patrolling the waters off Somalia, what can be done to discourage piracy and assist in the economic development of Somalia?

Harris: This is an issue that the Department of State is working with its Piracy Contact Group. They are much better suited to answer that question.

CHIPS: We also talked about the push to formalize a comprehensive approach to a variety of mission sets instead of the ad hoc methods commanders are forced to use as new requirements develop. Are you working *to formalize U.S. government, public, private and international partnerships, as well as procedures for integration and interoperability with partners?*

Harris: NIWO is working to formalize how we as a Navy work with others in this approach. We meet regularly with groups in and outside of DoD to see how to better integrate and operate.

CHIPS: The Navy's vision for irregular warfare describes a number of objectives to overcome threats, such as promoting regional security by training nations in maritime security; enhanced regional awareness of activities and social dynamics for a deeper understanding of cultural, ethnic and socioeconomic norms; and promoting economic opportunities and regional stability to help vulnerable populations from turning to terrorist or criminal activity. These are ambitious and complicated objectives. How will your office further progress in these objectives?

Harris: All of these objectives and efforts take place within the overall context of the strategies and goals that the U.S. government, through the State Department and DoD regional combatant commanders, want to see implemented. To better define and comprehensively explain what the naval force contribution to these mission sets is all about, the Navy, Marine Corps and Coast Guard are cooperatively developing a doctrine for maritime stability. This document should be completed later this year and will be integrated into the larger joint guidance for Security Force Assistance.

Second, the Navy continues to expand and make investments in growing its Language, Regional Expertise and Culture (LREC) elements across the service. An overall plan is now being implemented with the goal of teaching vital languages to our service members to prepare them to confront irregular challenges when needed.

A good operational example of how these objectives are put into practice can be seen in the Africa Partnership Station deployments. Originally only focused on the East Coast of Africa, APS had expanded to the west coast and the Gulf of Guinea region over the last year. Through repeated deployments and working with local naval forces these APS deployments have boosted the overall naval proficiency and training of regional forces. The bottom line of APS is to help local navies better patrol, enforce and conduct missions across the irregular challenges seascape so that extremists, and other unlawful elements that undermine the role of good governance, cannot establish themselves.

CHIPS: The Chief of Naval Operations said, "Leveraging the maritime domain will dissuade, deter and defeat irregular actors who seek to undermine security, stability and property." How will this be achieved?

Harris: Securing the maritime commons is absolutely vital to the continued prosperity the world's nations enjoy from globalization and trade. A host of underlying trends, ranging from changing demographics to more severe humanitarian disasters, are expected to create more issues across the littorals and lead to the proliferation of irregular challenges in coming years. That is what the Navy's 'Vision for Confronting Irregular Challenges' is all about — to engage with local forces on a persistent basis to improve their ability to confront these challenges before they spiral out of control and result in the formation of new ungovernable places like Somalia.

Confronting irregular challenges across the maritime domain is a top priority. But deterring and defeating irregular actors is increasingly a concern to the world's naval leaders as well. In October 2009, over 100 of the chiefs of navies from around the world gathered at the Naval War College to discuss such common issues as maritime domain awareness and improving cooperation and communication. It was a resounding success, and the next International Seapower Symposium will take place later this year. CHIPS

The Chief of Naval Operations and president of the U.S. Naval War College will co-host the 20th International Seapower Symposium at the U.S. Naval War College in Newport, R.I. Oct. 18-21, 2011. This event will allow the CNO to interact with his counterparts, chiefs of navies and coast guards from around the globe. For more information go to www.usnwc.edu/Events/International-Seapower-Symposium/ISS.aspx. The 20th ISS theme is "Security and Prosperity through Maritime Partnerships."

U.S. Navy's Vision for Confronting Irregular Challenges

STABILIZE … STRENGTHEN … SECURE

Vision Statement

The U.S. Navy will meet irregular challenges through a flexible, agile, and broad array of multi-mission capabilities. We will emphasize Cooperative Security as part of a comprehensive government approach to mitigate the causes of insecurity and instability. We will operate in and from the maritime domain with joint and international partners to enhance regional security and stability, and to dissuade, deter, and when necessary, defeat irregular threats.

We will confront irregular challenges by focusing on the following outcomes.

- Increased effectiveness in stabilizing and strengthening regions, by securing and leveraging the maritime domain, with and in support of national and international partners.

- Enhanced regional awareness of activities and dynamics to include a deeper understanding of ethnic, cultural, and socioeconomic characteristics and norms.

- Increased regional partner capacity for maritime security and domain awareness.

- Expanded coordination and interoperability with joint, interagency, and international partners.

To read the U.S. Navy's Vision for Confronting Irregular Challenges, go to the CNO's homepage on Navy.mil: www.navy.mil/cno/index.asp.

For more information about the work of the U.S. Department of State Piracy Contact Group go to www.state.gov/r/pa/prs/ps/2009/05/123584.htm.

GOING MOBILE

News from the DON Mobility Program

By Mike Hernon

This is a very active year in the area of enterprise mobility. In the commercial marketplace, dozens of new devices, the vast majority of which are tablets, were released, or announced for imminent release, as manufacturers race to meet growing consumer demand for greater mobile performance and functionality.

The Department of Defense mobile user community is no exception and expresses great interest in deploying tablets and smart phones more broadly to support the DoD mission from the executive suite — to the tactical arena. Within the Department of the Navy there are numerous requests for these devices to support senior executives, hangar deck operations, tactical deployments, and more.

This installment of Going Mobile will provide a number of updates on DoD and DON developments for enhancing mobility, summarize efforts, and look at potential future capabilities.

Overarching Policy Remains in Effect

Many Navy and Marine Corps personnel acquired smart phones and tablet devices to take advantage of advanced capabilities, such as enhanced document management. While the DoD and military departments are working to integrate these devices into the network to increase user efficiency, it is important that users understand that the overarching wireless policy, DoD Directive 8100.02, "Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)," remains in effect.

Consequently, use of these devices, even for government-furnished equipment, is subject to the following security requirements: (1) device may not be connected to any DoD or DON network for any purpose until Designated Accrediting Authority (DAA) approval is published; (2) device may not auto-forward government account email to a commercial email account; (3) device passcode must be enabled, and the simple passcode option, if available, must be disabled; and (4) device may not be brought into any area where classified information is stored or discussed without prior approval.

The demand to use mobile devices in areas where classified information resides or is processed remains strong. The National Security Agency (NSA) is drafting new guidance on this restriction; however, given the known vulnerabilities and potential exploitation paths, a blanket approval is not expected. Users, who have a requirement to use wireless devices in areas where classified material is processed, should continue to work with their command's information assurance manager to pursue approval for a local policy.

DoD Commercial Mobile Devices Working Group

In acknowledgement of other efforts underway, the DoD Chief Information Officer chartered a working group to explore whether to allow certain commercial off-the-shelf wireless devices on the network. The working group will facilitate introducing new devices and capabilities through information sharing across the DoD community. The working group will leverage certification and accreditation artifacts produced by any DAA, conduct pilots, and speak to industry representatives with a combined DoD voice. Membership includes the DoD and service CIOs, DAAs and wireless subject matter experts.

Secure Mobile Environment – Portable Electronic Device (SME-PED)

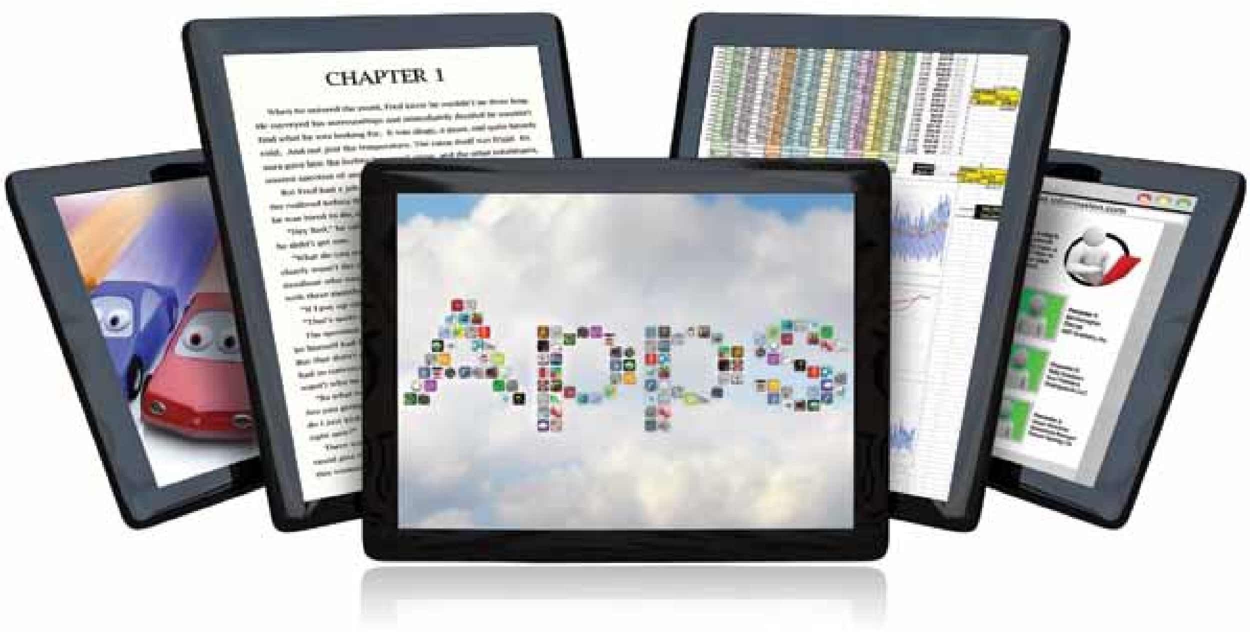
The SME-PED is nearing its end of life for technical and programmatic reasons. Technically, the circuit-switched data service that supports the secure voice capability of the SME-PED is being phased out by all cellular providers. Circuit-switched data is a legacy, slow speed data service that has little commercial value as providers continue to move to fourth-generation data networks. Unfortunately, a SME-PED cannot use 4G data networks to support secure voice. However, unclassified data and voice service, as well as connection to the SIPRNET, will continue to work.

Programmatically, the NSA, which led the development of the SME-PED, decided not to pursue further development on this device. While a Voice over Internet Protocol (VoIP) solution was envisioned to replace circuit-switched data secure voice, NSA decided the time and expense that would be incurred would not be cost efficient given the relatively small number of users it would serve. It is expected that much of the SME-PED capabilities will be met by the Commercial Solutions for Classified (CSfC) program.

Commercial Solutions for Classified Program

NSA launched the CSfC program to further extend COTS efforts into the classified area. NSA wants to provide classified wireless solutions in a manner that is significantly faster and cheaper than in the past. A key to this effort is implementing "good enough" security, for example, not building top secret protection into a solution that will be only used for secret communications.

As with the unclassified COTS solutions, CSfC will rely on additional software components to enhance the IA posture of COTS devices. NSA pilots are underway and broader deployment may be seen by the end of the year.



COTS Unclassified Solutions

Developing government-unique devices, such as the SME-PED, requires an enormous effort and significant resources. Given the fast-paced nature of the wireless industry, by the time a government solution is fielded it is likely to be obsolete. In recognition of this, significant work is underway to better leverage industry COTS solutions. Commercial devices still require some customizing to meet DoD information assurance requirements, such as Common Access Card support, encryption and centralized management. These requirements are being addressed by various software developers for a number of different platforms. When proven to work, a Security Technical Implementation Guide (STIG) will be released by the Defense Information Systems Agency. The STIG will provide DoD-approved, formal guidance for connecting COTS devices to Defense Department networks. STIGs are already in place for Windows Mobile and BlackBerry devices.

It is likely that devices based on Apple iOS, Android and RIM QNX operating systems will be approved for unclassified network connectivity in the coming months. Users should be aware, however, that to meet IA requirements, not all of the popular features available in the consumer model of a device will necessarily be available in the STIG-compliant version.

Apple iOS. The demand from the user community for iPhones, and even more so for the iPad, continues to be strong. The military departments are working to deliver this capability in a way that meets IA requirements. It is expected that a STIG for iOS devices will soon be adopted by DoD.

Android. There is similar demand for devices based on the Android operating system. DISA began developing a STIG for Android, and it is expected that these devices will also be approved shortly.

Research in Motion. The makers of the BlackBerry, which is ubiquitous within the DoD, also entered the tablet market with the release of the PlayBook. Because it is based on a new operating system, QNX, the PlayBook will require a more extended certification and accreditation effort than the routine release of a new BlackBerry. However, the C&A and draft STIG processes are underway and approval is expected.

Future Direction

The wireless work conducted throughout the DoD will not only provide improved mobility capabilities in the short term, but will also lay the groundwork for additional enhancements. Among the most exciting of these are: development of a DoD mobile apps store under investigation by DISA; allowing dual-use devices that will have both a "personal" and "government" profile that are segregated; and the potential for the government to act as a virtual mobile network operator, which would provide better IA controls across the entire communications path.

The DON CIO wireless working group remains engaged in all these efforts. To contact the group, email them at wireless.fct@navy.mil. CHIPS

Mike Hernon is the former chief information officer for the city of Boston. He supports the DON CIO in telecommunications and wireless strategy and policy.

Additional wireless information can be found on the DON CIO website: www.doncio.navy.mil/wireless.

NMCI Mobile Users Must Transition to NAVSUP Fleet Logistics Center San Diego Contracts

Users with Navy Marine Corps Intranet BlackBerrys, cellular phones or air cards must transition to the NAVSUP Fleet Logistics Center San Diego wireless contracts by Oct. 1, 2011. At that time, NMCI will phase out cellular devices and services offerings. Users who have not transitioned by Oct. 1 will have their services interrupted.

The contracts, an ordering guide and template, as well as the latest information are available on the Naval Supply Systems Command website at **https://www.navsup.navy.mil/navsup/ourteam/navsupgls/prod_serv/contracting/market_mgt.**

For additional information contact the FISC San Diego wireless team at **cellmac@navy.mil**.

DON Enterprise Architecture
Version 2.1.000 is Released

By Fumie Wingo

The Department of the Navy Chief Information Officer published the DON Enterprise Architecture v2.1.000 in April. As a result of stakeholder feedback, and in a continual effort to improve the practicality and usefulness of the DON EA, this release does not contain new artifacts. Instead, it refines existing DON EA processes and compliance and documentation requirements.

The changes in DON EA v2.1.000 include:

- Applicability and compliance criteria for some contents are updated to clarify tailored requirements based on each program, system, investment, or initiative size and type and its point in the acquisition life cycle;

- "Documentation Required" is added to the DON EA content types, which describes the usage requirement, to provide more options to meet compliance criteria; and

- Subject matter expert review is added to the DON EA compliance assessment process to adequately evaluate programs for information and cybersecurity related contents. Other contents were removed due to the lack of maturity in compliance review criteria.

Changes to the Department of Defense IT Portfolio Repository-Department of the Navy (DITPR-DON) to incorporate DON EA v2.1.000 updates are also implemented.

Many DON EA activities are underway. However, there is not easily understandable representation for these activities, how they relate to each other, and how they support achieving the department's overarching business goals and objectives. The lack of a consistent communications mechanism led to a lack of common understanding among DON EA stakeholders and participants about "where the DON EA is going." To address this issue, the DON CIO is developing a DON EA Strategic Roadmap with active stakeholder involvement. The strategic roadmap will be used to ensure alignment of near-, mid- and long-term DON EA activities with overarching DON business goals and objectives.

In addition, the DON EA Strategic Roadmap will be used as a key communications mechanism with DON senior leadership and internal stakeholders, as well as external partners.

To ensure the DON EA is providing true value to the enterprise, a key area of focus during the remainder of fiscal year 2011 and early fiscal year 2012 will be to incorporate key attributes of the strategies and plans associated with ongoing DON IT/cyberspace efficiency initiatives into the DON EA.

The architecture artifacts associated with these key attributes will be identified in the DON EA Strategic Roadmap to clearly demonstrate their alignment with overarching DON business goals and objectives.

Authoritative information about DON EA policy, procedures and content can be found at https://www.intelink.gov/wiki/DONEA. CHIPS

Fumie Wingo is the Department of the Navy enterprise architecture lead.

Talking with Capt. Paul C. Stewart
Commanding Officer, Naval Research Laboratory

Capt. Paul C. Stewart

NRL — 85 years of innovation

NRL helps make the U.S. Navy and Marine Corps the most formidable naval fighting force in the world with a record of technical excellence that has a profound importance to national security. NRL is the corporate research laboratory for the Navy and Marine Corps and conducts a broad program of scientific research, technology and advanced development. NRL has served the Navy and the nation for more than 85 years and continues to meet the complex technological challenges of today.

It was Thomas Edison, commenting in 1915 on the war raging in Europe, who argued that we should look to science to keep the nation safe. "The government," he proposed, "should maintain a great research laboratory." NRL became that laboratory, opening its doors in 1923.

NRL's research programs span the scientific spectrum, including studies in biomolecular engineering, remote sensing, virtual reality, superconductivity, nanoscience, and solar corona monitoring. NRL is the Navy's lead laboratory in space systems research, fire research, tactical electronic warfare, microelectronic devices, artificial intelligence, and research in ocean and atmospheric sciences. NRL shines as the Navy's corporate laboratory and as one of the federal government's leading in-house centers for innovative research in the national interest. CHIPS spoke with Capt. Stewart in June.

CHIPS: What single NRL-developed technology has the largest and most far-reaching effect on the fleet and industry?

Stewart: It is very hard to put your finger on one certain technology that has made the laboratory great. It is a collaboration of many different investments in basic research over many years since the '20s. Clearly, sonar is one of those big inventions that led back from the '20s all the way forward to many different investments and many different technological breakthroughs.

Radar was invented here and first discovered on the Potomac River. Two communicators were talking across the Potomac River when a ship passed between them, and they got radio wave reflections. That was the first discovery of the phenomenology of radio wave reflection. Since then, NRL has had about 90 years of investment in radar technology, and that includes the full spectrum of surface ships, aviation, and all types of basic research that feed into radar. That is one that was a game-changer.

When we look across the spectrum of naval assets today, many people and many flag officers point toward nuclear power as one of those game-changing technologies brought forth by the NRL back in the '30s that has changed the nature of warfare and warfare at sea. Without nuclear-powered submarines and carriers, we would be fighting a completely different type of battle. The first successful uranium-235 isotope separation was done at the laboratory and then moved off [to DOE]. There are many years of history with DOE (Department of Energy) and Adm. Rickover (Adm. Hyman G. Rickover). Without Adm. Rickover's push forward, we wouldn't be where we are today. The concept of a nuclear-powered submarine was first on the drawing board in the mid-30s by Dr. (Ross) Gunn at the laboratory. He was the one who put together the concept and took it to the Bureau of Engineering, which we know today as NAVSEA, or Naval Sea Systems Command. It was that concept of a nuclear-powered sub that brought forth what we have today. The Bureau of Engineering gave Dr. Gunn about $2,000 and sent him back to the NRL to work on his concept. The Bureau of Engineering later sent a young naval officer named Hyman Rickover to see what the scientists down at the laboratory were working on. We have nuclear power today because of that collaborative relationship between the Bureau of Engineering and the researchers. That is where you see the great news stories across the laboratories and across the Navy; it is that collaborative relationship between the warfighters, the operators and the researchers. The NRL does not ever want to be known as scientists that are in their laboratory simply doing work for the sake of scientific research. We're there to support our customers, whether they be Navy, Marine Corps — or any of the services — we want to be on the cutting edge of pushing technology forward.

> "There are many 'firsts' at the laboratory — radar, sonar, GPS and electronic warfare."

There are other great examples besides nuclear power. The space program in the United States, the birthplace is really here at the NRL. It started with the rocket technology that the Germans invested in back in World War II and with captured German V-2 rockets. In the United States, in 1946, the Army took the rockets and weaponized them, and that's where the ballistic missile program came from.

The NRL took V-2 rockets, and we used them to put sensors outside of the atmosphere to look back at the ionosphere to understand how radio wave reflections are affected by the ionosphere. When we were kids and turned on the AM radio in New England, we could hear radio stations from Georgia and Alabama, and you knew that there was something going on with the radio waves certain times of the day. It was the HF (high frequency) propagation [transmission] off the atmosphere. A technology discovered at NRL in the 1920s, known as the 'Skip Distance' effect, [is caused by reflection and refraction of radio waves from the ionosphere]. It wasn't until we brought rockets into this country in 1946 that scientists had an opportunity to use those platforms and study the phenomenology to understand what was going on in our atmosphere. We put sensors up, and we looked at the ionosphere to understand it, and that was essentially where the space program and space exploration began here in the United States.

"It was years later, in the 1950s, with the successful launch of the Vanguard satellite, shortly after Sputnik, we spun off about 250 scientists to form the space side of NASA."

It was years later, in the 1950s, with the successful launch of the Vanguard satellite, shortly after Sputnik, we spun off about 250 scientists to form the space side of NASA. Prior to that NASA was a different organization, mostly focused on aeronautics and aviation. President [Dwight] Eisenhower stood up that organization [Goddard Space Flight Center in Greenbelt, Md.].

There is a whole other area of space and exploration that we don't talk about much, which is spy satellites. The world's first signals intelligence satellite came from NRL. It was declassified about 15 years ago. It is called GRAB (Galactic Radiation and Background) and is the birthplace of the National Reconnaissance Office. The NRO and the NRL worked together very closely back in those days before the NRO actually had a name.

The intelligence community for many years relied on the very smart people here at the laboratory, who were trying to use space as an enabling media, to fight the next generation of war. We wouldn't be able to fly our jet engines the way we do today without the chemistry department at the laboratory, which focused on the 'Navy after Next,' always looking for what is the next great [game-changer].

The chemistry department has been working in nanotechnology for 35 years — well before it was ever a buzzword in the press. We see nanotechnology as an enabling capability of science that is going to change the way that we live in the next 10 to 15 to 20 years.

We do more work with the material known as graphene than probably any facility in the country. We see graphene as an enabling material to change the way we fight in the future. That could be anything from armor to computers, to power generation, and electronic warfare systems.

GPS is another example of one of those systems that has touched every American and everybody in the world. The Global Positioning System in your phone was invented here by Roger Easton. The program was called Timed Navigation (TIMe/navigATION or TIMATION), and it used the atomic clock based in space and time-distance navigation on the Earth. That clearly resonates with everybody under 25. All of my kids know what GPS is, and everybody 'speaks GPS.' Back in the 1960s, the people here at the laboratory had a good idea; it was great engineering, and they pushed the idea forward.

"The world's first signals intelligence satellite came from NRL. It was declassified about 15 years ago. It is called GRAB (Galactic Radiation and Background) and is the birthplace of the National Reconnaissance Office."

We are working on the improvements to the next generation of GPS. The next generation will be more reliable and support our warfighters. iGPS, Improved GPS, will be one of those systems that will be coming out in the next three years, and it will change the way we fight.

There are many 'firsts' at the laboratory — radar, sonar, GPS and electronic warfare. Then there are areas that we don't talk about a lot like fracture mechanics, the way things fail, and the way we engineer and test materials. The father of fracture mechanics, George Irwin, was at the laboratory for many years.

Back in the 1940s, the issue at hand for the Navy was Liberty ships [mass-produced cargo ships] that were coming back from World War II and were cracking. We put together a huge program at the laboratory to understand why the structures were failing. Analyzing structures, and not just ships, vehicles, cars, buildings, bridges, and everything that is structural — there isn't a structural engineer in the country that does not fully understand the impact of fracture mechanics.

There are areas of science that we do not talk about that are behind the scenes [in fracture mechanics] and people take for granted. [For example, to ensure] their cars will crumple in the right way when they get into a car accident, or if a building collapses that it will collapse in the right direction [to minimize injuries], or that it won't collapse.

CHIPS: What recent technology has the most immediate impact on the fleet?

Stewart: When you say recent, I like to look in the last 10 years. What has transitioned to the fleet that has made a big financial or a big operational impact? There are some that have made an operational impact that we can't talk about because of their classification level.

Corrosion is a $6 billion problem in the Navy. It is amazing how much money and time our Sailors spend scraping, painting, scraping, painting and doing maintenance on our vessels and our aircraft. This is a very big issue, and it is not just the rust that is on the surface, there are lots of other [corrosion] issues.

The chemistry department at the lab has been concerned about corrosion for about 50 years. They have been investing in all different types [of coatings] and trying to find new coatings and new applications. The [commander of] Naval Sea Systems Command, Vice Adm. [Kevin] McCoy said that NRL coating systems and single coat systems save the Navy between $250 and $300 million a year. That's cost avoidance. That's significant savings, and that money can be used elsewhere, but $250 million of a $6 billion problem is just a drop in the bucket. We have many other investments that we are pushing forward to reduce maintenance. We are looking to do away with paint, and in the future, we are changing the way we put ships together and how we weld.

Power and energy is the key topic. The Secretary of the Navy's goals set some very high standards for the Navy and Marine Corps, and we are working hard to meet those standards. One of the areas we have tested in the laboratory, and we think will be out soon, is the next generations of fuel and power.

Battery technology is a very big investment. The next generation of batteries will surpass our modern day lithium ion. Other systems that have been tested in the fleet, but are not on ships, are some of our autonomous fuel cell UAVs (unmanned aerial vehicles). A fuel cell powered UAV that is very quiet and can carry a payload is a game-changer. It depends on what type of platform it might be launched off, but UAVs will be able to be launched off any platform.

Autonomy is a big area of investment. Here at the laboratory, we broke ground last year on the Autonomous Systems Research Laboratory, the ASRL. It is a 50,000-square-foot facility that is going to change the way we work on autonomy. It takes about 20 different areas of autonomous investments in science and puts it all into one building. That is the beauty of the laboratory, it is a collaborative environment.

As an oceanographer, I am always concerned about the weather. The Navy's NOGAPS (Navy Operational Global Atmospheric Prediction System) was one of the best in the world, but today it is about middle of the road compared to some of the other models. We are working on the next generation of global models that will revolutionize how weather models, oceanographic models and space weather models are all interconnected.

Modeling and understanding the atmosphere affects all of us. Weather touches all of us. In the Navy, we have always been concerned about how the weather affected our ships, aircraft and submarines, underwater weather, or oceanography. For years we have enjoyed the position of being one of the global leaders in prediction, and we are pushing the envelope on where we are going in the future with that.

People who have not been out on a ship or a submarine scratch their heads and say why is firefighting such a big concern for the Navy. You can't get off the ship, and you can't get off the submarine, you have to fight it. You have to be able to survive a fire if it occurs when you are out at sea, so NRL has many years of investment [in firefighting and damage control].

AFFF (aqueous film-forming foam) was invented here, PKP (Purple-K-Powder) was invented here, high pressure water mist systems were invented here, and many of the communications systems that we use in our damage control systems on board ships were developed here at the laboratory. Every commercial airport in the world uses AFFF. We are working on the next generation of environmentally friendly AFFF. We are testing new chemistries and how those firefighting agents will fight fires, such as biofuel fires. We are bringing biofuels into the fleet in the next five years. How are we going to fight those fires? Are they going to be fought in the same way? Is the chemistry the same in a biofuel as it is in a hydrocarbon-based fuel?

Firefighting research and protection of our Sailors and Marines at sea is a critical area. Nine of the firefighting systems on the Littoral Combat Ship class were born here and tested at the laboratory.

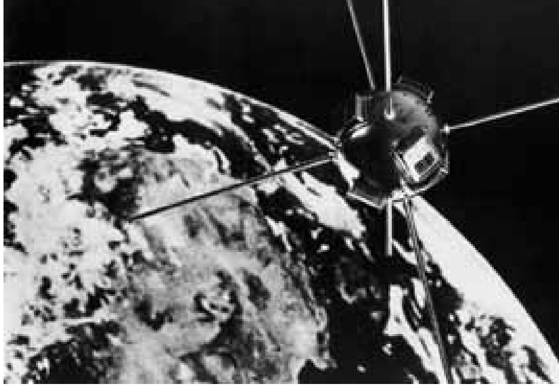
CHIPS: Could you talk about the transfer of technologies developed at NRL to industry?

Stewart: Science doesn't do anybody any good if it sits on the shelf of a laboratory. Every scientist here at NRL has the goal to do world-class research, but then they want to see it out there. We transition a great deal of our research into the commercial world; we partner with industry. The first CRADA, or Cooperative Research and Development Agreement, was signed at the NRL in the 1970s. Those CRADAs are important to the way we work together with industry as partners.

Basic research, or 6.1 [funds], and applied research, 6.2 [funds], are spent here at the laboratory, and then we want to find a transition partner. Sometimes those transition partners are the warfare centers, sometimes industry or other partners, but industry always has a key interest. They are always looking at the products coming out of 6.2 or 6.3 spending inside the Navy to see if there is a business opportunity.

If you look across the history of our investments, and that includes sonar, radar and electronic warfare, you will see that many of our concepts and ideas transitioned to a prime contractor who then brought them out into the fleet. You are not going to see NRL stickers on any of them, but what you will see is the patent law and the intellectual property tracking behind those. Companies, such as L-3 (Communications), Raytheon, Lockheed (Martin), and all of the big primes that you are familiar with, they know where the great research is done, and they watch our work very carefully.

The Office of Naval Research, our parent organization, hosts the Naval Science and Technology Partnership Conference, which is tentatively scheduled for the summer of 2012. The conference is filled with industry partners across all of the spectrums of naval warfare. Over the history of NRL, we have signed about 250 CRADAs with industry, universities and nonprofit organizations. We also partner with other government organizations



Above, the three-pound, grapefruit-sized Vanguard satellite launched on March 17, 1958. A team of Vanguard I scientists mount the satellite in the rocket. Photos courtesy of the NRL.

> Graphene is a relatively new carbon-based material with high potential for new fundamental science and technological applications. Graphene is a single sheet of graphite, which is either exfoliated from bulk graphite onto a substrate or "grown" by desorbing Si at high temperature from a SiC substrate. Our research is initially focusing on achieving wafer-scale growth of high-quality graphene followed by the pursuit of new science and electronic/sensor applications.
>
> – Naval Research Laboratory

and agencies. We do a lot of work for a lot of customers at the laboratory.

When you look at the spending profile at the laboratory, we don't have a budget. People are shocked by that, but the NRL is a 'coin-operated' laboratory. Every dollar that comes into the laboratory comes through a scientific proposal, including my salary. We do not have appropriated funds; we don't get money from Congress directly. The funding model at the laboratory is interesting. We operate everything including the buildings and the maintenance of the buildings, the salary and all the research through scientific proposals.

To leverage those dollars, we work with a lot of different organizations and a lot of different countries. We work with anybody that is interested in an area of investment that we are. About 60 percent of my budget, of our spending, comes in from Navy and Marine Corps sponsors, across the full spectrum, from operators to scientific organizations. Forty percent of my budget comes from non-Navy sponsors, and a lot of that work is dual-use. For instance, much of the work that I do for the Air Force is in satellite programs, and many of those satellites are the same ones [the Navy uses].

Many of the agreements and sponsorships that we enjoy, we put together after years of collaborative work together. We try to leverage research dollars. The operators and the Pentagon are primarily looking at the next two or three years, and the NRL is looking 15, 20 or 25 years down the road. With research money, you spend a couple of dollars today, and who knows what you might get 20 years from now. GPS is an example of that. The Navy didn't want to invest any money in it in the 1960s. They didn't see it as a scientific endeavor that they wanted to fund, so it was done with other sponsors. That is one of the major reasons that the Air Force picked up GPS and was the transition partner from the laboratory.

The licenses and agreements that we have are broad spectrum. We have the largest patent office inside the Department of Defense. We have quite a few patent lawyers to protect the intellectual property of our scientists. Our scientists own the intellectual property, and the royalties go to the scientists, as well as to the laboratory. We put that money back into the science program so the money is reinvested in the lab.

There are some areas of investments that are not going to transition next year or the year after. They may transition after 10 years of investments and science. Those are things that we track. We have a lot of metrics to talk about, the number of agreements, CRADAs and licenses, but I won't go into great detail. What you need to look at is the much broader spectrum of how we partner with all of these organizations to leverage the great science to get it out to the operators or to whomever those sponsors might be.

"The NRL does not ever want to be known as scientists that are in their laboratory simply doing work for the sake of scientific research. We're there to support our customers, whether they be Navy, Marine Corps or any of the services, we want to be on the cutting-edge of pushing technology forward."

CHIPS: Do you have any suggestions to streamline the acquisition process for new technologies developed by NRL?

Stewart: That's a touchy topic, and I have to be very careful about what I say. We work with some organizations that seed great research, and they want to transition it, and we work very closely with them to get it out there. Many of those [transitions] are done through CRADAs; many of those are worked with industry partners. When we build a system that has many years of 6.1, 6.2 and 6.3 spending, it gets into an [industry] transition and out to the fleet.

We are not a factory at the NRL. We like to build 'one-of' systems, or maybe two or three, and then bring industry in and let them build the rest. When they have to go through the rigorous process of the [DoD] acquisition world, sometimes it slows down that process. Many times the research that was great 10 years ago is now passé or is now the standard throughout the world. If we are not able to streamline it, and put it into a process and move it out there quickly, that is one of the risks that we run.

The leaders of the acquisition community throughout the Navy are aware of the concerns. You have to take pieces of the acquisition process and streamline that. The CNO has a new program that we are working on with N00X called 'Speed to Fleet.' The concept for that is that we get things out of technology quicker and get them out to the fleet quickly, and we test them.

One of the risks of getting science out there (every ship driver or every guy in an aircraft that has ever experienced this knows), the scientist shows up on the pier with some new box, he brings it on your ship, he walks away and leaves it — and it doesn't really work. That's the last thing the research community ever wants. We want to bring something out to the fleet, to be there with the fleet the whole time while we operate these things, and get their feedback and tailor it to fit their needs exactly. When we do that, we get a great relationship.

We work closely with the Special Operations Forces. SOF streamlined their process so we can build them systems and get them out there very quickly so that they can take care of the very sensitive nature of their business. They need the best programs out there. We have been able to streamline the acquisition process with certain customers. The CNO is focused on Speed to Fleet and he is making a brief this afternoon [June 1] at ONR on this topic.

The acquisition community writ large needs to take a big round turn and figure out how we can pull apart certain aspects and processes of acquisition today to make it more efficient and also to protect our laws. It is a very challenging problem. [Assistant Secretary of the Navy for Research, Development and Acquisition] Sean Stackley has a lot on his plate to take that topic on, but clearly it is something that he is concerned about. We, at the bottom of the scientific food chain, are very concerned because my scientists are passionate, and they want to get their systems out there as quickly as possible and save lives.

I will give you two examples. A couple of times in recent history, the Pentagon came to the lab, and said, 'We have a real need. We have young men and women that are getting wounded in Afghanistan and Iraq by low velocity projectiles from IEDs (improvised explosive device). What do you have on your shelf that you can turn around quickly and get out to

"The Naval Research Laboratory is one of the Navy's, if not one of the nation's, best kept secrets. We have a rich history here, and it is just a lot of fun."

us?' We came up with a program in 2003 called QuadGuard, a lightweight body armor. In about 16 months we had the first versions out in the fleet. We worked with an industry partner, and in a short time, we had lightweight body armors that augmented the body armor [they already had] and at a low cost. IEDs were another threat to our Sailors, Soldiers and Marines that we needed to combat very quickly. We worked hard behind the scenes to get things out there to save lives. One of the issues is that some of the technologies that we have are not going to transition into a direct program of record.

CHIPS: During your Navy career which is your most rewarding or interesting assignment?

Stewart: Hands down the NRL. I am a kid in a candy store. You see that kind of passion here at the laboratory in young college adults in their 20s to 80-year-old researchers who have been at the lab for 50 or 60 years. There is a passion and a love of working on science that is able to save lives, change the way we live, change the way the world lives, and the way the world fuels itself.

There are all kinds of different areas to talk about. The Naval Research Laboratory is one of the Navy's, if not one of the nation's, best kept secrets. We have a rich history here, and it is just a lot of fun.

I am an oceanographer and my passion is oceanography, and I get to do a little bit of that every now and then, but it is the broad investment and spectrum of the lab that I love so dearly.

It's rare that you get to wake up every single morning, excited to go to work and enjoy what you do. It's just a fun, fun place to be. I feel very privileged. I feel honored to be here working with some of the best scientists in our country to solve the problems of the future for the Navy and the Marine Corps and the other DoD services. CHIPS

For more information about NRL, go to www.nrl.navy.mil, or follow the NRL on Facebook and Twitter. Contact NRL's public affairs office at (202) 767-2541 or info@pao.nrl.navy.mil.

SCIENCE, TECHNOLOGY, ENGINEERING, MATHEMATICS
NRL Student Programs

The NRL encourages broad knowledge in all scientific disciplines to help ensure that cutting edge scientific capabilities exist in the future. Successful candidates at the graduate and postdoctorate levels can expand career goals by participating in research activities; interacting with scientists from NRL, other laboratories and academia; participating in scientific conferences and seminars; and publishing research results. CHIPS asked Capt. Stewart to discuss how NRL engages students at all age levels to foster interest in science, technology, engineering and mathematics (STEM).

I can t talk about the NRL program without first talking about the much broader program in the United States. The scientific education of our kids is a major problem, and it is recognized by leadership in our country. A National Academy of Sciences book, written about five years ago by Dr. Norm Abramson, 'Rising Above the Gathering Storm, talks about the problem and how we can mentor and educate our kids [to have an interest in science and math careers].

When I look at the NRL, and our future staffing, we are concerned about that because we want the best people, the smartest people to be working on the next generation of problems that affect U.S. citizens. We have many STEM programs at the lab and throughout the entire Navy. I would argue that the NRL has one of the best STEM programs for outreach. Assistant Secretary of the Navy for Research, Development and Acquisition Sean Stackley asked Rear Adm. Nevin Carr, the Chief of Naval Research, to be the STEM coordinator for the U.S. Navy. Rear Adm. Carr and I talk on a daily basis, and he sees our program as a model program as well.

We start at a very young age. We go out and lecture at schools, and our scientists participate at all of the local schools. When I look across our workforce, about 3,200 employees at the laboratory worldwide, all of those people are very passionate about science. They are very passionate about the mission of the laboratory and what science can produce. You simply have to look at the history of the lab to realize the wonderful work. When those people do outreach, whether they are scoutmasters, or assistant teachers, or they are just visiting schools, they influence a lot of kids, from age four all the way up. That type of outreach is very important. We judge at science fairs. We work at middle schools, high schools, and there is a lot of local outreach in the Washington, D.C., area to some of the less privileged schools. We have career programs where we bring students on, and they will work as technicians in a laboratory. They are doing real work in a lab, and are mentored by some of the best scientists in our country.

Maybe, if we as Americans are fortunate, that seed will be planted in their mind, and students will realize the wonder and beauty and future and the excitement of discovery and invention. There are a lot of examples across the lab of young people that got their start here 20, 30 or 40 years ago in high school, or maybe in college.

Mentoring is a person to person exchange, and we have lots of wonderful scientists here that realize what a key issue this is for our laboratory. We are very concerned when we look at our graduate school population, and estimates are that 50 to 60 percent of the graduate students in U.S. schools are foreign nationals. That doesn t help me here at the lab because you have to be a U.S. citizen, and you need to hold a secret clearance to work here. There are a lot of foreign national young adults that come here, are mentored, and eventually become a U.S. citizen and work here. That is a good news story. We wish that more of our foreign national graduate students stayed in our country and realized the opportunities here.

STEM [outreach] is a big priority for the Navy, and at the NRL, we have the model program inside the Navy for that outreach with a workforce to support it. CHIPS

For more information about NRL student and postdoctoral programs visit: www.nrl.navy.mil/accept-the challenge/students-postdocs/. For information about other student programs, go to: www.nrl.navy.mil/accept-the challenge/students postdocs/student-programs/.

Website Question Leads to a Strengthened Privacy Process

By Steve Muck

A question submitted to the "Ask an Expert" section of the Department of the Navy Chief Information Officer website underscores the need to improve business processes that involve the use of a Social Security number. While there are many legitimate requirements for SSN use, efforts must be made to reduce or eliminate reliance on this unique personal identifier. After reading the question and the DON CIO's response, consider if there are practices in your organization where a careful review of SSN use is necessary.

Question:

"Recently, a Department of the Navy employee solicited me via email regarding post Navy career opportunities. I am transitioning from the naval service next month. Without my prior approval or knowledge, the DON employee emailed me a For Official Use Only (FOUO) document containing my full SSN and date of birth to my personal/civilian email account.

I am frustrated by the lack of common sense this shipmate displayed. What if he/she had been one character off in typing my personal email address? What if my info ended up in someone else's inbox that had no need to see my personal information? We're all trained in personally identifiable information (PII), aren't we?

Bottom line: I'd like to know what the Navy's policy is regarding transmission of PII via email. For example, I have noticed a change in orders writing: no more full SSNs in message traffic or truncated SSNs posted to a public facing website. Does the same apply to other documents? Did this DON employee violate procedure when he/she sent me a FOUO document containing my PII to my personal email account? If there was a violation, how do I go about reporting this individual?

R/
-LT XXX"

Response:

"Dear LT,

Thank you for contacting the Department of the Navy Chief Information Officer. Your feedback is important to us.

We are contacting the privacy officer at the command where this occurred to look into this practice. To answer your specific question about emailing sensitive PII: DON policy states that all email containing sensitive information, including PII, must be digitally signed and encrypted. New (still in draft) policy will require that any use of the SSN must be justified by applying one of 13 authorized uses of the SSN. The email you received would have to be justified using this same process.

As an FYI, the draft policy will require most Navy business practices to use the DoD ID number: Electronic Data Interchange Personal Identifier (EDIPI) number in place of the SSN. The DoD ID/EDIPI is a unique number assigned to each person in the DEERS (Defense Enrollment Eligibility Reporting System) database and does not have any commercial application.

Best regards,
The DON CIO Privacy Office"

Although the incident the lieutenant described is not standard practice according to the responsible office, officials stated that they will strengthen PII handling procedures, such as enforcing the use of the Privacy Act Statement and ensuring documents containing PII are properly marked. They will justify the continued use of the SSN in business processes to prevent a repeat occurrence. Protecting the personally identifiable information of DON personnel is of the utmost importance to Under Secretary of the Navy Robert O. Work, who made significant reduction of PII breaches a priority in the Department of the Navy. Frequent reviews of how SSNs and other PII are used by your command are an important way to ensure that such information is used only when necessary and that the proper steps are taken when handling this information. Such efforts will help the department move closer to achieving the Under Secretary's goal. CHIPS

Steve Muck is the privacy lead for the Department of the Navy Chief Information Officer.

NRL RDT&E Protecting Ships and Crew

Interview with John P. Farley
Director for ex-USS Shadwell test operations

The Naval Research Lab's Technology Center for Safety and Survivability develops and tests cutting-edge technologies that involve combustion dynamics modeling, fire extinguishing agent development, fuel analytics, firefighting doctrine development and more. The center operates two specialized fire research facilities that include the Chesapeake Bay Fire Test Detachment (CBD) located in Chesapeake Beach, Md., and the full-scale fire test ship, the decommissioned ex-USS Shadwell (LSD 15) located in Mobile Bay, Ala. The ex-USS Shadwell is regularly set ablaze in a controlled environment to advance the safety of operational Navy and civilian shipboard firefighting.

Every Sailor is a firefighter first, and a large portion of basic training is dedicated to firefighting, damage control and prevention tactics because a fire aboard ship can be catastrophic for the ship and crew. The Navy is continuously researching and developing new technologies to protect the fleet and Sailors.

John P. Farley, director for Shadwell/CBD test operations, discussed NRL's research, development, test and evaluation efforts in improved firefighting technologies in a written response to questions in May.

CHIPS: The development of aqueous film-forming foam in the 1960s by NRL benefited the Navy, and it is now used in many civilian settings. What are the unique properties of AFFF?

Farley: As the name implies, AFFF enables the formation of an extremely thin layer of water, a few tenths of a millimeter, to form between the liquid fuel and the foam blanket. This aqueous film barrier helps to prevent the fuel vapor and oxygen from mixing, which is needed to support combustion.

Of course the question then becomes: how does one get a water film to float on a liquid hydrocarbon fuel surface? This feat is achieved due to the key ingredient of AFFF, which is a fluorinated surfactant. The fluorinated surfactant lowers the surface tension property of the water and enables, as the water drains from the foam, the formation of the aqueous film that floats on top of the liquid fuel surface.

Because of the superior fire extinguishing performance capabilities of MILSPEC (military specification) AFFF, it has become the agent of choice whenever there is a Class B (flammable liquid) hazard present both in the military and the commercial sector. The next time that you see a vehicle fire, a train derailment [or] refinery fire on the news, or traveling through an airport both here and abroad, you can be self-assured that MILSPEC AFFF is on the scene.

CHIPS: NRL research resulted in advances in shipboard firefighting using high expansion (HiEx) foam systems. How will HiEx systems change firefighting on Navy ships?

Farley: A high expansion foam system utilizes a series of fixed foam generators that are generally located high in the compartment. A nozzle within the generator sprays a foam solution against a screen which then forms foam bubbles that flow into the protected compartment. In some respects this is the same principle used when a child generates bubbles with a handheld wand. The advantage of a HiEx foam system over a conventional overhead sprinkler system is that the foam generated is 3-D capable; that is, it expands to fill a large volume in minutes, flowing around any obstructions enabling complete extinguishment of a fire that is independent of the type of fuel load present.

These noted advantages are particularly important to the Navy when considering the type of fuel loads that may be present in large volume mission critical spaces, such as a hangar bay, well deck, or vehicle storage areas. A large uncontained fire in one of these types of spaces could quickly lead to a ship conflagration, which could directly impact the ship's warfighting capability.

A HiEx foam system provides a 'quick response' solution that will not need a manual firefighting back-up response that is typically required for a ship fitted with conventional overhead sprinklers. This fact in itself is important because a rapidly growing fire in a large volume, highly cluttered space would pose sig-

1. The ex-USS Shadwell, a decommissioned U.S. Navy ship, serves as the Navy's full-scale damage control research, development, test and evaluation platform. Moored in Mobile Bay, Ala., the ex-USS Shadwell is regularly set ablaze in a controlled environment to further advance the safety of operational Navy and civilian shipboard firefighting measures.

2. High Expansion (HiEx) foam protects large volume mission-critical spaces. In shipboard firefighting applications, HiEx foam expands to fill up the volume of flammable spaces in minutes, flowing around obstructions that previously mandated manual firefighting. NRL researchers conduct HiEx foam tests aboard the ex-USS Shadwell.

3. A controlled fire in the well deck of ex-USS Shadwell.

nificant manual firefighting challenges even for a seasoned professional firefighter.

CHIPS: Long before the mandate in 1987 (Montreal Protocol on Substances that Deplete the Ozone Layer) to halt production of halons by 1994, NRL began research into halon replacement. What are some of the halon-free fire protection options that NRL transitioned?

Farley: In the fire protection community, we typically note halon substitute technologies as either replacement options or alternatives. Replacement options include gaseous agents. For the most part these replacement agents are halogenated hydrocarbons that have low ozone depletion potential (ODP). The NRL proposed Halon 1301 (CF3Br) replacement was heptafluoropropane HFC-227ea (CF3CHFCF3), which the Navy calls HFP. HFP is currently used for engine enclosures or flammable liquid storeroom applications. For halon alternatives, NRL recommended the use of water mist and self-contained aerosol generator technologies.

Water mist systems create a fine mist of water droplets, allowing the use of smaller quantities of water than conventional sprinkler systems. Due to their ability to quickly absorb heat, the water mist systems are found to be very effective for machinery space applications. Water mist systems are now employed on the LPD 17 class (amphibious transport dock ship), LHD 8 (amphibious assault ship), LCS (Littoral Combat Ship), the DDG 1000 (destroyer) and the U.S. Coast Guard National Security Cutter. Aerosol generators on the other hand distribute micron-sized dry chemicals that interrupt the chemical chain reaction of a fire. Aerosol generator technologies have been found to be very effective for those applications where a low weight and low cost alternative is paramount to the fire protection design.

CHIPS: The Navy is developing a new vessel, the Ship-to-Shore Connector, to replace the landing craft air cushion. Can you talk about the firefighting systems on the SSC vessel?

Farley: The SSC fire protection design was particularly challenging because the SSC design, like the existing LCAC, is extremely weight critical, and the operating parameters include the need for a fire protection strategy that can operate in a temperature range of 10 to 200 degrees Fahrenheit. It was determined that the aerosol generators were the best Halon 1301 alternative system for the SSC gas turbine engine enclosures, auxiliary power units and fuel bay. The aerosol units enabled a 70 percent reduction in weight, were inexpensive, and also enabled a maintenance-free solution since the aerosol generators have a 10-year shelf life.

For the SSC Cargo Deck, the best Halon 1211 alternative turned out to be a 150-pound monoammonium phosphate dry chemical ABC extinguisher. [An ABC fire extinguisher can be used on three different kinds of fires: Class A (ordinary combustibles such as wood or paper), Class B (flammable liquid fires such as grease or gasoline) or Class C (electrical fires)].

It should also be mentioned that the successes of the SSC Halon alternative program led directly to transitioning of the aerosol generator technology to the U.S. Navy Landing Craft Utility for diesel engine room and flammable liquid storeroom protection. There is also considerable interest in the aerosol generator technology by the U.S. Coast Guard for potential use on the new National Security Cutter and Utility Barge application.

Corrosion Science & Engineering

Interview with Edward Lemieux
Director, Center for Corrosion Science & Engineering, Chemistry Division, Naval Research Laboratory

One of the the most insidious threats the U.S. Navy faces is a foe whose name you probably could not guess because it is so mundane and unexpected. The threat is rust, and other corrosives, which gobble up $3 billion of the fleet maintenance budget each year. But the Navy has an able defender, the Naval Research Laboratory Center for Corrosion Science and Engineering, which conducts broad scientific and engineering programs to reduce the effects of the marine environment on naval systems.

With a goal to increase understanding of corrosion mechanisms through the study of passive films and their breakdown, the CCSE performs investigations of surface properties, chloride and metal oxides to provide a theoretical understanding of corrosion to develop the foundation for corrosion control systems.

The corrosion engineering section operates the Marine Corrosion Facility in Key West, Fla., which provides engineering solutions to Navy corrosion control problems. Specific expertise in cathodic protection systems, alloy exposure and testing, seawater system corrosion and fouling control, and aquatic nuisance species test and evaluation are maintained.

The marine coatings section operates as part of the lab in Key West and partly in Washington D.C., with a focus on the evaluation of shipboard coatings and development of new resin technology. Investigation of the properties of coatings that meet environmental restrictions on volatile organic compounds and hazardous air pollutants are continuing. Single coat systems, high solid epoxies, edge retentive tank coatings, camouflage and nonskid coatings are initiatives to combat corrosion and extend fleet service life.

The Marine Corrosion Facility plays an important role in providing technical expertise to Naval Sea Systems Command and supports the command directly as a designated engineering authority (EA) for the Navy Materials/Corrosion/Coatings/Environmental Technical Authority. The facility is additionally designated by NAVSEA as the cathodic protection design agent for Navy ships and serves as EA in the areas of cathodic protection, environmental effects and marine coatings systems.

Edward Lemieux, director for the center for corrosion science and engineering, in NRL's chemistry division, provided a written response to questions about his work in May.

CHIPS: The characteristics of siloxane nonskid coating make it much more cost efficient than traditional surfaces for use on Navy ship decks. Can you explain how SiloxoGrip was developed?

Lemieux: The SiloxoGrip system was developed as part of an ONR (Office of Naval Research) Future Naval Capabilities (FNC) program for maintenance reduction technologies for which NRL is the principle investigator. Product development began in January 2009.

Several refinements have been made resulting in the first shipboard demonstration in May 2010. Five subsequent demonstrations were completed by the end of September 2010. Transition [to

Combating one of the U.S. Navy's oldest enemies through science and research…

the fleet] is expected to take place within the next fiscal year.

CHIPS: What are the characteristics of the SiloxoGrip that make it most valuable in the maritime environment?

Lemieux: All ships in the fleet coat interior and exterior deck surfaces with aromatic epoxy-based nonskid coatings which last 12 to 36 months and generally fail due to amine blush, corrosion, wear and weathering. The annual replacement cost exceeds $4 million per ship.

NRL's Center for Corrosion Science and Engineering developed new organo-siloxane-based nonskid coatings suitable for all deck surfaces, which exhibit increased exterior durability and color retention, along with direct-to-metal adhesion. With the improved performance, the NRL organo-siloxane is anticipated to provide a 60-month operational cycle, prior to replacement. The NRL nonskid coating has been demonstrated in the past year on USS Ponce (LPD 15), USS Ramage (DDG 61), USS Oak Hill (LSD 51), USS Whidbey Island (LSD 41), USS Cole (DDG 67) and the USS Mason (DDG 87) and has shown dramatic performance improvement against standard qualified Navy nonskids.

CHIPS: What about solvent-free rapid-cure coatings developed for ship structures, such as fresh water tanks?

Lemieux: Based on the fiscal year 2007 Cost of Corrosion Study, sponsored by the Office of the Secretary of Defense, the Navy spends an estimated $3.2 billion on corrosion costs for Navy ships. The top cost drivers for Navy ships, based on the study, were painting, dry-docking and ballast tanks. Due to this and the time-consuming, tedious, and labor-intensive characteristics of the legacy three-coat system for ship tank application, researchers at the NRL developed a high-solids, rapid-cure, single coat paint system.

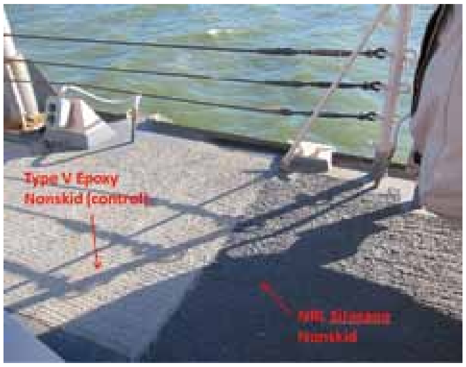
Currently, it is evident that this advance in technology has revolutionized maintenance, sustainability, and overall value of the Navy ship force. The research began under the single coat program, a Future Naval Capability program, sponsored by the Office of Naval Research. The goal of the program is to reduce maintenance time and provide cost savings by introducing rapid-cure coatings technology to the fleet.

In 2009, Naval Sea Systems Command officials mandated that all seawater ballast tanks on submarines, surface ships and aircraft carriers in service be required to utilize rapid-cure, single coat paint. Advantages of the new coating include: reduced coating application process time due to rapid cure (in minutes, not hours or days as with other systems); one coat application capability dramatically reducing the coatings system process bottleneck; reduced life cycle cost due to excellent adhesion; high impact resistance and high chemical resistance improving the coatings service life in harsh outdoor, chemical and marine environments; and environmental compatibility with solvent free, (volatile organic compound) VOC-free, and odor free coatings that ensure environmental compliance in many uses.

The potential fleetwide cost savings over the coatings' expected 20-year life cycle is $1.8 billion. The estimated savings from installing rapid cure coatings on all Navy seawater ballast tanks via a single coat process is $14 million over the next five years. In addition, it is expected that the time required for painting will be cut in half, which will conserve precious depot time for other work.

In FY10, the rapid-cure, single coat initiative was fully implemented fleetwide, in all fuel tanks, sewerage tanks and oil waste tanks. The projected savings in repair and maintenance cost avoidance is $125,000 per Los Angeles-class submarine major availability and $433,000 per aircraft carrier major availability. This technology is being extended for use in potable water tanks, well deck overheads and as primer systems for topside coatings systems.

CHIPS: Are there other game-changers that will lead to energy and cost efficiencies?



Comparison of siloxane nonskid coating with traditional aromatic epoxy-based nonskid coating aboard USS Mason (DDG 87). NRL is testing siloxane treated deck surfaces aboard several ships. It demonstrates increased exterior durability and color retention, along with direct-to-metal adhesion. With the improved performance, the NRL organo-siloxane is anticipated to provide a 60-month operational cycle, prior to replacement. Organo-siloxane is also more reflective, which reduces solar absorption.

Lemieux: There are several key corrosion prevention efforts underway, in addition to the nonskid efforts identified above. NRL is leading the development and transition of the next generation topside Navy 'haze gray' coatings systems and cavitation resistant rudder coatings within an ONR FNC program.

New coating systems, which are color matched and color stable, together with [the] ultra-high solids primer system will provide an excellent corrosion barrier with significantly increased weathering resistant topcoats based on polysiloxane and fluoropolyurethane chemistries. These include both NRL formulations and commercial products.

These systems are being demonstrated in the fleet. NRL also modified a conventional cast in place of the polyurethane system to allow for spray applications for U.S. Navy rudders. These systems exhibit excellent cavitation and cathodic disbondment resistance, making them good candidates for improved rudder coatings. The first shipboard application is planned in FY12. CHIPS

Contact NRL's public affairs office at (202) 767-2541 or info@pao.nrl.navy.mil.

NRL Websites:

The Navy Technology Center for Safety and Survivability: www.nrl.navy.mil/chemistry/6180/index.php.

Center for Corrosion Science & Engineering: www.nrl.navy.mil/chemistry/6130/.

DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

5 May 2011

MEMORANDUM FOR DISTRIBUTION

Subj: DEPARTMENT OF THE NAVY (DON) INFORMATION MANAGEMENT/INFORMATION TECHNOLOGY/CYBERSPACE CAMPAIGN PLAN FOR FISCAL YEARS 2011-2013

Ref: (a) UNSECNAV memo of December 3, 2010, Subj: Department of the Navy (DON) Information Technology (IT)/ Cyberspace Efficiency Initiatives and Realignment
(b) DON CIO memo of December 20, 2010, Subj: Department of the Navy (DON) Information Technology (IT)/ Cyberspace Efficiency Initiatives and Realignment Tasking

Encl: (1) DON IM/IT/Cyberspace Campaign Plan FY 2011-2013

Fiscal realities in the Defense community today and in the anticipated future will not support our continued development and delivery of Information Management (IM), Information Technology (IT) and Information Resources Management (IRM) capabilities as we have in the past. References (a) and (b) direct the DON to leverage Department of Defense IT consolidation efforts and make DON IM/IT/Cyberspace and IRM more efficient. Consequently, we are undertaking several information environment initiatives.

The enclosed plan outlines our IM/IT/Cyberspace and IRM priorities for the next 24 months. We recognize that some of the goals may be difficult to achieve, but they are the right set of initiatives to move us in the direction we need to go. And while we will spare no effort to accomplish our aims, we will retain the flexibility to respond to emerging challenges and opportunities. Therefore, the plan is a living document, which will incorporate feedback and updates as necessary. As we implement the planned initiatives, decisions will be grounded in the following concepts:

- An Enterprise approach;
- Centralized and consolidated efforts;
- Maximized security;
- Protected Personally Identifiable Information; and
- Effective and cost-efficient implementation.

The plan's effectiveness will be measured by metrics derived from key performance indicators (KPI) that will be routinely reviewed by the DON Information Enterprise Governance Board. Trend analyses will inform Program Objective Memorandum development and provide leadership the visibility to assess IT investments and adjust resources.

The plan is intended to support the DON, Sailors and Marines, and their mission partners conducting global military and business operations. We will continue to build and strengthen our collaborative efforts as we execute the plan.

Terry A. Halvorsen

DON IM/IT/Cyberspace Campaign Plan for FY2011-2013
"Be Enterprise, Be Effective, and Be Efficient"

Vision

Secure, relevant, accessible information provided in an Effective and efficient manner throughout the Naval Enterprise.

Mission

Provide Effective/efficient, trusted and shared IM/IT/Cyberspace and Information Resources Management (IRM) enterprise capabilities to support the DON, Marines, Sailors, and their mission partners conducting global military and business operations.

Goals

Goal 1	Goal 2	Goal 3	Goal 4
Sustain an operationally Effective, integrated, secure, and efficient IM/IT/Cyberspace and IRM capability.	Ensure protection of sensitive information, including personally identifiable information, and timely access to trusted authoritative information to enable Effective decision making and mission support.	Attract, develop and retain a highly competent IM/IT/Cyberspace and IRM Total Force.	Ensure all IM/IT/Cyberspace and IRM investments are Effective, efficient, planned, aligned, and acquired to support DON enterprise strategies.

Initiatives

Goal 1	Goal 2	Goal 3	Goal 4
Implement Naval IT Portfolio Management across the mission areas. Conduct deliberate consolidation of DON data centers. Implement DON-wide IT asset management process.	Develop and implement Naval enterprise data and information plans. Develop and implement Naval portal consolidation plans. Ensure authorized data sources are contained within the DON Enterprise Architecture. Optimize the DON Knowledge Management Plan. Revise IRM policy and procedures.	Promulgate Cyber/IT Workforce Communication Plan. Develop Cyber/IT Workforce Development Strategy. Revise and promulgate Information Assurance Workforce Improvement Guidance. Implement Cyber/IT Civilian Workforce Community Management Plan.	Establish process for visibility of all Naval IT expenditures. Develop standards and common criteria for capital planning and investment review. Mandate a common business case analysis process. Implement DON processes to evaluate and approve enterprise software licenses. Develop and use a strategic sourcing process for IT hardware, software, and services.

Key Performance Indicators (KPIs)

Goal 1	Goal 2	Goal 3	Goal 4
Assessment of the ability to provide current, relevant, and reliable information via protected, trusted and net-centric data sharing solutions. Assessment of how the DON acquires and manages IT according to federal mandates, to include environmentally responsible and resource efficient approaches. Assessment of the recommended actions and decisions of DON IT governance boards.	Assessment of community-based efforts that are used to provide information sharing capabilities and services. Assessment of the ability to securely access information and services.	Assessment of accession and separation trends relative to meeting workforce needs in the future. Improvement in IA workforce levels relative to targets by role and certifications. Improvements in levels of education, training and certifications, relative to defined targets. Use of IT workforce recognition programs across the DON.	Assessment of the completeness and accuracy of IT investment data associated, maintained, and available to support enterprise decisions. Assessment of the DON Enterprise Architecture to inform and guide investment decisions. Assessment of the rapid deployment of IT capabilities.

Performance Metrics[1]

Goal 1	Goal 2	Goal 3	Goal 4
Percent of DON systems compliant with FISMA standards (e.g., ATO/IATO, security testing and contingency plan testing). Percent of DON systems with Host Based Security System deployed. Percent of IT expenditures compliant with DON Enterprise Architecture. Percent of legacy networks reduced and returned value to the Information Enterprise. Percent of data center consolidation and degree of improved Effectiveness and savings to the DON. Percent of applications reduced and extent of network operational and security improvement.	Percent of systems that completed Privacy Impact Assessments. Analyze changes in the number of authorized data sources in the DON Enterprise Architecture. Number and type of critical incidents affecting network health.	Percent of certified and qualified personnel in the Cybersecurity/IA workforce. Percent of required training completed. Percent of workforce transitioned to competency-based recruitment, development and promotion.	Reduction of cost of licenses and savings to the DON. Improved Effectiveness in network operations and security resulting from enterprise agreements. Improvements in Programs of Record (POR), to include cost reductions as a result of enterprise agreements.

[1] The DON IT Efficiency IPTs will reference the goals herein, and on a continuous basis, inform and recommend refinements to the performance metrics.

NAVY INFORMATION PROFESSIONALS SUPPORT OPERATION TOMODACHI

U.S. military commands and agencies work bilaterally with Japan to assist after devastating triple disasters

By Capt. Craig Goodman, Capt. Carlene Wilson, Cmdr. Jeffrey Buss and Lt. Ryan Tashma

Imagine a 9.0-magnitude undersea megathrust earthquake, one of the five largest ever recorded, followed by a 128-foot tsunami that traveled up to six miles inland, followed by a level 7 nuclear accident, in one 24-hour period. On March 11, 2011, that is precisely what happened on the northern shore of Japan's Honshu Island, leaving an estimated 4.4 million people without electricity and 1.4 million without water.

In response, U.S. forces in the Pacific immediately began to organize. U.S. Pacific Command activated elements of Joint Task Force (JTF) 519 to augment staff from U.S. Forces Japan (USFJ) forming the Joint Support Force (JSF) headquarters at Yokota Air Base, located west of Tokyo, and 175 miles south of the Fukushima Daiichi nuclear power plant. Within hours of the event, PACOM ordered the launch of Operation Tomodachi to provide humanitarian assistance/disaster relief (HA/DR), foreign consequence management (FCM), and military assistance with the voluntary authorized departure of U.S. military family members in the affected area.

Navy information professionals from across the Pacific answered the call, including IPs from U.S. Pacific Fleet, 7th Fleet, Task Force 76, Task Force 70, Naval Forces Japan, and Naval Computer and Telecommunications Station Far East, by forming a core team that led the way in providing assistance to Japan.

The sheer magnitude and scope of the crisis brought together a host of challenges not typically seen in operations U.S. forces responded to in the past. The joint force was faced with unique communications challenges from the start, specifically in transmission, communications control, information management, interoperability and joint and bilateral information sharing.

Infrastructure

Major portions of the Global Information Grid were disrupted due to damage from the earthquake. Defense Information Systems Agency Pacific, along with DISA Japan Field Office, rapidly identified and reported damage and did an absolutely incredible job of restoring critical bandwidth in record time. Within two days, DISA restored most of the terrestrial connectivity via alternate routing, contracting new services, and repairing fiber-optic cables. Without this core infrastructure, the operation would have never gotten off the ground.

Rapid Growth

U.S. Forces Japan headquarters, at Yokota Air Base, became the nucleus for U.S. operations. Prior to the disasters, USFJ had a staff of 180 personnel, but within days personnel began to converge to support operations, including military and civilian personnel from every service; personnel from the U.S. Agency for International Development (USAID)/U.S. Office of Foreign Disaster Assistance; Nuclear Regulatory Commission; USAID's Disaster Assistance Response Team; Department of Energy; and various other government and non-governmental organizations.

Within two weeks of the disasters, nearly 800 personnel were working from USFJ headquarters. The rapid growth created numerous network infrastructure challenges. The first few days after the disaster were spent transitioning more than 300 SIPRNET and Combined Enterprise Regional Information Exchange System-Japan (CENTRIXS-JPN) clients to the unclassified NIPRNET; expanding the infrastructure to accommodate an increase in users; setting up hundreds of accounts; and working out office space requirements. U.S. Forces Japan J6's command, control, communications and computer (C4) systems branch added more than 500 workstations to its NIPRNET domain in less than two weeks.

Despite massive and swift growth, USFJ maintained a forward-leaning information assurance posture by using operational risk management and daily resource requirement board meetings to assess the IT needs of the command and the most prudent method of satisfying the requirements. The key to the speed of this activity is that USFJ's J6 is the Designated Accrediting Authority (DAA) for USFJ network domains (NIPRNET, SIPRNET and CENTRIXS-JPN), allowing short-cycle time from request to approval and implementation. Had the DAA been at a higher

YOKOTA Air Base, Japan (April 4, 2011) Personnel from the Joint Support Force Japan J6 directorate gather for a group photo. U.S. Navy photo.

echelon, or if the USFJ network were part of a larger enterprise-wide managed network, rapid growth and responsiveness would simply not have been possible.

Additionally, Joint Support Force headquarters was manned with personnel from all the services, which was essential for the rapid growth of communication capabilities for USFJ headquarters, to support air, land and maritime operations. For example, CTF 76 and III Marine Expeditionary Force provided manpower and network equipment to supplement resource shortfalls at USFJ.

YOKOTA Air Base, Japan (April 4, 2011) Members of the Joint Communications Support Element establish self-sufficient working spaces for personnel supporting Operation Tomodachi using the Deployable Joint Command and Control core. DJC2 communications equipment provide a self-sufficient command and control center. Joint communicators developed solutions to provide data transport via terrestrial fiber that enabled an extension of the USFJ headquarters network domain. U.S. Navy photo by Lt. Ryan Tashma.

Need for Assured Access

With an uncertain capacity for the USFJ headquarters infrastructure to accommodate additional personnel and the possibility for rolling blackouts, PACOM's Deployable Joint Command and Control core, based out of Pearl Harbor, Hawaii, was requested. Within 96 hours, DJC2 core equipment and the Joint Communications Support Element (JCSE) team were loaded on two C-17 Globemasters and on the way to Yokota Air Base.

Within 72 hours of arrival, the DJC2 had reached initial operating capability with 56 seats providing NIPRNET, SIPRNET, CENTRIXS-JPN, Voice over Internet Protocol, and secure telephones using commercial and military satellite communications. The deployment proved to be an opportunity for USFJ's J6 staff and the JCSE team to engineer new solutions to meet the changing operational landscape.

While the principal purpose of a DJC2 core is to provide a JTF commander with a self-sufficient command and control center, solutions were developed to provide data transport via terrestrial fiber which enabled an extension of the USFJ headquarters network domain. The right people were present to develop these remedies in the field; however, events highlighted the need for pre-engineered modularity and flexibility for joint communications packages.

Information Sharing

One of the most significant challenges of Operation Tomodachi was the need to rapidly share critical information. While DoD personnel are accustomed to using the SIPRNET, HA/DR operations are typically conducted via unclassified networks which allow access to everyone involved in the relief efforts. Since much of the information produced for Operation Tomodachi was designated "For Official Use Only," access required additional controls. Because most of our partner organizations are not within DoD, they do not have Common Access Cards, or alternate tokens, so a non-CAC-enabled method of sharing was developed.

Within hours of the disasters, PACOM established the "Japan Earthquake 2011" site on the All Partners Access Network. APAN (www.apan.org/) is a PACOM-owned and operated, unclassified network in the public domain that was used in previous PACOM theater HA/DR international operations. APAN is designed to foster collaboration between DoD, U.S. government agencies and NGOs.

For Operation Tomodachi, PACOM created an unlisted, non-advertised APAN group — known as the Virtual Civil Military Operations Center (VCMOC) — accessible only by invitation. Approval was obtained from JSF to post certain controlled, unclassified information to the group, providing a secure path for unclassified information exchange.

In the first two weeks, membership in the VCMOC group grew to more than 500. One of the keys to success was that PACOM flew four of the world's premier APAN experts to JSF headquarters to support local efforts. Their ability to customize a website to support user requirements is remarkable and was critical to sharing information. Though using APAN was a success in many ways, APAN was not the single, authoritative unclassified network in the public domain used for collaboration between government agencies and NGOs. HARMONIEWeb, which is similar to APAN, was also used and preferred by some groups because they were more familiar with HARMONIEWeb features. Because it took valuable time to establish APAN access to the VCMOC, some groups were reluctant to switch to APAN.

HARMONIEWeb (www.harmonieweb.org) is a portal site built for government agencies and NGOs to work together in a collaborative environment to achieve common goals in the areas of HA/DR and stability and reconstruction efforts. Users can request portal sites to meet the collaborative needs of a given situation. Once the site is created, users build the sites, manage access, provide content, and designate their own administrators. HARMONIEWeb is funded by U.S. Joint Forces Command. To more efficiently manage operations, whether it is APAN, HARMONIEWeb, or some other unclassified network, we recommend that only one network be used to keep information centralized and up-to-date.

At the time of the disasters, USFJ's information management/knowledge management plan was a draft concept that had not been exercised. With hundreds of staff members coming from different services and locations, the need for a com-

OSHIMA, Japan (April 4, 2011) Marines assigned to the 31st Marine Expeditionary Unit (31st MEU) pick up debris on Oshima, as part of ongoing disaster relief efforts. Marines and Sailors with the 31st MEU are on Oshima Island to help clear a harbor and assist with cleaning debris from roads and a local school in support of Operation Tomodachi. U.S. Navy photo by Mass Communication Specialist 2nd Class Eva-Marie Ramsaran.

prehensive IM/KM plan became apparent very quickly. But differences in what the IM/KM vision should look like became evident, and with the help of numerous communication experts from every branch of the services, information management standard operating procedures (IMSOP) were developed and approved.

The IMSOP provided clear guidance on how the JSF staff and components should share specific operational products, designated which collaborative tools should be used, and articulated how to post and share information. The end result was a shift from more than 12 varied and often redundant mediums to four common tools, greatly reducing effort and enhancing knowledge transfer.

One issue was how to include users with low bandwidth. Ship personnel had challenges with downloading briefs and accessing Defense Connect Online (https://ww.dco.dod.mil) conferences that were mandated in the IMSOP. To work around this challenge, video teleconferencing, a primary information sharing tool for this operation, was used. However, we found no perfect solution for connecting low-bandwidth users.

Classification

Another challenge involved how to share and classify sensitive information. This took considerable time at the beginning of the operation because boundaries were not clearly defined. In some instances, U.S.-derived information was determined by the United States to be unclassified and FOUO, while the Japanese government determined the same information should be handled more cautiously, for example, information pertaining to radiation levels within Japan, due to the potential for unnecessarily alarming Japanese citizens.

Sharing and disseminating information of this nature required careful and continuous communication and coordination at all levels. A lesson learned is that clear procedures for foreign disclosure, information sharing and posting guidelines should be established early.

Continuity of Operations

From the moment the disasters struck, a continuity of operations plan (COOP) was in development to ensure operations would not be interrupted if the crisis were to escalate. With an estimated 400 aftershocks following the earthquake this was a very real possibility. Just as the aftershocks subsided, the uncertainty regarding the stability of the Fukushima Daiichi nuclear reactors increased, and the possibility of radioactive contamination spreading through air, water, soil, and even food, became a significant factor in planning. COOP development typically considers short- and long-term relocation of personnel to ensure execution of the command's primary mission. However, a standard COOP would not account for the extraordinary threats facing the Joint Support Force. With three major lines of operations, HA/DR, FCM, and the voluntary authorized departure for military family members, ensuring C2 capability was critical. Add in the fact that all the U.S. military bases around Tokyo were potentially at risk, including many critical C4I nodes, and you have a serious situation that required significant thought.

The DJC2 core, while initially envisioned as an asset to expand headquarters capacity, rapidly became the cornerstone for Joint Support Force's COOP planning. It was the only self-sustaining, scalable and mobile command center readily available that could support such an operation.

A complicating factor in COOP development was the unpredictable nature of radiological exposure. Planning was required for sheltering-in-place, potentially combined with execution of a COOP.

Shelter-in-place is a process for taking immediate shelter in a location readily accessible to affected individuals in an emergency by sealing a single area, for example, a room, from outside contaminants and shutting off all heating, ventilating and air conditioning systems. These actions would generally be taken after a chemical accident, civil emergency or terrorist attack. Few, if any, shore facilities plan how to continue extended operations with ventilation completely secured. Accurate communications estimates of supportability were only possible because of heat surveys which were conducted prior to the disasters.

Common Operational Picture

The ability to see the location of U.S. and bilateral forces was critical for both nations. Prior to the disasters, USFJ's common operational picture focused primarily on integrated air and missile defense. Further, USFJ lacked sufficient manning and capabilities to properly manage and maintain the robust and persistent COP capabilities that were required. The formation of JSF brought together the necessary skills and capabilities for an effective operational COP specific for Operation Tomodachi, including operations specialists (COP fusion managers), information systems technicians (Global Command and Control System administrators), and a fleet systems engineering team who brought the COP to life.

YOKOTA Air Base, Japan (March 25, 2011) Adm. Robert Willard, Commander, U.S. Pacific Command, presents his command coin to members of the Joint Support Force Japan J6 directorate in recognition of their efforts during Operation Tomodachi. U.S. Navy photo by Cmdr. Jeffrey Buss.

Keys to collaboration success:

- Pre-existing infrastructure to support a large influx of personnel;
- Strong U.S.-Japan alliance and longstanding bilateral relationship with the Japanese government;
- Communicators from all four services with knowledge of each services' unique capabilities;
- Understanding of the communications infrastructure in the Pacific area of responsibility;
- Local (U.S. Forces Japan) DAA allowing rapid and flexible network changes;
- Prior joint experience within the communications staff;
- Development of an information management SOP early in the operation that facilitated information sharing;
- Quickly determining mission-essential functions, tasks and personnel despite ever-increasing requirements; and
- On-call mobile communications assets.

Websites

APAN – www.apan.org
HARMONIEWeb – www.harmonieweb.org
Joint Support Force – www.usfj.mil/JSF/Index.html
U.S. Forces Japan – www.usfj.mil
U.S. Pacific Command – www.pacom.mil
Yokota Air Base – www.yokota.af.mil

One of the challenges with the COP was trying to meet the demands of different commanders. Each service is accustomed to tracking different components on a COP. For example, a joint force air component commander needs to see air tracks by air tasking order line item, and a joint force land component commander needs to see ground tracks and terrain features.

COP technicians developed a picture by manipulating aircraft Identification Friend or Foe settings to discretely identify aircraft. Friendly Force Trackers were obtained and registered to show the movement of critical ground-based units. The key to success was working with each component commander's operations staff to clearly define what they needed the picture to look like.

Since the main effort of the operation was to support our bilateral partner, U.S. and Japanese planners needed to see the same COP and have a mechanism for transferring data from U.S.-only systems to Japanese compatible systems. This requirement highlighted the criticality of cross-domain solutions, such as the Radiant Mercury system, to move data from SIPRNET to CENTRIXS-JPN.

Outside the Box

COP capability was taken to a new level by working with Google to develop imagery to support the operation. More than 300 highly skilled Web developers from Google headquarters in Tokyo volunteered to help by setting up a site (www.google.com/crisisresponse/japanquake2011.html) that provided a means to identify and locate missing persons. The site included maps and shelter locations, decontamination sites, news, updates on transportation routes and schedules, as well as a way to collect donations. The imagery tools are nothing short of amazing. The ability to zoom in to before and after photos of a specific area was very helpful in JSF's planning efforts (www.sigacts.com/sendai/).

More than 1,000 people volunteered to transcribe the names of missing persons into a people finder website. We highly recommend that this type of coordination be done early in HA/DR operations.

A team from J6, with assistance from Google programmers, added Google Earth to the bilateral COP further enhancing operational capability. When the J6 team visited Google headquarters many people from the disaster-affected areas expressed appreciation to the team for their efforts, with some at the point of tears. The team got the picture very quickly that everyone was working toward the same goal.

Aftermath

In spite of the significant challenges posed by the multiple disasters, Navy Information Professional officers and joint communicators, working together as a team, successfully supported the bilateral command and control of several extraordinarily complex lines of operation. The success of this effort and the lessons learned will continue to pay dividends in the future.

For the most part, Operation Tomodachi and the corresponding communication support have come to an end. However, the Japanese government, for the foreseeable future, will continue to manage the instability of the nuclear reactors and radioactivity levels, and will direct recovery efforts.

The United States will continue to assist Japan as requested by the Japanese government. The IP community, as an integral part of the U.S. forces here in Japan, will provide communication support.

Capt. Craig Goodman is the J6 at U.S. Forces Japan.

Capt. Carlene Wilson is the deputy J6 at Commander U.S. Pacific Fleet and the J6 for JTF 519.

Cmdr. Jeffrey Buss is the assistant chief of staff for C4I/N6 Expeditionary Strike Group 7/Commander, Task Force 76.

Lt. Ryan Tashma is a communications planner on the staff of U.S. Pacific Fleet.

JAPAN'S "3/11" TRIPLE DISASTER

A call for a new lessons learned paradigm for Navy Information Dominance

By Cmdr. Steve Jacobs

The disasters that occurred in Japan March 11, 2011, are nearly beyond imagination. It is doubtful that any exercise scenario could capture the catastrophic implications of a combined earthquake, tsunami and three damaged nuclear reactor cores, and the subsequent international assistance response. U.S. combined operations in support of search and rescue, humanitarian assistance and disaster relief (HA/DR), consequence management, U.S. military assisted voluntary departure of family members and major continuity of operations (COOP) crisis planning and implementation were without precedent.

The combined, complex operations tested all aspects of U.S. Navy, joint and coalition doctrine, command and control, and information sharing. The events present a rare opportunity to refine C2 doctrine, requirements, and tactics, techniques and procedures (TTPs) for very complex, real-world contingency operations. This opportunity should not be lost to study, but rather serve as catalyst to review valuable lessons learned for advancing information dominance. The opportunity should be taken to study why some lessons had to be *relearned* and to transform the Navy and joint lessons learned systems into resolution processes, instead of archives to store past lessons.

Continuous process improvement, capturing lessons and implementing improved information sharing and means of executing C2 under these arduous conditions align with the Chief of Naval Operations' desire to codify processes for leading the future "Implementation of Navy Information Dominance" as described in his letter to "All Navy Admirals and Vice Admirals" of March 20, 2011.

The CNO directs specific actions to advance capability and proficiency in the information domain, and he assigned stakeholder organizations of Navy information dominance to lead and support roles in this task. While the CNO's letter is not specifically related to the Navy's HA/DR efforts in Japan, it clearly addresses the same challenges of lessons relearned. The responsible organizations have now been empowered to focus on deliberate, long-term after action processes.

Operation Tomodachi, meaning "friend" in Japanese, presented lessons collected from the crisis that span all aspects of information exchange processes and information technology implementation. While some obvious observations and recurring lessons learned should lead to immediate improvements in requirements, doctrine or TTPs, such as establishing an operations center with a sufficient number of unclassified computers, many lessons are more nuanced because of the complexity of the operations and will require analysis to decide the best approach for resolution. A good example is the difficulty of delivering information across domains of different classifications.

Many lessons demand a sense of urgency for correction before memories fade or leadership forgets. Often urgency and resolving complex challenges don't go hand-in-hand, especially when exercising fiscal restraint. It is time to refine the lessons learned paradigm into a deliberate and methodical process. This approach could use the existing Joint Lessons Learned Information System (JLLIS), but in a transformative way to improve the entire lessons learned process by determining and addressing root causes of issues and recommending more comprehensive resolution actions.

Lessons learned should then be incorporated into existing training and experimentation venues within the fleet. This will lead to more valuable exercises, experimentation, wargaming, and a new concept of operations (CONOPS) in the information disciplines.

On the information sharing side, there is a set of lessons addressing unclassified collaboration and information sharing needs during Operation Tomodachi. The All Partners Access Network (www.apan.org) is the U.S. Pacific Command owned and operated unclassified collaboration venue for HA/DR planning that allows interagency, joint, coalition and non-governmental organizations participation. However, there was a need for, but a lack of, a comprehensive unclassified common operational picture (COP), which would have provided shared situational awareness of all HA/DR participants for decision makers.

PACOM created an unlisted, non-advertised APAN group, known as the Virtual Civil Military Operations Center (VCMOC), accessible only by invitation. From a military perspective, one limitation of APAN is that unclassified content from military classified systems is not readily portable to APAN and downgrading classified content is not a simple process.

Both of these capabilities would need a defined process for future use because finding a method during a crisis normally makes any success a temporary local solution. Delivering content across classifications with the ability to downgrade classifications readily are processes frequently found in the Navy Lessons Learned Information System (NLLIS).

To ensure APAN use is inculcated into HA/DR processes, joint task force and carrier strike group workups should include APAN accounts and use in an HA/DR scenario. This would include ensuring key staff planners and knowledge managers understand information sharing capabilities and shortfalls. For example, from initial relief efforts, APAN was adopted quickly, but the capabilities of APAN were not well-known by watchstanders due to its minimal use in Japan theater exercises, and little formal standing doctrine, TTPs or CONOPs existed for its usage.

The formal adoption of APAN as the unclassified collaboration tool of choice was also slowed by a shortage of unclassified network workstations in some operational command centers.

When integrating APAN into existing operations centers, capabilities shortfalls were discovered and some solutions were implemented on the fly. The final choice for establishing a COP was the continued use of the secret bilateral Combined Enterprise Regional Information Exchange System-Japan (CENTRIXS-JPN). Thus, the desired unclassified data sharing was not accomplished in an automated system. Refining the use of APAN and the delivery of an unclassified COP capability are recommended and will require significant work by the stakeholders identified in the CNO's March 20 letter to ensure development and integration into future exercises and events on a worldwide basis.

The need to inculcate the lessons of the information technology used in HA/DR operations into training, operations, doctrine and TTPs is a common NLLIS lesson. The Information Dominance Corps should partner with pertinent Navy organizations as part of a future Navy lessons learned process to continually move purchased solutions and installed technologies into the realm of fully delivered information dominance capabilities.

Many Navy information sharing lessons learned from Tomodachi are much more complex at best or even ambiguous at worst. These lessons require analysis to develop more complete response options for future use. One longstanding example is the ad hoc C2 structure of disparate information systems at each echelon when forming new coalitions, JTFs or larger organizational alignments that include interagency entities and NGOs.

After the disasters, a Joint Support Force Japan network was stood up on U.S. Forces Japan systems along with JTF 505 with III Marine Expeditionary Force as the commander. JTF 505 was activated by PACOM to facilitate the orderly processing and departure of American citizens and designated foreign nationals to safe havens. These organizations had to form quickly and then operate in synchronization with their superiors, component commanders and coalition partners.

Synchronization was very difficult when forces operated on different networks at home stations and then deployed to other installations to work on different networks. This situation is nothing new to Navy operators, but advanced study is needed to recommend actions to correct C2 and information system shortcomings, and to avoid relearning this lesson again in the future.

Ultimately, a theater or even overarching Defense Department architecture is recommended based on common and approved standards for joint forces for plug and play operations. It is a known shortcoming in the Far East area of operations that the many service and joint networks and enclaves are sometimes not compatible when applying applications across them. The right attention is needed to recommend consistent and standardized corrective actions.

PACOM is leading the coalition effort for enhancing the interoperability of CENTRIXS enclaves, but much more work is recommended for advancing coalition networking and multilevel security by information dominance stakeholders. Once the technical piece is sorted out, training scenarios should be regularly practiced that include use of the revised architecture and information sharing processes.

Network, software and hardware interoperability requirements are common lessons in the NLLIS and fortunately are getting a great deal of attention with many positive results. This category of lessons will need constant attention in any Navy lessons learned process and in systems acquisition for the foreseeable future.

Another area for serious examination was the need for quick alterations to Navy information assurance policies to keep up with the rapidly changing C2 architecture and multimission nature of Operation Tomodachi. Policies were temporarily modified for use of removable USB hard drives and controlled cryptographic items storage to support COOP planning and implementation.

Public affairs officers and COOP planners quickly required larger email mailboxes and turned to commercial cellular Internet providers for greater capabilities and operational flexibility. Network owners built temporary firewall-protected communities of interest to allow other services to tunnel through networks.

After the dust settles, an examination of how these lessons could be used to develop doctrine and requirements at the operational level should be done. Each change should be understood and considered for a deeper look at IT policies to determine more permanent solutions that are aligned within DoD. While improved technology and training are important to formalize procedures, they alone are not the only answers. Organizational changes and alignments are also recommended to truly improve the lessons learned process.

The volume and complexity of collecting, analyzing and implementing lessons learned in a chain of corrective actions is so great that it should not be the sole responsibility of the commands directly involved in the operations. Lessons learned should be evaluated in the context of the larger joint and interagency effort, which may not be apparent at the unit level.

A well-known weakness in the lessons learned process is that lessons are recorded but often left unresolved. Difficulties with resolution range from unclear responsibility, to lessons that are so complex that they require many diverse organizations and expertise to develop solutions. Other impediments include identifying solutions sets that are repeatable, fundable, measurable and able to be successfully implemented.

A good example from Operation Tomodachi is the difficulties with scheduling and conducting video teleconferences so that all the required organizations could attend. Conducting a VTC in a high OPTEMPO environment when the number of participants and bridge connections are increased above day-to-day operations or exercises is difficult to say the least.

More stress was added to the VTC infrastructure by the constant evolution of the Tomodachi battle rhythm because conference times, configuration and participation were rapidly changing. Establishing a solution requires technical, process and organizational alignments done at a leadership level to ensure resolution since interservice and interagency interoperability gaps are common lessons in NLLIS.

So what does the future of the lessons learned process look like? If one follows the blueprint of the CNO's letter, it appears stakeholders will work as a team but within specific areas of responsibility. The critical density for change would be generated by the singleness of direction from these various organizations. Addressing the details of the numerous lessons learned and recommendations associated with APAN could comprehensively address a single, worldwide "system of systems" HA/DR collaboration solution. CHIPS

Cmdr. Steve Jacobs is an information professional officer and member of the Information Dominance Corps. He is the Commander, Naval Forces Japan assistant chief of staff for C4I and Commander, Navy Region Japan chief information officer.

Next Generation Aircraft

NAVAIR's rapid development of naval air assets

By Holly Quick

This year marks the Centennial of Naval Aviation, a yearlong celebration in which the naval aviation community reflects on the past 100 years and its unrelenting commitment to sustaining a Navy, Marine Corps and Coast Guard that wins wars, protects the homefront and enables peace. During this time of reflection on how the Navy's flight program has grown to become a guardian of freedom for America and its allies, it is also a time to look ahead to the next generation of aircraft in development.

Naval Air Systems Command (NAVAIR), whose priorities include delivering new aircraft, weapons and systems that provide a technological edge over adversaries, presented some of its latest developments at the Sea Air Space 2011 Exposition in April. The featured aircraft —the CH-53K Heavy Lift Helicopter, P-8A Poseidon and MQ-4C BAMS UAS — are all in the development phase with the initial operational capability (IOC) planned between 2013 and 2018. At the Service Chiefs Panel, Vice Adm. David Architzel, NAVAIR Commander, explained, "Over the past year, development of air assets has continued at a pace never seen before."

CH-53K Heavy Lift Helicopter

The program office for H-53 Helos (PMA-261) manages the cradle to grave procurement, development, support, fielding and disposal of the entire family of H-53 helicopters. This includes the CH-53D Sea Stallion, CH-53E Super Stallion, MH-53E Sea Dragon, and the newest development, the CH-53K Heavy Lift Helicopter.

As the U.S. Marine Corps mission changes, so does its aircraft — evidenced by the development of the cargo helicopter CH-53K, the future of heavy lift rotorcraft. CH-53K will provide the assault support function in expeditionary maneuver warfare, significantly improve operational capabilities, and reduce life-cycle costs.

The next generation heavy lift aircraft will offer improved performance in support of future warfighting concepts and the Marine Corps Vision and Strategy 2025.

CH-53K, the follow-on to CH-53E, will maintain virtually the same footprint, but will carry out an unrefueled mission of 110 nautical miles (nm) with a 27,000-pound external payload, nearly doubling the existing payload.

CH-53K will increase the maximum gross weight from 73,000 pounds to 84,700 pounds and will be able to perform in mountainous areas and extremely hot conditions.

Additionally, CH-53K will provide the following increases in performance and capability:

- Four times the lift under hot conditions at 110 nm compared with current heavy lift aircraft;
- Reduction in material maintenance cost;
- Increased survivability; and
- Twenty-three-percent reduction in fuel consumption.

CH-53K will provide the Department of Defense with the best high-altitude capability which is critical to operations in austere high-altitude conditions.

Other features of the CH-53K include: General Electric (GE)-381B engines; advanced drive train; fourth-generation composite rotor blades; fly-by-wire flight

CH-53K Heavy Lift Helicopter

CH-53K

Length
Fuselage: 73.4 feet (22.4 meters)
Rotors turning: 99 feet .5 inches (30.2 meters)
Height: 28 feet 4 inches (.81 meters)
Width
Fuselage: 18 feet (5.5 meters)
Rotor: 79 feet (24.1 meters)
Cabin dimensions
Length: 30 feet (9.2 meters)
Width: 9 feet (2.8 meters)
Height: 6 feet 5 inches (1.9 meters)
Weight
Empty: 43,750 pounds
Max Weight on Wheels: 74,500 pounds (40,000 kilograms)
Internal Load: 30 troops or 24 litter patients plus four attendants or 30,000 pounds (13,636 kilograms) cargo or two 10,000-pound 463L pallets
Max Gross weight w/External load: 88,000 pounds (38,409.1 kilograms)
External Load: Hook rated to 36,000 pounds
Main Rotor diameter: 79 feet (24.1 meters)
Range
Without refueling: 507 nautical miles
With aerial refueling: Indefinite
Endurance: 4 hours (unrefueled)
Ceiling: 18,500 feet
Speed: 195.6 miles per hour (170 knots)
Armament: Three GAU-21 .50 caliber machineguns
Crew: 2 Pilots and 1 to 3 air crew

As the U.S. Marine Corps mission changes, so does its aircraft.

controls; Rockwell Collins glass cockpit; improved external and internal cargo handling systems; and survivability and force protection improvements, allowing it to range the entire battlefield while protecting the crew and occupants from advanced threats.

The CH-53K program passed Milestone B in December 2005, and a contract was awarded in April 2006. To pass Milestone B, the milestone decision authority must, among other things, approve the acquisition strategy, the acquisition strategy program baseline, and the type of contract that will be used to acquire the system.

The program conducted its preliminary design review in September 2008 in which it completed a critical design review for 30 of 70 subsystems, and successfully conducted a full system CDR in July 2010. Major components to aid in airframe test article assembly are being produced. Initial operational capability is planned for 2018. IOC is the phase in the acquisition cycle when a capability is available in its minimum usefully deployable form.

P-8A Poseidon

The Maritime Patrol and Reconnaissance Aircraft Program Office (PMA-290) manages the acquisition, development, support and delivery of the Navy's maritime patrol and reconnaissance aircraft. Its newest development in multimission maritime aircraft, P-8A Poseidon, will replace the P-3C Orion as a long-range anti-submarine warfare (ASW), anti-surface warfare (ASuW), intelligence, surveillance and reconnaissance (ISR) aircraft capable of broad area, maritime and littoral operations.

P-8A Poseidon is the U.S. Navy's persistent, maritime patrol aircraft that will provide superiority in both the open ocean and littoral environments. It will leverage the experience and technology of the P-3C's capabilities and assets to meet the Navy's need for developing and fielding a maritime aircraft equipped with significant growth potential, including an extended global reach, greater payload capacity, higher operating altitude, and an open systems architecture.

P-8A Poseidon will provide more combat capability from a smaller force and less infrastructure while focusing on worldwide responsiveness and interoperability with traditional manned forces and evolving unmanned sensors.

P-8A Poseidon will provide the following capabilities:

- Next generation ASW to counter subsurface threats;
- Detect, locate, identify and track targets in the surface, subsurface and littoral battlespace, and if required, deny, disrupt or destroy;
- Conduct armed ISR in maritime and littoral areas of operation;
- Provide command, control and communications and serve as an interoperable C3 node; and
- Provide accurate stand-off targeting and strike support for naval, joint and multinational operations.

Other state-of-the-art features of the P-8A Poseidon include: International Maritime Satellite communications, sonobuoy launchers, tactical workstations, air refuel receptacles, multimode radar, bomb bay, wing stores, CFM56-7B turbofan engines with 180-kVA integrated drive generators, and an electro-optical/infrared (EO/IR) turret that provides an ever-growing array of co-boresighted video-rate sensors that cover a wide variety of wavebands and fields of view.

In August 2010, the P-8A Poseidon program reached Milestone C and received approval for low-rate initial production. Achieving Milestone C means the program is ready to manufacture production aircraft and begin the process of maturing manufacturing processes and capabilities to support future full-rate production. The Navy plans to purchase 117 production grade P-8A Poseidons, an IOC is planned for 2013.

P-8A Poseidon

Primary Function: Anti-Submarine Warfare (ASW) and Anti-surface Warfare (ASuW), Intelligence, Surveillance and Reconnaissance (ISR)
Propulsion: 2 CFM 56-7B engines with 27,300 lbs thrust each
Length: 129.5 feet (39.47 meters)
Height: 42.1 feet (12.83 meters)
Wingspan: 123.6 feet (37.64 meters)
Maximum Gross Takeoff: 189,200 pounds (85,820 kilograms)
Airspeed: 490 knots (564 mph) true air speed
Ceiling: 41,000 feet (12,496 meters)
Range: 1,200 nautical miles radius with four hours on station
Crew: Nine
Armament: Torpedoes, cruise missiles, bombs, mines

P-8A Poseidon

MQ-4C BAMS UAS

The Persistent Maritime Unmanned Aircraft Systems Program Office (PMA-262) manages the development, production, fielding and sustainment of all persistent maritime unmanned aircraft systems including the MQ-4C Broad Area Maritime Surveillance (BAMS) Unmanned Aircraft System.

The MQ-4C BAMS UAS will be a forward deployed, land-based, autonomously operated system that provides a persistent maritime ISR capability using a multi-sensor mission payload, including: maritime radar; EO/IR; electronic support measures; Automatic Identification System; and basic communications relay. EO/IR sensors classify, identify and geolocate air, sea-surface and ground targets with signal and image processing techniques that operate from the visible through long wave infrared bands. The MQ-4C air vehicle is based upon the U.S. Air Force RQ-4B Global Hawk, while its sensors are based upon components of (or entire systems) already fielded in the DoD inventory.

As an adjunct to the P-8A, the MQ-4C BAMS UAS will provide combat information to operational and tactical users, such as the expeditionary strike group, carrier strike group and the joint forces maritime component commander. The MQ-4C will provide intelligence preparation of the environment by providing a more continuous source of information to maintain the common operational and tactical picture of the maritime battlespace. Additionally, MQ-4C-collected data posted to the Global Information Grid (GIG) will support a variety of intelligence activities and nodes. In a secondary role, the MQ-4C will be used alone or in conjunction with other assets to respond to theater-level operational or national strategic tasking.

MQ-4C BAMS UAS

Primary Function: Persistent Maritime ISR
Propulsion: Rolls-Royce AE3007H
Endurance: >27 hours
Length: 47.6 feet (14.5 meters)
Wingspan: 130.9 feet (39.9 meters)
Height: 15.4 feet (4.7 meters)
Weight: Max design gross take-off: 32,250 pounds (14,628.4 kilograms)
Airspeed: 330 knots (approximately 380 miles per hour)
Ceiling: 56,500 feet (17,220 meters)
Range: 8,200 nautical miles (15,186.4 kilometers), max unrefueled range
Crew: 4 per ground station (Air Vehicle Operator, Tactical Coordinator, 2 Mission Payload Operators)

The Navy acquired two Global Hawk Maritime Demonstration (GHMD) unmanned aircraft in 2006 to be utilized for the development of Navy doctrine and concepts of operations for large persistent unmanned air vehicles. The system has been renamed the Broad Area Maritime Surveillance-Demonstrator (BAMS-D).

The BAMS-D team utilizes the RQ-4A long endurance air vehicle to refine tactics, techniques and procedures for use by persistent UASs in a maritime environment.

When fielded, the MQ-4C BAMS UAS will offer a much larger sensor radius than BAMS-D.

While BAMS-D offers a 45-degree field of view for Synthetic Aperture Radar, Inverse Synthetic Aperture Radar and maritime surveillance, the MQ-4C radar will provide a 360-degree field of view.

MQ-4C BAMS UAS

Other improvements will be made to subsystems, engine efficiency and safety.

- Subsystems improvements include:
  - ✔ Improved environmental cooling system and liquid cooling system.
  - ✔ Upgrade to a 30 kilovolt amps (kVA) generator.
  - ✔ Wing and V-Tail deicing.
  - ✔ AN/ZPY-3 Multi-Function Active Sensor – a 360-degree Active Electronically Scanned Array radar.
  - ✔ AN/DAS-3 EO/IR – 360-degree full motion video capable.
  - ✔ AN/ZLQ-1 Electronic Support Measures – all digital, 360-degree Specific Emitter Identification capable.
- Engine Improvements:
  - ✔ Bleed air engine inlet anti-icing. Bleed air is compressed air taken from within the engine that can be used in different ways, including deicing.
  - ✔ Full Authority Digital Engine Control software changes. FADEC is a system consisting of a digital computer, called an Electronic Engine Controller, and its related accessories that control all aspects of aircraft engine performance.
  - ✔ Additional Built in Test functionality.
  - ✔ Accessory gear box improvements.
- Safety Improvements:
  - ✔ Fire sensing.
  - ✔ Fire containment: resistive materials and fire suppression bottle.
  - ✔ Lightning protection.
  - ✔ Crash recorder.

The MQ-4C BAMS UAS is a DoD acquisition category (ACAT) 1D program that received approval from the Under Secretary of Defense for Acquisition, Technology and Logistics (USD AT&L) to enter the system development and demonstration phase of development April 18, 2008. The MQ-4C BAMS UAS program successfully conducted system functional review in June 2009 and is progressing toward future program milestones utilizing the systems engineering technical review process. SDD delivery is anticipated in 2012 with IOC planned for 2015. CHIPS

Go to www.navair.navy.mil for information about NAVAIR and its many products.

Holly Quick is a contributor to CHIPS and supports the public affairs office of SPAWARSYSCEN Atlantic.

Report Your Breaches

By Michelle Schmith

The privacy of an individual is a fundamental right that must be respected and protected. While improved handling and security measures within the Department of the Navy are noted in recent months, the number of incidents in which loss or compromise of personally identifiable information (PII) occurs remains unacceptably high.

The DON Chief Information Officer Privacy Office evaluates an average of one PII breach report per day in which privacy sensitive information is compromised, lost or stolen. To ensure all DON personnel understand their breach reporting responsibilities, this edition of CHIPS will detail that process rather than publish the recurring "Hold Your Breaches" column.

PII Breach

The Department of Defense (DoD) defines PII as information about an individual that identifies, links, relates, or is unique to, or describes him or her (e.g., a Social Security number; age; military rank; civilian grade; marital status; race; salary; home phone numbers; and other demographic, biometric, personnel, medical and financial information, including any other personal information that is linked or linkable to a specific individual).

A PII breach occurs when there is a loss or suspected loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any situation where people other than authorized users, for other than authorized purposes, have access or potential access to PII. This includes PII on the SIPRNET, which carries the same inherent risks of disclosure if sensitive information is not properly protected.

PII breaches affect all DON personnel, whether military, civilian or support contractor. Eighty percent of all breaches are caused by human error; the majority of breaches involve the loss, theft or compromise of SSNs. And while identity fraud linked to the loss of DON information remains low, the number of PII breaches must be reduced.

Responsibilities

All DON personnel must protect PII so that no one can access sensitive information without a need to know. In addition, all DON personnel must report a loss or suspected loss or compromise of PII to their supervisor or privacy official upon discovery. Finally, commands must designate a person in writing who is responsible for submitting DON breach reports using OPNAV 5211/13: "DON Loss or Compromise of Personally Identifiable Information (PII) Breach Reporting Form" and OPNAV 5211/14: "DON Loss or Compromise of Personally Identifiable Information (PII) After Action Reporting Form."

Actions

Within one hour of discovery of a loss or suspected loss of PII, the designated privacy official must notify proper authorities using OPNAV form 5211/13. The initial report must include a brief description of the incident, including circumstances of the breach, type of information lost or compromised, whether the PII was encrypted, and whether the recipients had a need to know.

Within 24 hours of receipt, the DON CIO will review the initial report and determine, using DoD's Risk Analysis Methodology, the potential risk of harm to affected personnel.

Within 10 days, if required, the designated privacy official must mail notification letters to affected personnel.

And within 30 days of the breach, the designated privacy official, using OPNAV form 5211/14, must send notice to the appropriate authorities of remedial actions taken to prevent recurrence, notification status, lessons learned and disciplinary action taken, where appropriate.

All DON personnel must be aware of their roles and responsibilities related to reporting a known or suspected loss of PII. Compliance will help protect privacy sensitive information when a breach is discovered. Look for new breach reporting forms, which will be released by the DON CIO, in summer 2011. Additional information regarding safeguarding PII is located on the DON CIO website at www.doncio.navy.mil/privacy.

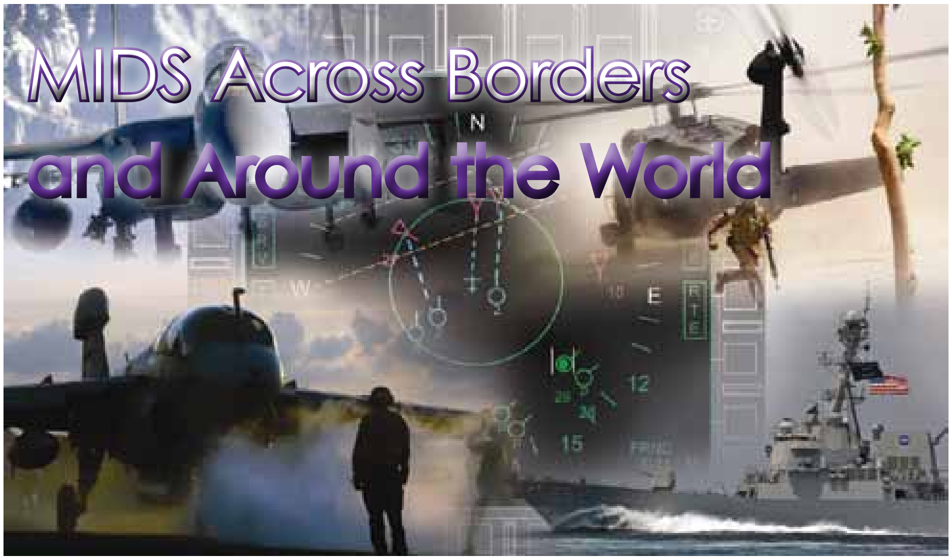
Michelle Schmith is a privacy analyst for the Department of the Navy Chief Information Officer.

Department of the Navy Breach Reporting Process

Responsible Organization	Time Frame	Action	Resources
Discovering Command		Breach discovered	
Discovering Commands	Within one hour	Breach reported to DON CIO and U.S. Computer Emergency Readiness Team	DON CIO Message DTG 291652Z FEB 08; OPNAV Form 5211/13
DON CIO	Within 24 hours	Individual notification determination made; command notified whether individual notifications required	DoD Risk Analysis Methodology
US-CERT		Assign US-CERT number	
DON CIO	Within 48 hours	Forward breach report to the DoD Privacy and Civil Liberties Office	
Accountable Command	Within 10 days	If required, signed letter sent to each affected individual	Sample notification letter
Accountable Command	Within 30 days	After action report sent to DON CIO	OPNAV Form 5211/14

*For all DON PII breach reporting resources visit: **www.doncio.navy.mil/privacy**.*

MIDS Across Borders and Around the World



MIDS-LVT terminals are successfully integrated into a diverse, yet complementary set of platforms, including ships, aircraft, missile defense systems, and national and international command and control agencies. Forty nations and two international organizations possess MIDS-LVTs or have been approved to acquire them.

Today's Soldiers and Marines struggle to gain instant and persistent access to essential situational awareness information, such as enemy and friendly force locations and force disposition. Unfortunately, technology has yet to consistently provide this information, which is a critical tool in the warfighting effort on the ground. In the future, ground force communications will enjoy a generational leap in capability when terrain-flattening man-portable, vehicle-mounted networking radios are fielded. Until then, real-time situational awareness will remain solely within the domains of tactical aircraft operations and strategic command and control.

MIDS Transforms Communications

Airborne operations must constantly distinguish friends from foes throughout the full spectrum of warfare operations, from passive surveillance to the heat of battle. In these situations, warfighters have depended upon the Multifunctional Information Distribution System (MIDS) to give them the information and communication abilities they need to be successful. MIDS is a secure, scalable, modular, wireless and jam-resistant digital information exchange system providing real-time Link 16, tactical air navigation (TACAN), and voice communications to airborne, ground and maritime platforms. MIDS has completely changed the way the warfighter sends and receives data, not just in Iraq and Afghanistan, but also within and between the military forces of many countries around the world.

The MIDS program was established by a multinational program memorandum of understanding signed in 1991. The MIDS program office, located in San Diego, Calif., is part of the Joint Program Executive Office for the Joint Tactical Radio System (JTRS) and is a consortium of five nations — France, Italy, Germany, Spain and the United States.

MIDS entered production with the MIDS Low Volume Terminal (LVT) in 2000. The MIDS-LVT product is built by three vendors: ViaSat and Data Link Solutions in the United States and EuroMIDS in Europe. The program's mission is to develop, field and support interoperable, affordable and secure MIDS tactical data link and programmable networking technologies and capabilities for the joint, coalition and international warfighter.

To that end, MIDS-LVT terminals are successfully integrated into a diverse, yet complementary set of platforms, including ships, aircraft, missile defense systems, and national and international command and control agencies. Forty nations and two international organizations possess MIDS-LVTs or have been approved to acquire them.

The MIDS program office is working hard to field the "form, fit, function" upgrade to MIDS-LVT known as the MIDS JTRS. The MIDS JTRS terminal is a software defined networking terminal equipped with all MIDS-LVT capabilities, plus three growth channels into which qualified waveforms can be installed. This will allow capability expansion beyond Link 16, to create even greater connectivity and communication among its operators. MIDS JTRS can also be used as a replacement for MIDS-LVT with only minor host platform modifications.

MIDS JTRS development began in 2004 and to date has successfully completed F/A-18E/F platform integration, F/A-18E/F developmental test, attained National Security Agency certification with the Link 16 waveform, and completed initial operational test and evaluation (IOT&E). Additionally, MIDS JTRS developmental test flight activities with E-8C Joint STARS are ongoing.

MIDS JTRS is in production with a limited production lot awarded in March 2010 and a second limited production lot awarded in February 2011. During MIDS JTRS initial operational test and evaluation with F/A-18E/F, some deficiencies within the MIDS JTRS system were discovered. Uncovering deficiencies in IOT&E is not uncommon, and the MIDS program office quickly conducted root cause analysis on the terminals and the system as installed in the F/A-18E/F.

A team of engineers from government and industry isolated every anomaly and simultaneously developed a verification of the correction of deficiencies (VCD) lab and flight test plan. VCD flight test events will be conducted beginning in July 2011 with the goal of attaining initial operational capability (IOC) by October 2011.

MIDS — a Worldwide Success

The MIDS program's success is clearly demonstrated by the large number of countries and platforms procuring and using MIDS-LVTs. As of late 2010, there were more than 7,600 terminals delivered, or on contract, worldwide. The most significant reason for this success is that the MIDS-LVT provides reliable, advanced, real-time communication capabilities at an affordable cost. Its tactical data link capabilities enhance situational awareness in the battlespace and enable the warfighter to cooperatively engage multiple hostile targets, and monitor those suspected of being hostile, while simultaneously avoiding the fratricide that can be caused by poorly communicated missions.

Another reason for the success of MIDS-LVT is its versatility. This versatility not only refers to the number of platforms into which the terminals are incorporated, but also to their operational usage. MIDS-LVT allows U.S. collaboration in both peacetime and wartime operations with allied partners. For example, the advanced communication that MIDS provides has been used in combat operations in Iraq, the Balkans and Afghanistan. It was especially useful in Afghanistan, where the absolute paucity of a pre-existing air traffic control system suitable for tactical air operations made coordinating aerial attacks, defenses and logistics very challenging.

MIDS-LVT provides a solution to language barriers between allies and coalition partners because the tactical data link technology makes it possible for those who do not share a common spoken language to share a common operational language.

With the original introduction of MIDS-LVT in 2000, U.S. and coalition aircraft were able to join a real-time battlespace command and control system that helped them better organize and carry out their missions. The MIDS Assistant Program Manager for Foreign Military Sales, Steve Kolbert, summarized the advancement, "This was the first time the warfighter got a real-time picture of what was going on in the air, and that's huge."

MIDS-LVT use is not limited to active war zones. NATO is incorporating MIDS-LVT into a unique system designed to connect the allies across the entire European continent. The program, Air Command and Control System (ACCS), will allow NATO members to integrate air traffic control, surveillance, air mission control, airspace management, and force management functions.

The goal is to provide a unified air command and control system, enabling NATO's European nations (including new alliance members) to seamlessly manage all types of air operations over their territory and beyond. The end result will be an airborne tactical network that is unprecedented in size and scope. This increased communication ability will be a major boost to allied defensive efforts and operational coordination.

MIDS-LVT can also be used to coordinate actions in crisis areas around the world. Such areas may include nations experiencing humanitarian or natural disasters, political unrest, or military tensions. In these instances, it is often the case that multiple outside parties will orchestrate a joint effort to send aid or to prevent tensions from worsening. This type of coordination can be problematic if the participants do not speak the same language. MIDS-LVT provides a solution to this language barrier because the tactical data link technology, as the MIDS Program Office Director of Operations, Michael Posner, explained, makes it possible for those who do not share a common spoken language to share a common operational language.

MIDS in Tactical Aircraft

This is a very exciting time for the MIDS program office. As MIDS-LVT use continues to expand and MIDS JTRS continues to reach critical milestones, the MIDS program office is looking toward the future. All MIDS-LVTs are planned to undergo a major upgrade, known as Block Upgrade 2. MIDS-LVT BU2 will provide Link 16 frequency remapping, enhanced throughput, information assurance modernization, and other significant updates to ensure that MIDS-LVT's operational preeminence will stand for years to come.

Meanwhile, the MIDS program office expects to verify the correction of many MIDS JTRS deficiencies, enter into full production, and achieve IOC in 2011. Platforms procuring MIDS JTRS include the F/A-18E/F Super Hornet, E-8C JSTARS, and the Air Force's RC-135 Rivet Joint and EC-130H Compass Call. Future MIDS JTRS platforms include the EA-18G Growler, E-2D Advanced Hawkeye, EC-130E Senior Scout, F-15E Strike Eagle, B-1B Lancer and B-52H Stratofortress.

PACIFIC OCEAN (June 6, 2011) A F/A-18E Super Hornet assigned to Strike Fighter Squadron (VFA) 81 maneuvers during an air power demonstration over the Nimitz-class aircraft carrier USS Carl Vinson (CVN 70). Carl Vinson and Carrier Air Wing (CVW) 17 are underway in the U.S. 7th Fleet area of responsibility. U.S. Navy photo by Mass Communication Specialist 3rd Class Travis K. Mendoza.

Concerning near-term fielding of MIDS JTRS, MIDS Program Manger Capt. Scott Krambeck said, "I am extremely pleased with the progress the team is making, the new trails we are blazing and the lessons learned that we are sharing with our JTRS teammates. The outstanding government and industry MIDS JTRS team continues to advance and demonstrate JTRS technology and soon the warfighter will benefit. I am anxious to get MIDS JTRS operating in the fleet."

With both the fielding of MIDS JTRS and the upgrade to MIDS-LVT, the MIDS program will advance even closer toward its goal to increase situational awareness across borders and around the world. CHIPS

For more information about the NATO Air Command and Control System, go to www.nato.int/cps/en/natolive/topics_8203.htm. For more information about JPEO JTRS, go to http://jpeojtrs.mil.

CENTRIXS-Maritime: connecting the warfighter

By Ann Dakis

The Space and Naval Warfare Systems Center Pacific's C4ISR department is working to make information dominance a reality by providing integrated command, control, communications, computers, intelligence, surveillance and reconnaissance systems to the U.S. Navy and coalition partners in the Asia-Pacific region.

"We are a key part of SSC Pacific's interface to the fleet," said Brad Carter, head of the maritime C4 systems engineering branch. "We interact daily with operational commanders and their staffs — they are the ones that give us requirements and tell us what's coming down the road operationally."

The Pacific C4ISR department provides the full spectrum of support services, from engineering to deployment, for Combined Enterprise Regional Information Exchange System efforts in the Pacific area of responsibility. CENTRIXS is a collection of classified coalition networks, called enclaves, that enable information sharing through the use of email and Web services, instant messaging or chat, the Common Operational Picture service, and Voice over IP. CENTRIXS supports combatant commands throughout the world, including the U.S. Pacific, Central and European commands.

"We support eight enclaves, each with a particular mission and particular set of coalition partners that participate in it," said Daryl Ching, head of the network engineering branch. "Two are bilaterals, CENTRIXS-JPN between the United States and Japan, and CENTRIXS-K, between the United States and Republic of Korea. The rest are multilateral among specific communities of interest, for example, CENTRIXS Cooperative Maritime Forces Pacific links the U.S. with Australia, Japan, Singapore, India, Korea and many other nations with Pacific navies."

CENTRIXS networks are used to support coalition interoperability among partner nations in antiterrorism, antipiracy, and humanitarian assistance and disaster relief operations throughout the world. CENTRIXS is also used extensively to support exercises like RIMPAC, or Rim of the Pacific, which can involve more than 14 countries.

Ching is responsible for the design and sustainment of CENTRIXS Network Operations Centers (NOCs) for the Navy. He ensures that the infrastructure at these shore stations support U.S. afloat forces and also integrate with coalition NOCs around the world. Ching is involved in a military construction project called P-173 with Naval Computer and Telecommunications Area Master Station Pacific in Wahiawa, Hawaii. He explained the significance of the project, "P-173 will be a new communication center supporting all Navy communications in this region, and we're on task to move the CENTRIXS Pacific Region NOC over from the old building."

This project includes the relocation of seven coalition network enclaves, each consisting of routers, switches, servers, desktop computers, computer network defense systems, circuits, modems and cryptographic devices.

The CENTRIXS portion of P-173 allows Ching's engineers to improve the system design and gain efficiencies through virtualization. Each CENTRIXS network enclave will be redesigned to have improved performance, redundancy and future growth potential with an overall reduction in the server footprint. Through virtualization techniques, the physical server count will be reduced from 88 down to 24, which will also reduce the demand for space, power, cooling and ventilation in the new building.

The new CENTRIXS NOC will allow coalition countries improved access to the various networks through the use of the Internet and allow watchstanders improved monitoring capability through increased workstation access. The improved CENTRIXS NOC system will also be used as the baseline system for the Unified Atlantic Region Network Operations Center located in Norfolk, Va.

Ching is also working with the CENTRIXS Battle Force Tactical Network (BFTN) program, an effort to design a fail-safe system to maintain coalition networking communication in a satellite denied environment. The BFTN and CENTRIXS-M programs teamed up to focus on providing the warfighter with coalition interoperability in the event of loss or reduction in satellite communications.

"Traditional communications are hub and spoke, with the NOC being the hub and ships being the spokes," Ching said. "In the event that connectivity to the hub is lost, ships still need to communicate and interoperate with each other."

The BFTN group focuses on the physical hardware and communication devices for line-of-sight (LOS) and over-the-horizon (OTH) capability, while Ching's CENTRIXS-M engineers focus on the software applications and ad hoc networking environment.

"The ad hoc network environment is created when U.S. and coalition ships join in LOS or OTH communications," Ching said. "This creates an interesting challenge as the routing architecture and software applications have to adjust to this constantly changing network environment. In addition to the routing architecture, the computer network defense architecture has to adjust to this as well."

In the past, the NOCs were the perimeter defense for ships providing computer network defense. With LOS and OTH communications, a U.S. Navy ship has the ability to directly communicate and establish a network connection with a coalition ship.

Carter oversees the design, configuration and deployment of both portable and permanent CENTRIXS capability for coalition partners. In this regard, fly away kits are provided to partner nations that do not have a deployable or permanent CENTRIXS capability to rapidly support a coalition operation or exercise.

The kits provide the temporary connectivity required for countries to participate in the event, and hopefully, entice them to have CENTRIXS permanently installed. The kits have the capability to connect quickly and securely to a variety of wide-area circuits for communicating with other CENTRIXS units. For example, the fly away kits have interfaces to Inmarsat-B, Fleet Broadband, Ku-Band, Broadband Global Area Network (BGAN), VSAT, Iridium and Fleet 77 satellite systems.

The kits also support the Integrated Services Digital Network (ISDN), regular telephone lines, and tunneling via the Internet to link into the proper CENTRIXS enclave. The Pacific C4ISR department developed many of the networking standards and settings for these different configurations, which have been shared and propagated to other combatant commands. This standardization results in a globally scalable maritime design enabling seamless connectivity from almost anywhere on the planet.

"At any given time, we have anywhere from five to 15 kits deployed," Carter said. "Each one requires quite a bit of preplanning and testing because it has to be configured to work with the designated country's shipboard design and onboard systems. In addition, we are constantly making modifications to the kits to take advantage of new technologies."

The fly away kits led to the successful installation of permanent CENTRIXS capabilities in various countries in the region, for example, in Singapore and Malaysia.

The department maintains a secure laboratory, known as the Technical Development Center (TDC), where equipment for temporary and permanent CENTRIXS installations for coalition partners can be staged, configured, and tested end-to-end using a country's specific circuit paths. The TDC's extensive capability results in a tremendous improvement in efficiencies for CENTRIXS deployments and installations in coalition countries.

Efforts that previously had to be done weeks in advance can now be done in only a few hours saving considerable time and money while increasing warfighting effectiveness. The rapid deployment enabled installations on units within one day of getting underway, greatly enhancing interoperability.

"We successfully installed kits on Indian navy ships scheduled to participate in Malabar 2011 in one day, and similar efforts were used to deploy more than 25 kits in supporting units participating in RIMPAC 2010," Carter said.

The maritime industry is transitioning to the next generation of satellite systems, and the Pacific C4ISR department followed suit for the Navy to take advantage of cost savings and increased services. Transitioning from Inmarsat-B to the BGAN satellites allowed fly away kit holders to move from paying by a per-minute rate to a per-megabyte data rate. The large reduction in cost for connectivity enabled the kits to stay continuously connected, allowing coalition partners to greatly increase situational awareness and participate full time in collaboration at sea.

Space and Naval Warfare Systems Center Pacific's C4ISR department personnel provide integrated command, control, communications, computers, intelligence, surveillance and reconnaissance systems to the U.S. Navy and coalition partners in the Asia-Pacific region.

CENTRIXS is a collection of classified coalition networks, called enclaves, that enable U.S. and coalition information sharing through the use of email and Web services, instant messaging or chat, the Common Operational Picture service, and Voice over IP.

"CENTRIXS has become more prevalent in recent years because of growth in the need for secure coalition networks that allow partner nations to work more closely in their operations," said CENTRIXS lead engineer Dr. Russ Grall. "But a second reason is efficiency. By standardizing network designs we've addressed problems that have existed in the past where countries build their own systems then try and interface with the U.S. and cannot because of protocols or standards."

Permanent CENTRIXS installations also reduce U.S. naval costs because partner nations pay for the connectivity, and U.S. personnel do not have to continually prepare, deploy and recover fly away kits. One of the most significant developments has been the capability to access certain CENTRIXS enclaves via the Internet.

"Rather than have countries pay thousands of dollars to put in a dedicated classified circuit, they can use the Internet as a transport to get to CENTRIXS which costs a few dollars a month," Grall said.

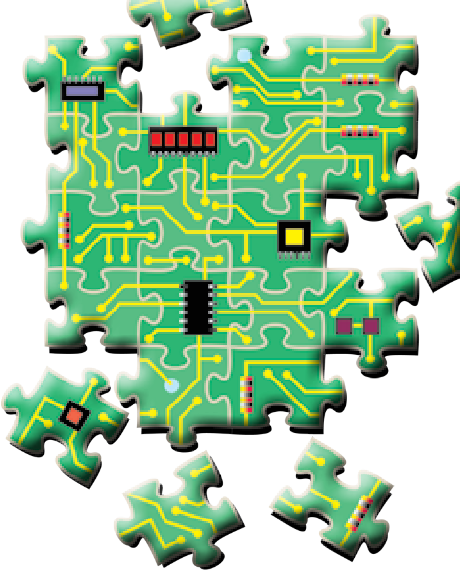
Carter and Ching's branches are working together to expand the presence of CENTRIXS over the Internet to additional enclave networks. They work together on many efforts to ensure consistency in the design and performance of products.

"Improvements to the hardware that is deployed, reductions in equipment size, efficiencies in long haul connectivity, the wide area circuits that connect countries to the U.S. NOC, as well as tunneling over the Internet, have all helped facilitate further CENTRIXS growth and successes because these are capabilities that countries want and are willing to buy," Grall said.

The efforts of Carter, Ching and Grall in Hawaii are critical for allowing the U.S. Navy to interoperate with coalition partners within the joint community. Their familiarity with partner nation platforms, requirements and operations ensure that the future of coalition information sharing remains strong. CHIPS

Ann Dakis is a staff writer with SSC Pacific's public affairs office.

Building a Small KM Collaboration Portal



In the Beginning

The distributed information systems experimentation (DISE) team, at the Naval Postgraduate School, uses knowledge management to plan and execute Department of Defense experiments. For example, the annual Trident Warrior series involves year-round coordination with geographically disparate organizations and personnel using both classified and unclassified networks.

During planning, execution, and the post-experiment stages of TW, data is collected through online feedback forms. The analysis of this and other collected data culminates in multiple decision informing reports.

DISE has been on the forefront of using KM for nearly a decade. The initial DISE team implemented a KM solution called FIRE (FORCEnet Innovation and Research Enterprise) in 2004 with the Oracle Collaboration Suite for Trident Warrior planning. OCS is comprised of a "shrink-wrapped" server with portal and collaboration applications. Before the advent of Web 2.0 collaboration and the flexibility of service oriented architecture, FIRE was considered somewhat advanced, and it served the needs of KM well.

The core backend of OCS is the database server which made Oracle a good choice. The "out-of-the-box" software was both a plus and a curse. For those just beginning KM and collaboration, the out-of-the-box approach simplified many aspects of maintenance, but could also serve as a straightjacket because of the inability for customizing to meet ever-changing user requirements. Nevertheless, the simplified approach allowed extensive portal post-development work that included the development of forms and reports needed by the experimenters.

Over time the FIRE solution grew into an enterprise-wide product. With growth came production challenges, including the need for hardware upgrades; software updates and security patches; backup and recovery decisions; and a requirement for help desk support. In addition, because DoD-wide systems must be certified and accredited according to information assurance policies to operate on a defense network, we had to satisfy security requirements. Many of the collaborative and data collection tools were limited on FIRE, and not flexible enough to expand capability and functionality when needed. The options for backup and recovery solutions were limited. In addition, our servers were reaching the five-year end of life cycle, and there was an opportunity to migrate to faster and cheaper servers to meet the new demands.

Since the heart of the system is the database, we decided to stay with an industry leader, so we chose Oracle Database 11g. The added bonus to using Oracle 11g is that the Navy has an Oracle Database Enterprise License which provides significant benefits, including substantial cost avoidance for the DON. (See page 66 for more information about the Navy's Oracle Enterprise License Agreement which requires mandatory use for Navy programs and activities covered by the agreement.)

For designing the next-generation architecture to build around the database, we determined that the system must:

- Work in three enclaves, unclassified, secret and top secret, with minimum IA work.
- Be easily maintained by a small team of IT personnel and faculty but still be scalable.
- Minimize the number of single points of failure and offer a robust backup and recovery capability.
- Leverage current developers' knowledge and our development investment.
- Take advantage of new technologies, such as SOA and Web 2.0, while maintaining a bridge from the legacy solution to the new.
- Include developer tools for simple applications used to import Microsoft Excel and Access files.
- Use open source standards as much as possible.
- Work with a wide range of operating systems from Windows 7, to Snow Leopard, to Red Hat Linux. The platform must support a wide-range of developer tools and languages, such as Java, JavaServer Faces and C#, and be able to integrate third-party apps, such as Microsoft SharePoint.
- Minimize licensing costs.
- Incorporate strong help desk and vendor support.

Hard work, perseverance and the Navy's Oracle Enterprise License Agreement build a KM solution that suits user needs

Because our team is small, and we are risk averse, we took an evolutionary approach. There are many good KM collaboration products, but we used a conservative approach while creating options to add best-of-breed products when users required additional capability. We stayed with Oracle products to minimize costs for licensing and training developers and maintainers because we concluded Oracle's features best met our requirements.

While the products are Oracle-specific, they are Java-based; therefore, the chance of vendor lock-in is reduced, and we could use other products, for example, from IBM or Microsoft, with the new KM portal. Because of our conservative approach, we reluctantly ruled out virtualization for this KM portal iteration, but it will remain a goal for future upgrades.

The Oracle solution consists of two major parts each connecting to an Oracle database. One part is Oracle Fusion Middleware that consists of the WebLogic Server, and the Oracle Portal 11g, which supports knowledge management efforts with seeded portlets, forms and reports. Oracle Portal also comes with a suite of developer tools, including JavaServer Faces and Application Express (APEX), which allow custom development.

The second part of the new solution is collaboration and social networking capability using Oracle Beehive for chat, team workspaces, tasks, wikis, discussion groups, content management and Web conferencing. These features are tied together with Oracle Single Sign-On and Oracle Internet Directory (SSO/OID) which provide a single sign-on, not only for Oracle products, but any third-party products, such as SharePoint, that you might decide to add later.

Research and Learning

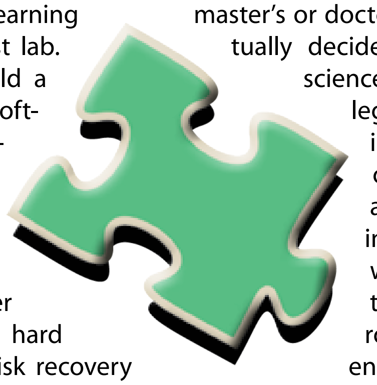
Even if your staff is experienced in IT management and programming, reaching a solution requires extensive research, learning about options and analysis. Prior to proposing an architecture to sponsors, a requirements and feasibility study should be conducted with a review of technology candidates that includes how easily a proposed technology can be bridged to your legacy system.

Technology is always in a state of flux so there is a point you just have to pull the trigger and go with the best technology at the time. Great care should be taken to explain backend improvements from a management perspective because users naturally concentrate on user enhancements and not necessarily in understanding management issues related to selecting enterprise software.

Production systems cannot just be thrown away and replaced by a new system, so decision makers must carefully consider how a new technology can be implemented without risking the whole enterprise.

Both Oracle and Red Hat products can be downloaded and used at no charge if you are testing concepts. Oracle also provides many of its applications (pre-built appliances) virtually through VirtualBox (www.virtualbox.org/), including Oracle 11g, WebLogic, TimesTen, APEX SQL Developer Data Modeler and JDeveloper. The VirtualBox allows a quick way to explore software candidates without extensive installation or new hardware.

Once the basic architecture and requirements are determined in the critical research and learning stage, you will need a test lab. Our plan was to first build a lab to test various vendor software and hardware candidates, and on successful completion, move them to the production environment. To build the lab we salvaged old server hardware and restored hard drives using SpinRite, a disk recovery tool. For some older servers we had to upgrade memory and central processing units. We then rack mounted all the servers, added a network switch, a kernel-based virtual machine, and an uninterruptible power supply to make the lab simulate the production environment.



Our small lab was not only a test environment but a learning one as well. We reinstalled test systems so many times that we could do it almost without thinking about it. We made many mistakes, but they were not costly because they were made in the lab and not in production. Installation mistakes can be fatal in a production environment, but in a test environment, they are instructional. While you do not need to test the exact same architecture, you must mimic the general design of the production system. We emphasize that you must have test servers available even after moving into production.

Manpower and IA Challenges

Hardware and licensing are but a small part of the cost of any KM system. Initially, one person managed FIRE. But, with growth in the number of users, FIRE went through a major upgrade in 2007 using industry consultants working with DISE team members. By 2008, due to budget constraints, DISE faculty team members learned to run FIRE by attending Oracle and Red Hat classes.

The effort to modernize FIRE was spearheaded by DISE team members who began by researching new collaboration solutions at Oracle OpenWorld 2008. Most DISE team members are faculty who teach two to four classes a year, as well as working on other projects, so we had to identify additional team members for the project. NPS students were unavailable because most were working full time on master's or doctorate degrees. We eventually decided to recruit computer science interns from local colleges to assist. The resulting team was comprised of two faculty members and up to two to four interns. Although we all worked part time on the project, we worked round-the-clock to ensure rapid progress.

Before going live on operational networks, all our servers went through a certification process conducted by an NPS information assurance team. Because DISE members are typically researchers who work on KM, and not IA professionals, this was particularly challenging. Approximately 80 percent of manpower costs may be related to IA requirements. Anyone fielding a system in a classified environment should be careful not to underestimate the level of effort required.

Instead of a standard Red Hat Enterprise Linux installation, which requires extensive post-installation rework to comply with IA security requirements, we installed a mini version of Red Hat using a custom configuration file known as Kickstart. Kickstart manages the operating system installation process to ensure required files and correct security and network settings are used.

Our Kickstart approach is based on the Defense Information Systems Agency's DoD Bastille, one of the projects of Forge.mil (www.forge.mil/), a DISA collaboration activity designed to improve the ability of the DoD to rapidly deliver dependable software, services and systems in support of net-centric operations and warfare. Forge.mil capitalizes on concepts proven in open source software development that have already reaped tremendous benefits for software and technology development communities. Along with accelerating technology development and fostering innovation, Forge.mil can also enable early and continuous collaboration and information-sharing among all stakeholders in a secure development environment.

Bastille integrates the specific security, technical and implementation guidelines required by DoD. We further modified Kickstart so that the Red Hat installation would also meet Oracle technical requirements. The Kickstart file can be reused for other OS installations with minimum modification, thus ensuring consistency and simplicity that would automatically implement our security and technical best practices.

Using Kickstart was only a first step; we then had to run DISA's approved Security Readiness Review (SRR) and Retina Network Security Scanner. The SRR produces a detailed report and delineates alerts based on severity as Category 1, 2 or 3, with CAT-1 as the most severe. Retina reports are more detailed and provide more specific fixes. Since the two software tools detect virtually all possible security holes, the reports are extensive, with each IA alert corrected one-by-one.

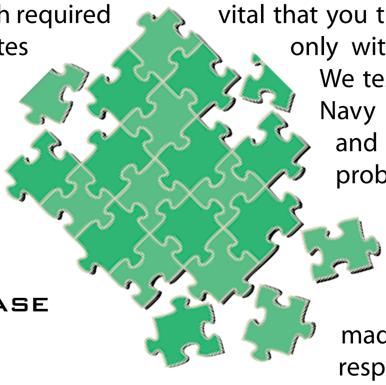
We resolved most of the more complex alerts with help from DISA documents and NPS faculty members, who were Linux experts. At times, the IA solutions made our system unstable so we had to reverse some changes. For this we used a server with a RAID 1 mirrored pair and always maintained a system backup to revert back to the original version. RAID, an acronym for redundant array of independent disks, is a technology that provides increased storage functions and reliability through redundancy.

Oracle server software uses a wide range of ports that may not be compatible with DoD network policy so it is important to consult with your network administrator and IA office. We recommend that you illustrate your architecture using Microsoft Visio, or a similar program, so that all parties have a clear understanding of the proposed architecture and how it fits into the overall infrastructure.

Oracle default ports can be changed, but this should be done prior to installation. The installation may need a reverse proxy; we used Squid, an open source high-performance caching proxy server designed to run on Unix systems.

Opening a port is complicated and tedious, involving a lot of time and paperwork, so the Squid reverse proxy server was a quick and adequate solution. Our solution involved four physical servers residing on the DMZ and the internal network. A DMZ, or demilitarized zone, is a subnetwork that exposes an organization's external services to a larger untrusted network, usually the Internet; it also adds an additional layer of security.

We recommend that the database and Oracle Single Sign-On and Oracle Internet Directory reside on internal networks. The Oracle Portal and Beehive should reside in the DMZ. To get this configuration to work properly, we had to construct unique port configurations. Finally, all Web connections had to be encrypted connections (HTTPS), which required testing DoD root certificates in a development lab to ensure trusted site identification for users accessing FIRE, and generating new certificates for production servers.



Handling Database Growth

Originally, the servers were running from a single server with approximately 300 gigabytes of storage. We quickly realized the storage disks were reaching capacity, and we were routinely deleting files to increase available disk space.

In our lab we tested a Dell disk storage array dedicated to the database that gave us more room to work with and expand. We are also exploring automatic storage manager (ASM) solutions to seamlessly grow Oracle database storage. Changing RAID configurations to allow growth might be difficult or impossible after installation so it's better to get it right the first time.

Vendor Support

Selecting the right hardware and software greatly depends upon the quality of support available for your system. For Oracle support we purchased a plan for 24/7, 365 days of online and telephone support. The Oracle support team has experts for each of its applications, and we talked to them whenever we had a problem to resolve. In some cases, Oracle support staff would call us or set up a Web conference if we were dealing with an issue that was critical to our mission.

They were also great teachers if we didn't understand a concept. For this support we chose a pricing model based on number of users as opposed to number of processors. This worked well within our budget, and it is the cheapest way to go if you have less than 300 users.

In addition to the savings we obtained by using the Navy Oracle Database Enterprise License Agreement, we used contract models, like the GSA Schedule, to bring costs down.

Testing Your System and Going Live

Even with a well-planned system, it is vital that you thoroughly test and not only within your environment. We tested our system on the Navy Marine Corps Intranet and found additional port problems so having users access the system via different networks is important to eliminating problems. We made a major effort to respond quickly to our representative users to quickly resolve any connectivity problems, but it may take several weeks to resolve site-specific network or specific client problems. The success of these efforts begins with a well-written test plan.

With little developer work required, Oracle Beehive provides collaboration and social networking tools right out of the box. Some development work is required for the Web portal to provide users with dynamic content and an interactive experience. Portal 11G offers developers a variety of tools and seeded portlets to capture and display data and reports.

We chose the Linux operating system to run Oracle products, and we used the NPS Information Technology and Communications Services (ITACS) contract with Red Hat, Inc. Red Hat's Web and phone support is comparable to the support that Oracle and Dell offer. On the hardware side, we chose Dell servers. ITACS has a contract with Dell, and Dell support is provided around-the-clock. We could also get replacement parts within one workday.

The architecture leaves a small footprint, just 5U (a rack unit measurement), consisting of five rack-mounted PowerEdge R610 servers featuring reduced power consumption. The 610s offer room to grow with two sockets and up to 48 gigabytes of memory. The servers have room for six 2.5-inch Serial Attached SCSI (SAS) drives that allowed us to configure RAID 1 mirrored (two) hard drives for the operating system and RAID 5 striping (four) hard drives for the databases and Web servers. This configuration allowed some fault tolerance in case of hard drive failure.

SAS is a computer bus used to move data to and from computer storage devices. In computer data storage, data striping is the technique of segmenting logically sequential data, such as a file, in a way that accesses of sequential segments are made to different physical storage devices.

Striping is useful when a processing device requests access to data more quickly than a storage device can provide access. By performing segment accesses on multiple devices, multiple segments can be accessed concurrently. This provides more data access throughput, which avoids causing the processor to idly wait for data accesses. Striping is used across disk drives in RAID storage, network interfaces in grid-oriented storage, and RAM in some systems.

The DISE and ITACS teams signed a memorandum of understanding that enabled us to host servers in a production grade network operations center. The temperature and dust-controlled NOC has high-speed connectivity to the Internet and to military (.mil) networks. In addition, it provides power backup using batteries and generators.

Backup and Recovery

Because we are running several different servers, we had to implement separate backup strategies. For the Oracle Database 11G, we used information gleaned from the database training class and ran the database in archive log mode, which enables hot backup (also called a dynamic backup), point-in-time recovery and scheduled daily backup.

A hot backup can be performed on data even though it is actively accessible to users and may be in a state of being updated. Hot backups can provide a convenient solution in multi-user systems because they do not require downtime, as does a conventional cold backup.

We use Dell Storage Enclosure to store backups on a single array. The servers are connected to the single storage array with multiple disk controllers for redundancy. We also produce large capacity tape drive backups for off-site storage.

Lessons Learned

We believe that a small team can create an effective enterprise KM system if the team plans well and addresses the issues we discussed. Critical in all of the efforts is a robust test environment and strong support from your IA team.

Nothing we did was extremely technical. If your team is willing to do some "homework" and has the patience to persevere though occasional setbacks, the reward could be a KM portal that will specifically meet the needs of small groups doing important work. CHIPS

Arijit Das is a faculty member in the computer science department at the Naval Postgraduate School.

Tony Kendall is a faculty member in the information sciences department at the Naval Postgraduate School.

ONR Announces Multimillion-Dollar STEM Grand Challenge

By the Office of Naval Research Corporate Communications

The Department of the Navy's Office of Naval Research provides the science and technology necessary to maintain the Navy's and Marine Corps' technological advantage. Through its affiliates, ONR is a leader in science and technology, with engagement in 50 states, 70 countries, 1,035 institutions of higher learning and 914 industry partners.

June 15, the Chief of Naval Research announced an incentive plan to award up to $8 million for ideas aimed at boosting K-12 education in the sciences. Rear Adm. Nevin Carr made the announcement during the Naval STEM Forum, in Alexandria, Va., June 15-16.

"Today's approaches to training and education must seek new innovative ways to sustain America's position as a global technology leader," Carr told the more than 650 government, academia and business leaders gathered at the forum.

"I wouldn't begin to pretend that the Navy is going to solve the country's STEM problem…there are others out there working very hard to do that," Carr said, "but we also want to make sure we are all intersected in a way that we can get the most out of the collective."

The challenge is one of many efforts the Navy has developed to encourage students, parents and teachers to pursue STEM (science, technology, engineering and mathematics) education and careers. The Navy seeks to increase the talent pool of future Sailors, naval scientists and engineers through its STEM initiatives.

The Navy will award up to $1.5 million to each Phase One selectee. Teams will compete to advance to Phase Two. In the second stage, up to two teams will be awarded as much as $1 million each to extend their Phase One success to a Navy training challenge for another year. The technologies will be designed to meet students' individual learning style. ONR will issue the proposal as part of its Long-Range Broad Agency Announcement for Navy and Marine Corps science and technology efforts. Contract awards are expected in fiscal year 2012, and ONR officials anticipate multiple awards for Phase One.

In Phase One, participating Grand Challenge teams must develop an intelligent tutor, a system that uses computers and provides direct customized instruction to augment classroom instruction, which will serve as an aid for teaching middle to high school STEM curriculum. Teams will be evaluated on how well they demonstrate significant student improvement in retention, reasoning and problem solving at an affordable cost. Based on these results, up to two teams will be selected to advance to Phase Two.

In Phase Two, selected team(s) must adapt their "tutor," or software, to effectively address Department of the Navy-specific training audiences and criteria. The winning team will be able to demonstrate a tutor that cost effectively produces significant improvements similar to its Phase One effort.

For more news from ONR, visit www.navy.mil/local/onr/. CHIPS

A Legacy of Efficiency

By Amanda George

Efficiency is the watchword of the Department of Defense as Defense Secretary Robert Gates implemented business reforms and eliminated duplicative and unnecessary overhead costs in the last 18 months. This article summarizes several key efficiency efforts Secretary Gates undertook.

When Gates took office in December 2006, the defense budget was buoyed by a strong economy. As he leaves office June 30, the defense budget is declining, strongly affected by the fiscal crisis. While there are many questions regarding the conflicts the United States may become involved in, and other missions the military may be required to perform, in the future, one thing is clear: the defense budget will decline.

From the onset of the financial downturn, Gates proactively worked toward increasing the efficiency of the department with a four-track efficiency program. This approach is designed to move the defense enterprise toward a more efficient, effective, and cost-conscious way of doing business, Gates wrote in a memorandum issued Aug. 16, 2010.

The first track specifies shifting overhead costs to fund force structure and future modernization. The second track invites outside experts to suggest ways for the department to become more efficient. The third track uses front-end assessments to inform fiscal year 2012 budget requests. The fourth, and most challenging track, focuses on reducing excess and duplication across the entire defense enterprise.

Track 1: Shifting Overhead Costs to Force Structure and Future Modernization

The demand for military missions continues to rise; however, savings are still possible. Gates instructed each of the services to find efficiencies in overhead costs and use the savings to strengthen direct support to the warfighter. Gates said, "The goal is to cut our overhead costs and to transfer those savings to force structure and modernization within the programmed budget. In other words, to convert sufficient 'tail' to 'tooth' to provide the roughly 2 to 3 percent real growth — resources needed to sustain our combat power at a time of war and make investments to prepare for an uncertain future."

Secretary Gates originally introduced his efficiency and savings initiative in a May 8, 2010 speech at the Eisenhower Presidential Library in Abilene, Kan., Gates said, "I am directing the military services, the Joint Staff, the major functional and regional commands, and the civilian side of the Pentagon to take a hard, unsparing look at how they operate — in substance and style alike."

This initial direction was codified in a memo to all services June 4, 2010. The memo emphasizes the logic behind the efficiencies, which is to move resources from bureaucracies to accounts for new weapons, existing force structure and personnel bills.

For this tail to tooth effort, Gates directed the Army, Navy, Marine Corps and Air Force to find savings of a combined $84.9 billion from the fiscal year 2012 to 2016 budgets and divert those funds into acquisition, personnel and maintenance accounts. To find these savings Gates instructed the service secretaries to look to many areas of the budget, but to focus in particular on headquarters and administrative functions, support activities and other overhead costs.

Another $17 billion in efficiency savings is sought from other DoD agencies and field activities, such as the Joint Staff, Under Secretary for Intelligence, and others. The total savings are to be spread over five years with each department tasked to find $2 billion in FY 2012; $3 billion in FY 2013; $5.3 billion in FY 2014; $8 billion in FY 2015; and $10 billion in FY 2016. The savings goals and plans will be incorporated into the services' FY 2012 program objective memorandum (POM) proposals.

Jan. 6, 2011, the military departments announced the results of their efforts as outlined below.

The Air Force proposes efficiencies measures will total some $34 billion over five years. Among the proposals are:

- Consolidating two air operations centers in the U.S. and two in Europe;
- Consolidating three numbered Air Force staffs;
- Saving $500 million by reducing fuel and energy consumption within the Air Mobility Command;
- Improving depot and supply chain business processes to sustain weapons systems, thus improving readiness at lower cost; and
- Reducing the cost of communications infrastructure by 25 percent.

The Army proposes $29 billion in savings over the five years. The measures include:

- Reducing manning by more than 1,000 civilian and military positions by eliminating unneeded task forces and consolidating six installation management commands into four;
- Saving $1.4 billion in military construction costs by sustaining existing facilities; and
- Beginning consolidating the service's email infrastructure and data centers, which should save $500 million over five years.

The Department of the Navy proposes savings of more than $35 billion over five years. Actions include:

- Reducing manpower ashore and reassigning 6,000 personnel to operational missions at sea;
- Using multi-year procurement to save more than $1.3 billion on the purchase of new airborne surveillance, jamming and fighter aircraft; and
- Disestablishing staffs for submarine, patrol aircraft, and the destroyer-squadrons, plus one carrier strike group staff.

Track 2: Inviting Outside Experts

The Defense Business Board provided Gates with recommendations to increase efficiency and find savings across the department in July 2010. Most of the suggestions were incorporated in Gates' initial efficiencies memo of Aug. 16. The recommendations are grouped under four major recommendations. First, initiate a hiring freeze and headcount control process. The board recommends that the DoD establish a high-level process to track and control military, civilian and contractor staffing and costs denominated by full-time equivalents. The DBB recommends reducing civilian staffing levels back to FY 2003 levels, or reducing by 15 percent, whichever is greater. Second, the DBB recommends eliminating organizational duplication and overlap, focusing first in areas, such as in the Office of the Secretary of Defense and Joint Staff, in areas like public affairs, legislative affairs, legal affairs, personnel oversight, and in the office of the Director of OSD Cost Assessment and Program Evaluation (CAPE), Joint Requirements Oversight Council (JROC) and Under Secretary of Defense for Acquisition, Technology and Logistics (USD AT&L). Third, the DBB recommends downsizing the combatant command staffs. Finally, the DBB recommends curtailing indirect spending by reducing the frequency of duty station moves, reducing travel requirements and the number of conferences, and modifying its end of the year "use it or lose it" policy.

Track 3: Front-end Assessments

In April 2010, the Defense Department released a memo detailing updates to the budget process. As part of the revamping of the budget process known as planning, programming, budgeting and execution (PPBE), Gates directed front-end assessments of 20 capability areas that drive operational, force structure and investment needs, such as long-range strike, shipbuilding, electronic attack, satellites and end strength, to better shape Pentagon spending decisions.

The CAPE is conducting the assessments. The systems to be assessed are: tactical aircraft; integrated air and missile defense; reset of equipment from operations; global posture; cybersecurity; surveillance and reconnaissance; airborne intelligence; long-range strike capabilities; and strategic communications/information operations.

Track 4: Reducing Excess and Duplication Across the Entire Defense Enterprise

The fourth track initially consisted of a series of initiatives designed to reduce duplication, overhead and excess, and instill a culture of savings and restraint across the DoD. As the budget continued to tighten through the end of 2010, the Defense Department refined the objective to include a targeted amount of efficiency savings that will not be reinvested in the DoD. Jan. 6, 2011, DoD announced that it will cut $78 billion over the next five years from its previously projected Future Years Defense Program (FYDP). The cuts come from four major areas: DoD-wide overhead reductions and efficiencies; shifts in economic assumptions and other changes relative to the previous FYDP; savings to the Joint Strike Program to reflect re-pricing and a more realistic production schedule given recent development delays; and finally, a reduction in the number of active duty Army and Marine Corps personnel.

The Army and Marine Corps will take a 6 percent reduction in ranks starting in FY 2015 with end strengths of approximately 542,000 and 180,000, respectively.

The DoD estimates that its department-wide overhead reductions and efficiencies will generate roughly $54 billion in savings. These changes will affect three areas: personnel, day-to-day operations and individual agency structures. To reduce the costs associated with personnel, the DoD will start by freezing all government civilian salaries for two years. Additionally, for the next three years, the DoD will cut the size of its staff of support contractors by 10 percent per year.

Finally, Gates approved the elimination of more than 100 general officer and flag officer positions from the roughly 900 currently on the books. He also directed the elimination or downgrading of nearly 200 Senior Executive Service, or equivalent positions, from a total of 1,400 civilian executives. Although the savings will be modest, the primary purpose behind the shift is to create fewer, flatter, more agile, and thus more effective, organizations. Thus, the personnel changes are designed to create a leaner, more efficient cadre of government employees.

The zero-based reviews of OSD, defense agencies, field activities and combatant commands to rebalance resources, staffs and functions within and across components produced a number of opportunities to trim the size of the workforce. Additionally, Gates approved a plan to consolidate hundreds of data centers and move to a more secure information technology enterprise system.

Finally, Gates focused on paring down the costs associated with the multitude of reports that the DoD produces each year. He eliminated nearly 400 internally-generated reports, representing about 60 percent of all non-statutory reports. Also, effective April 2012, the requirement for any internal report with a commissioning date prior to 2006 will be canceled. To increase awareness of the costs associated with producing a report, every report printed after February 2011 must include the cost of its production.

Secretary Gates looked at individual agency structures and the overarching structure of the department and the combatant commands for opportunities to increase efficiency. After the Sept. 11 terrorist attacks intelligence operations multiplied. Therefore, one efficiency effort Gates backs is the consolidation of various redundant intelligence programs into two task forces located within the Defense Intelligence Agency (DIA). The two task forces will focus on counterterrorism and investigate how terrorism is financed. This effort will change the intelligence organization from one with a permanent organic apparatus staffed on a wartime level to one that can surge intelligence support as needed from the DIA.

Additionally, Gates examined possible rearrangements and disestablishments within the DoD. At press time, the Assistant Secretary of Defense (Networks and Information Integration) (NII), Business Transformation Agency and U.S. Joint Forces Command are in the process of disestablishment, with a reduced number of their essential functions transferred to other organizations.

Secretary Gates' efficiency measures are in motion, but several of the measures proposed require congressional approval. Although, some independent sources raised questions as to what the true monetary savings of the initiatives may be, Mr. Gates' changes instilled a cultural change in the Defense Department for more effective resource management.

All speeches by the Secretary of Defense are available at www.defense.gov/speeches/secdef.aspx. Defense Business Board reports are available at http://dbb.defense.gov/.

Amanda George is a strategic analyst in the corporate strategy group of Space and Naval Warfare Systems Center Pacific.

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 website at www.esi.mil/. If you cannot find the product or service provider you are looking for, please contact ESISupportTeam@navy.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: 23 Mar 15

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: 13 May 11 (Please call for extension information.)

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

Database Management Tools

Microsoft Products

Microsoft Database Products – See information under Office Systems on page 65.

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 on page 66.

Contractors:

Oracle Corp. (W91QUZ-07-A-0001); (703) 364-3110

DLT Solutions (W91QUZ-06-A-0002); (703) 708-8979

immixTechnology, Inc. (W91QUZ-08-A-0001); Small Business; (703) 752-0628

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: 01 Apr 13
immixTechnology: 02 Mar 16
Mythics: 18 Dec 11
TKCIS: 29 Jun 11 (Please call for extension information.)

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 66 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

www.esi.mil

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: Identity Management Suite; Communications Suite; Availability Suite; Web Infrastructure Suite; MySQL; xVM and Role Manager. 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

Ordering Expires: 24 Sep 12

Web Links:
Sun Products
www.esi.mil/agreements.aspx?id=160
Commercial Data
www.esi.mil/contentview.aspx?id=160&type=2
Dynamic Systems
www.esi.mil/contentview.aspx?id=162&type=2

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; (703) 752-0641 or (703) 752-0646

Ordering Expires: 03 May 11 (Please call for extension information.)

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

VMware

VMware – Provides VMware software and other products and services. This BPA has been designated as a GSA SmartBUY.

Contractor: ***Carahsoft Inc.*** (W91QUZ-09-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: 27 Mar 14

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

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 12

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

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) 820-4889

DLT Solutions (W91QUZ-06-A-0004); (703) 708-9127
Ordering Expires:
Quest: 29 Dec 15
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 62.*

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: www.esi.mil/contentview.aspx?id=150&type=2

SAP

SAP Products – Provide 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 Links:
SAP
www.esi.mil/contentview.aspx?id=154&type=2
Advantaged
www.esi.mil/contentview.aspx?id=155&type=2
Carahsoft
www.esi.mil/contentview.aspx?id=156&type=2
Oakland
www.esi.mil/contentview.aspx?id=157&type=2

Information Assurance Tools

Data at Rest (DAR) 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 to include approved U.S. thumb drives. 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 Army issued an enterprise solution for Army users purchasing DAR software. See the information provided on the Army CHESS website at https://chess.army.mil/ascp/commerce/contract/FA8771-07-A-0301_bpaorderinginstructions(2)_ARMY.jsp. As of this printing, the Air Force has not yet provided a DAR solution.

Mobile Armor – ***MTM Technologies, Inc.*** (FA8771-07-A-0301)
McAfee – ***Rocky Mountain Ram*** (FA8771-07-A-0302)
Information Security Corp. – ***Carahsoft Technology Corp.*** (FA8771-07-A-0303)
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)
Checkpoint – ***immix Technologies*** (FA8771-07-A-0307)
SPYRUS, Inc. – ***Autonomic Resources, LLC*** (FA8771-07-A-0308)
WinMagic, Inc. – ***Govbuys, Inc.*** (FA8771-07-A-0310)
CREDANT Technologies – ***Intelligent Decisions*** (FA8771-07-A-0311)
Symantec, formerly GuardianEdge Technologies – ***Merlin International*** (FA8771-07-A-0312)
Ordering Expires: 14 Jun 12 (If extended by option exercise.)
Web Link: www.esi.mil

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

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: https://esi.telos.com/contract/overview/default.cfm

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
www.esi.mil/contentview.aspx?id=118&type=2
Softmart
www.esi.mil/contentview.aspx?id=117&type=2
SHI
www.esi.mil/contentview.aspx?id=123&type=2

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: www.esi.mil/contentview.aspx?id=73&type=2

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: www.esi.mil/contentview.aspx?id=145&type=2

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. (N00104-08-A-ZF33); (800) 248-2727, ext. 5303

CDW Government, LLC (N00104-08-A-ZF34); (703) 621-8211

GovConnection, Inc. (N00104-08-A-ZF35); (301) 340-3861

Insight Public Sector, Inc. (N00104-08-A-ZF36); (443) 534-6457

Ordering Expires: 30 Jun 12

Web Links:

Adobe Desktop Products
www.esi.mil/agreements.aspx?id=52
Dell
www.esi.mil/contentview.aspx?id=53&type=2
CDW-G
www.esi.mil/contentview.aspx?id=52&type=2
GovConnection
www.esi.mil/contentview.aspx?id=33&type=2
Insight
www.esi.mil/contentview.aspx?id=54&type=2

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: www.esi.mil/contentview.aspx?id=186&type=2

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 Government, LLC (N00104-02-A-ZE85); (888) 826-2394

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

GovConnection (N00104-10-A-ZF30); (301) 340-3861

GTSI (N00104-02-A-ZE79); (800) 999-GTSI ext. 2071

Hewlett-Packard (N00104-02-A-ZE80); (800) 727-5472 or (845) 337-6260

Insight Public Sector, Inc. (N00104-02-A-ZE82); (800) 862-8758

SHI (N00104-02-A-ZE86); (800) 527-6389 or (732) 564-8333

Softchoice (N00104-02-A-ZE81); (877) 333-7638

Softmart (N00104-02-A-ZE84); (800) 628-9091 ext. 6928

Ordering Expires: 31 Mar 13

Web Link: www.esi.mil/agreements.aspx?id=173

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 websites 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 websites 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
www.disa.mil/gccs-j/index.html
GCSS users: Global Combat Support System
www.disa.mil/gcssj

Contractor: ***August Schell Enterprises*** (www.augustschell.com)

Download Site: http://redhat.augustschell.com
Ordering Expires: (Please call (703) 882-1636 for information about follow-on contract.)
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: www.esi.mil

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 (Please call for extension information.)
Web Link: 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: 30 June 11 (Please call for information about follow-on contract.)
Web Link: 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 websites 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 Dec. 1, 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: www.esi.mil/contentview.aspx?id=171&type

Department of the Navy Agreement

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 Dan McMullan, NAVICP Mechanicsburg contracting officer, at (717) 605-5659 or email daniel.mcmullan@navy.mil, for further review of the requirements and coverage.

This license is managed by the Space and Naval Warfare Systems Center (SPAWARSYSCEN) Pacific. The Navy Oracle Database Enterprise License provides significant benefits, including substantial cost avoidance for the department. It facilitates the goal of net-centric operations by allowing authorized users to access Oracle databases for Navy internal operations and permits sharing of authoritative data across the Navy enterprise.

Programs and activities covered by this license agreement shall not enter into separate Oracle database licenses outside this central agreement whenever Oracle is selected as the database. This prohibition includes software and software maintenance that is acquired:
a. as part of a system or system upgrade, including Application Specific Full Use (ASFU) licenses;
b. under a service contract;
c. under a contract or agreement administered by another agency, such as an interagency agreement;
d. under a Federal Supply Service (FSS) Schedule contract or blanket purchase agreement established in accordance with FAR 8.404(b)(4); or
e. by a contractor that is authorized to order from a Government supply source pursuant to FAR 51.101.

This policy has been coordinated with the Office of the Assistant Secretary of the Navy (Financial Management and Comptroller), Office of Budget.

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

THE DoD ESI PROGRAM OFFERS GREAT CUSTOMER SERVICE!

To contact the Navy Software Product Managers below, go to the ESI website at www.esi.mil/askSPM.aspx. If you cannot find the product or service provider you are looking for, please contact the ESI support team at ESISupportTeam@navy.mil.

Program Manager
Hank Ingorvate

Oracle (DEAL-O) Navy Project Management
Jeffrey Ho

Microsoft Products
Terry Sampité

iGrafx, Research and Advisory BPA, SAP
Nina Diep

Adobe Desktop Products, Adobe Server Products,
Enterprise Application Integration, Sun Software
Susan Ellison

Minitab, PowerSteering, RWD Technologies
Thao Vu

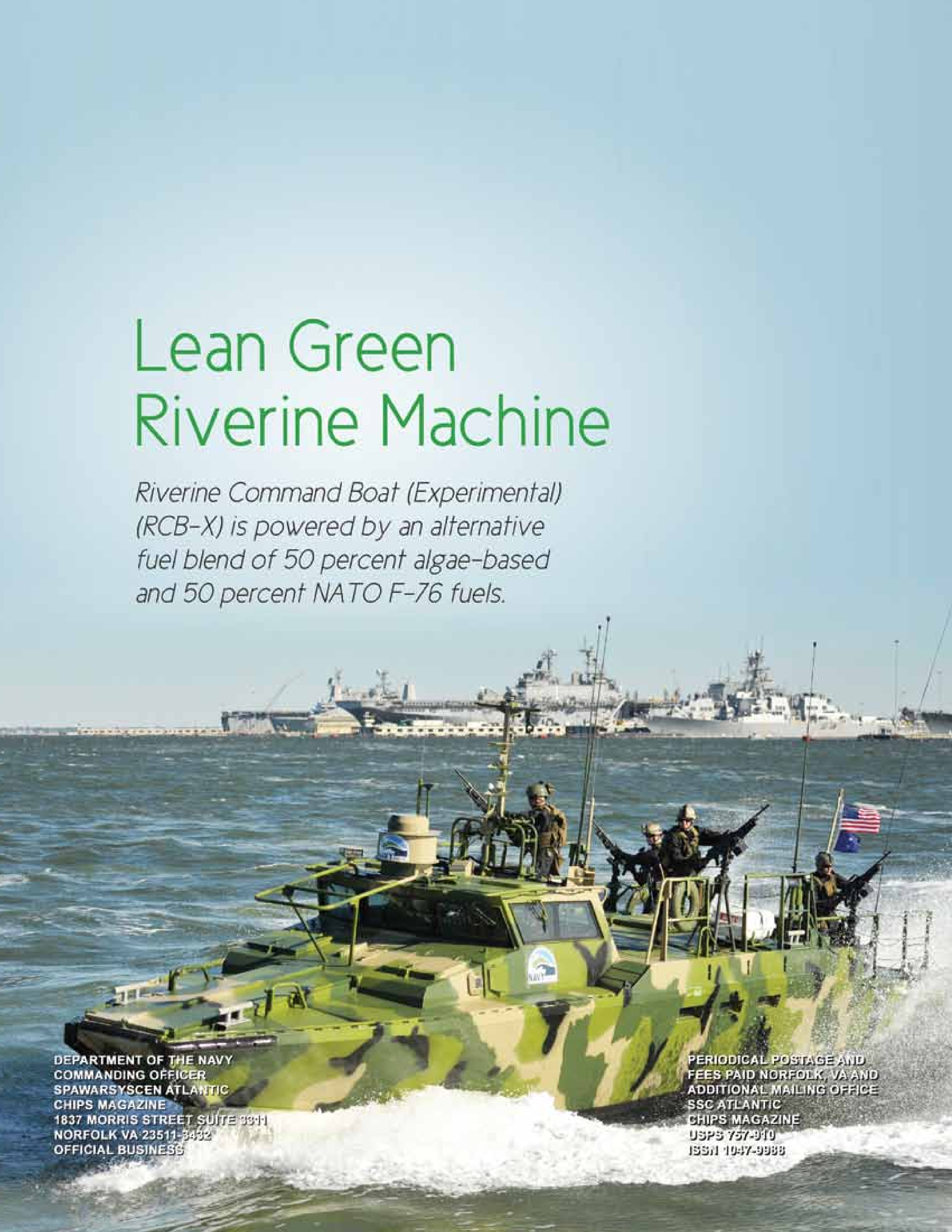
For your convenience all enterprise contract information
is consolidated under
www.esi.mil

www.chips.navy.mil

www.doncio.navy.mil

ENTERPRISE COST $AVINGS ARE JUST A CLICK AWAY

VISIT OUR E-COMMERCE SITE - WWW.ITEC-DIRECT.NAVY.MIL



Lean Green Riverine Machine

Riverine Command Boat (Experimental) (RCB-X) is powered by an alternative fuel blend of 50 percent algae-based and 50 percent NATO F-76 fuels.

DEPARTMENT OF THE NAVY
COMMANDING OFFICER
SPAWARSYSCEN ATLANTIC
CHIPS MAGAZINE
1837 MORRIS STREET SUITE 3311
NORFOLK VA 23511-3432
OFFICIAL BUSINESS

PERIODICAL POSTAGE AND
FEES PAID NORFOLK, VA AND
ADDITIONAL MAILING OFFICE
SSC ATLANTIC
CHIPS MAGAZINE
USPS 757-910
ISSN 1047-9988