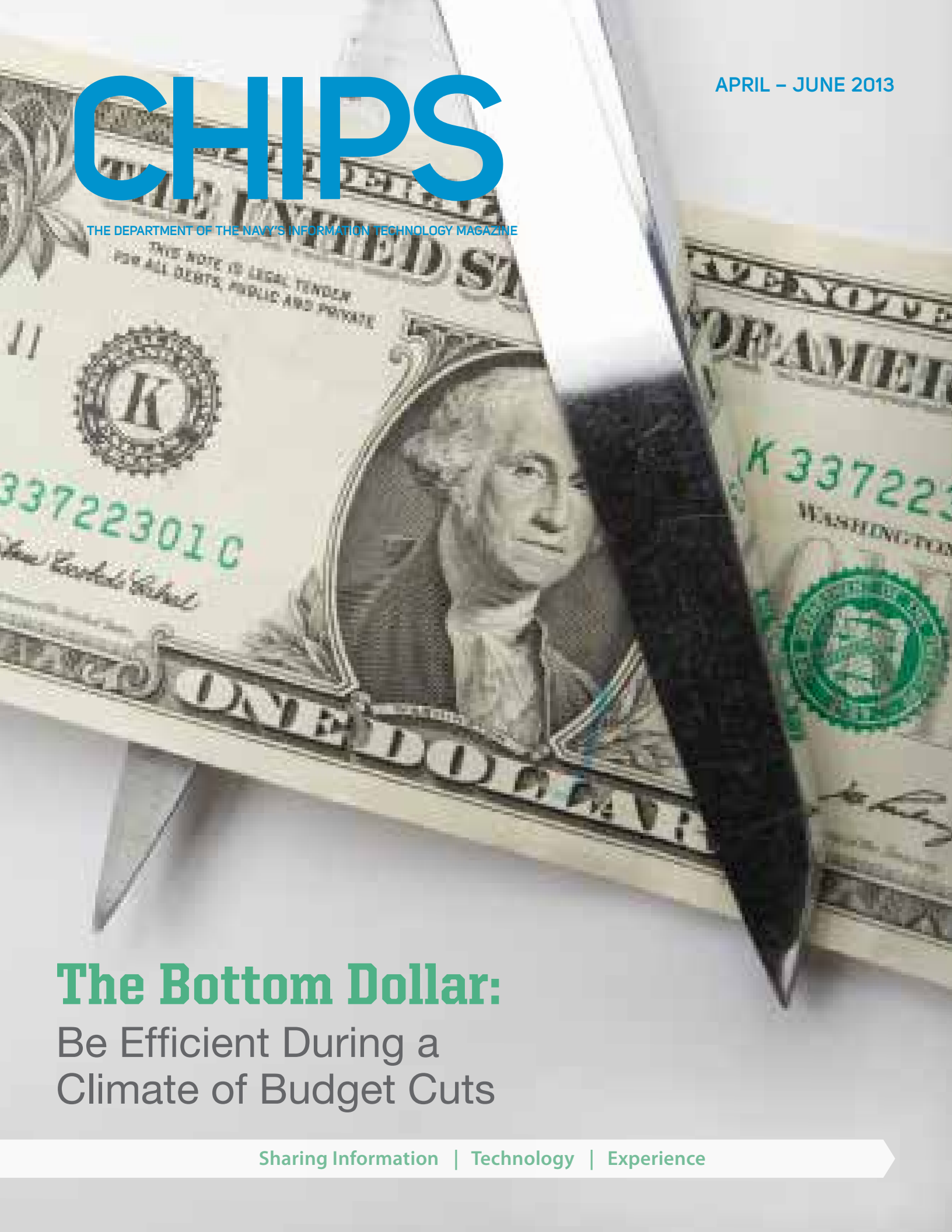


APRIL – JUNE 2013

CHIPS

THE DEPARTMENT OF THE NAVY'S INFORMATION TECHNOLOGY MAGAZINE



The Bottom Dollar:

Be Efficient During a
Climate of Budget Cuts

Sharing Information | Technology | Experience

CONTENTS

CHIPS

APRIL – JUNE 2013, VOL. XXXI ISSUE II

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 CAPT. MARK V. GLOVER

SPACE & NAVAL WARFARE SYSTEMS CENTER PACIFIC
COMMANDING OFFICER CAPT. JOSEPH J. BEEL

SENIOR EDITOR/LAYOUT AND DESIGN
SHARON ANDERSON

ASSISTANT EDITOR
HEATHER RUTHERFORD

WEBMASTER
DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER

COLUMNISTS
SHARON ANDERSON, STEVE DAUGHETY, TERRY HALVORSEN,
THOMAS KIDD, STEVE MUCK, ZAID YACU

CONTRIBUTORS
LYNDA PIERCE, DON ENTERPRISE IT COMMUNICATIONS
MICHELE BUISCH, DON ENTERPRISE IT COMMUNICATIONS

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, 1837 MORRIS ST., SUITE 3311, NORFOLK, VA 23511.

REQUESTS FOR ASSISTANCE SHOULD BE DIRECTED TO EDITOR, CHIPS, SPAWARSYSCEN ATLANTIC, 1837 MORRIS ST., SUITE 3311, NORFOLK, VA 23511-3432, OR CALL (757) 443-1775; DSN 646. EMAIL: CHIPS@NAVY.MIL; WEB: WWW.DONCIO.NAVY.MIL/CHIPS.

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.

ISSN 1047-9988

WEB ISSN 2154-1779: WWW.DONCIO.NAVY.MIL/CHIPS.



DEPARTMENT

In Every Issue

- 04** Editor's Notebook
- 05** A Message from the DON CIO
- 11** Hold Your Breaches!
- 18** Full Spectrum
- 58** Enterprise Software Agreements

Highlights

- 12** Don't Get Caught by Spear Phishing
By Steve Muck
- 32** Advances in Synthetic Aperture Sonar Transform Mine Countermeasures and Undersea Warfare
By Dr. Daniel D. Sternlicht, Jose E. Fernandez and Dr. Timothy M. Marston
- 42** Play the Game, Change the Game
By Heather Rutherford
- 48** A Night of Honor and Grace ...
A Tribute to Rear Adm. Grace M. Hopper
By Jennifer Ralston

Q&A

- 6** Janice C. Haith
Director, Department of the Navy Deputy Chief
Information Officer – Navy (DDCIO-Navy)
OPNAV N2/N6
- 8** Cmdr. Steve Shedd,
Commanding Officer, USS Milius (DDG 69)
- 14** Rear Adm. David G. Simpson
Vice Director, Defense Information Systems Agency



- 21** Rear Adm. Brian B. Brown
Commander, Naval Meteorology and
Oceanography Command
- 28** Cmdr. Sean O'Brien, Deputy Chief Information Officer
Naval Education and Training Command
- 38** Rear Adm. Terry B. Kraft
Commander, Navy Warfare Development Command
- 54** Robert Scott Jack II, Deputy Director,
Deputy Chief Information Officer for Command,
Control, Communications and Computers,
Headquarters Marine Corps

FEATURES

- 25** Navy Leaders Announce Plans for Deploying Cost-Saving
Laser Technology
By Office of Naval Research
- 26** DoD's Commercial Mobile Device Implementation Plan
By Sharon Anderson and Heather Rutherford
- 30** The Unmanned Combat Air System Demonstrator X-47B
*By Heather Rutherford and the Deputy Chief of Naval
Operations for Information Dominance*
- 37** New Department of the Navy IT Policies Signed
By DON IT Enterprise Communications Team
- 44** The Department of the Navy and Defense Logistics Agency
Partner to Deliver Savings
By the DON and DLA Print and Imaging Solutions Team
- 50** Modernizing and Securing Navy's MPTE Environment ...
and Winning a DON IM/IT Excellence Team Award
By the EIM Team and Sharon Anderson
- 53** The National Initiative for Cybersecurity Careers and Studies
By CHIPS Magazine



ON THE COVER

Simple changes in energy usage, minimizing document printing, and conducting meetings on Defense Connect Online can lead to significant savings for the Department of the Navy when everyone pitches in.

The Greatness of Change

If NOTHING ELSE, THE events of the last several months taught us that change is a constant that we can count on in the departments of the Navy and Defense looking far ahead into the future, as well as in the near term. Adapting to change isn't easy. It has been said that people and organizations when attempting change often fall short when they dream and set goals for themselves because they underestimate what they're capable of. They're afraid to think big; afraid of challenging themselves to greatness. Another problem with achieving real change is that people can view change as a loss because it is a disruption in beliefs they hold dear or an inconvenience to their long-held habits and behavior.

But change is inevitable and urgent, and across the DON and DoD, leaders are asking folks to step forward with ideas. Chief of Naval Operations Adm. Jonathan Greenert is calling for junior leaders, officers and enlisted, to be *disruptive thinkers*.

DON CIO Terry Halvorsen continues to say the department is considering and adopting changes it might have thought to be too extreme at one time to achieve efficiencies and cost savings in the DON's business IT processes. Everything associated with business IT spending and processes is on the table for analysis to further reduce the department's IT bill, he said.

It takes courage and determination to change — and to achieve greatness — but fortunately these are traits the DON has never been short of.

Welcome new e-subscribers!



SHARON ANDERSON



NORFOLK (April 4, 2013) The amphibious transport dock ship USS Arlington (LPD 24) is moored at Naval Station Norfolk for its commissioning ceremony. As the third Navy vessel to bear the name, Arlington commemorates the lives lost and the heroism demonstrated in the aftermath of the Sept. 11, 2001 terrorist attacks. U.S. Navy photo by Mass Communication Specialist 3rd Class Frank J. Pikul.

EDITORIAL CORRESPONDENCE

QUESTIONS? SEND all inquiries and questions to our editor
chips@navy.mil

Adapting and Overcoming Resistance to Change in an Evolving IT World



THE CHANGING TECHNOLOGY IS ONLY PART OF THIS “ADAPT AND OVERCOME” EQUATION. THE FOCUS ON BUDGET REDUCTIONS HAS MADE US MORE ACCEPTING OF IDEAS THAT, IN THE PAST, WE MAY HAVE THOUGHT TOO EXTREME TO CONSIDER.

IN THE 1986 movie, “Heartbreak Ridge,” Clint Eastwood plays the salty Marine Gunnery Sgt. Thomas Highway, an old-school Marine who realizes he must change some of his ways to succeed in a changing world.

His personal mantra — “improvise, adapt, overcome” — is also a teaching point he uses — relentlessly — with the Marines of his underperforming reconnaissance platoon.

We, in the Department of the Navy, face a similar challenge. With budgets already cut and more austere times ahead, we must adapt to our new environment and overcome the obstacles that block our path to achieving greater IT efficiencies. In other words, we must change the way we think about data and how we use it.

For example, we recently established a new policy regarding the department’s copiers, printers, faxes and scanners and our move to multifunction devices, which eliminates the need to have a separate device to perform each function. The policy is a first step at a major change in the department’s mindset toward printing. On the surface, this may appear to be an effort to simply save paper, but it’s much more than that. It’s about reducing the number of stand-

alone printers and going to multifunction devices; centralizing printing on a primary network; consciously determining when to print in color; and focusing on what — and when — we must print. Printing in color can cost up to 10 times as much as black-and-white printing, which can add up to millions of dollars in savings governmentwide. Furthermore, if a brief or an agenda can be displayed on screen, then there is no need to print a copy for each meeting participant.

Another example of adapting to our changing economic reality is rethinking how we store, display and host data. The DON Secretariat recently took the innovative first steps of moving unclassified data to a commercial hosting environment. The Secretary of the Navy’s public-facing information portal (www.secnav.navy.mil) is now hosted in the Amazon Web Services cloud. The decision to host the data on a public Web server resulted from an analysis of several factors, including the type of data stored in the portal, the ease of access due to significantly faster response times, security and cost.

The DON first considered a government site to host the portal, but found that commercial sites are less expensive. Further, congressional guidance

requires the department to evaluate and select commercially provided services that meet security standards and are less expensive than what it costs to perform those services internally. As a result, the DON has achieved a 50 percent reduction in cost to operate the portal.

The Amazon option is the first case of the DON placing low-risk, public-facing data on a commercial server to save money. The department will continue to explore similar savings opportunities.

Changing technology is only part of this “adapt and overcome” equation. The focus on budget reductions has made us more accepting of ideas that, in the past, we may have thought too extreme to consider. The next step is a more fundamental change to the way we do business and the way we act as a business.

And like Gunny Highway’s recon Marines, we will continue to adapt and overcome resistance to change to succeed in the department’s vital mission. ●

Terry Halvorsen

Janice C. Haith

Director, Department of the Navy Deputy Chief Information Officer - Navy
(DDCIO-Navy) OPNAV N2/N6

Ms. Haith is responsible for all CIO matters related to the Navy. This includes governance, enterprise architecture, information assurance, information management/information technology and Clinger-Cohen Act Compliance.

Ms. Haith responded in writing to questions regarding ongoing efforts across the Navy to reduce business IT spending and increase efficiencies in mid-March.



Janice C. Haith

Q: Due to the chance of a continuing budget resolution and sequestration, the Department of the Navy had to take immediate action on several fronts and has announced that it will cut back its spending on information technology in 2013 by 25 percent. The IT cut is effective immediately, and is in addition to the service's previous commitment to reduce its technology expenditures by 25 percent between 2011 and 2016. What will be some of the immediate effects of this policy?

A: We can anticipate a slowdown of IT spend in all areas, except warfighting. We can expect aggressive enforcement of cost-saving policies such as the multifunction device policy which requires us to improve management and use of standalone printers, copiers, fax machines and scanners, and move to multifunctional devices that include all these functions. We are also optimizing cell phone and BlackBerry usage to reduce over and underutilization and zero use. We have expanded the use of Defense Connect Online vice modernizing VTCs and are looking to significantly reduce our legacy networks for integration into the enterprise network environment. We have also embarked on a very aggressive

effort to reduce the overall number of applications and systems within the Navy inventory.

Q: You mentioned at an AFCEA luncheon in February that the fiscal year 2013 cost estimate for information technology is \$11 billion; what does that include?

A: This was for the Department of Navy, not [just] Navy. There has not been any new money applied, the increase reflects a more accurate reporting of IT spending based on rules established by FMB (Deputy Assistant Secretary of the Navy for Budget).

Q: Regarding the 25 percent reduction in IT costs that CNO Adm. Greenert directed for FY13, will it be applied to the \$11 billion estimate?

A: Yes, in the areas mentioned in the first question and possibly more. This will be determined after the sequestration and CR (continuing resolution) matters are resolved.

Q: You indicated at the AFCEA luncheon that there are more than 210 Navy data centers maintaining 302 legacy and excepted networks and servers

and applications that were recently discovered, which were thought to have been consolidated under the NMCI, and there is little idea of the exact expenses of these operations. Why is that?

A: Navy has previously adopted a decentralized approach to IT execution. As a result, the Echelon IIs and IIIs [commands] established capability to support their internal environments vice aligning to the enterprise, and it resulted in duplication in many areas. Point of clarification: the excepted networks include our medical and RDT&E (research, development, test and evaluation) networks which are not, nor were they intended to be part of the enterprise. These are special environments, and we will consolidate within the Defense Department enterprise network environment as appropriate.

Q: What will be the process to consolidate these newly discovered IT assets since Adm. Greenert wants them to be migrated by 2014?

A: Legacy/excepted networks are now under review by the Navy Enterprise Information Technology Guidance Board (NEIGB). As such, all legacy/excepted

I ENVISION AN END-STATE THAT ALLOWS FOR THE SEAMLESS EXCHANGE OF DATA TO OUR PERSONNEL GLOBALLY USING NEW TECHNOLOGY WHICH REDUCES OUR REQUIREMENTS FOR HARDWARE AND FACILITIES YET DELIVERS THE INFORMATION RAPIDLY, SECURELY, AND WITHOUT ANY INTERRUPTION FROM OUR ADVERSARIES.

network owners (less medical and RDT&E) are presenting rationale as to why these networks should be retained and not migrated into the enterprise — the Next Generation Enterprise Network (NGEN) or One-Net. Thus far, the NEIGB has determined over 75 percent will be migrated into the Navy Marine Corps Intranet/NGEN due to maturation of the capability in the past seven years. This eliminates many of the Echelon II's previous concerns about the enterprise.

Q: How would you rate the success of the data center consolidation efforts across the Navy so far?

A: Good. Our most significant challenges thus far have been the identification of the total number of servers on-site and the use of these servers; end of life software; total number of circuits used at the site, and total number of personnel on-site involved in data center management, operations, etc.

Q: In setting up the new Navy enterprise data centers, is the Navy using a model that will also fit within the DoD's plan for data centers, and does the Navy have an efficiency target for how many centers will be needed and the costs to operate, including manpower, security and energy?

A: Yes, the overall Navy plan does fit into the DoD plan which is aligned to the Joint Information Environment and the Federal Data Center Consolidation Initiative. We have not yet released the

total number for our end-state as it is pending approval with the VCNO and ASN RDA (Assistant Secretary of the Navy for Research, Development and Acquisition). The final result for the end-state does account for manpower, security and energy, as well as other factors, such as transport and bandwidth.

Q: Consolidating the data centers offers a chance to innovate and possibly save more money in the long term – are there funds available to take advantage of this opportunity?

A: During FY11, when the U.S. Navy was directed to close and consolidate data centers, we allocated a percentage of funds for the actual effort which includes incorporating new technology in a cloud. Our initial plan is to migrate to an Infrastructure as a Service environment with future goals and efforts migrating to [a] Software as a Service [delivery model].

Q: You talked about an IT asset management tool to give commands a better way to manage their software licenses since this is another area that can achieve significant cost savings. Can you explain how the tool would work?

A: An IT asset management tool provides a critical component to not only data center consolidation but all application rationalization. It provides us data on the frequency of the use of a software product and a application; number of users; ability to shift software licenses which are not used; identify trends

relative to software and hardware use and challenges; security/IA issues; [ability to] plan for future procurements of hardware and software, and visibility into ensuring our IT spend aligns with the commodity use.

Q: Can you talk about long-range plans for improving the efficiency and effectiveness of Navy business IT systems?

A: Yes, as we prepare to implement the CNO's mandate for implementing a reduction of our overall IT spending, we will be establishing more governance in various areas such as IT procurements for contractor support services; hardware, enterprise software licensing, new capability development, portals for collaboration and websites, as well as streamlining the Echelon II command information officers reporting under the DDCIO-Navy. We have several others we are considering; however, these have not been vetted and approved by Navy leadership, so release of this information at this time is premature.

Q: As the representative of the DON Deputy CIO (Navy), is there an end-state for business IT systems that you envision?

A: Yes. I envision an end-state that allows for the seamless exchange of data to our personnel globally using new technology which reduces our requirements for hardware and facilities, yet delivers the information rapidly, securely, and without any interruption from our adversaries. ●

Cmdr. Steve Shedd Commanding Officer, USS Milius (DDG 69)

A key aspect of the Navy's modernization planning is upgrading cybersecurity, command and control, communications and electronic warfare capabilities for ships at sea. The Navy's next generation tactical afloat network is CANES – or Consolidated Afloat Network Enterprise Services. CANES is designed to provide standardization by reducing the number of network variants by ship class and across the fleet. In addition to reducing the system's total ownership costs for the Navy, Sailors will benefit by having greater familiarity with ship network configuration. The Program Executive Office for Command, Control, Communications, Computers and Intelligence – also known as C4I – is the Navy's lead for the CANES program.

"CANES is more than a system, it is also a new business model for delivering capability to the fleet," said Rear Adm. Jerry Burroughs, PEO C4I. "It takes five legacy networks and combines them into one network, allowing us to streamline support, training and operating procedures."

Since the first CANES installation kicked off in late December 2012 aboard the destroyer USS Milius (DDG 69), we wanted to get perspective about the process from the ship's CO, Cmdr. Steve Shedd. Cmdr. Shedd was interviewed in early March by Sandy DeMunnik, who provides communications support for PEO C4I.

Q: What work is being done with your ship right now?

A: Right now, the ship is in the middle of an extended drydock availability that's scheduled to last 10 to 11 months. During this availability we're scheduled to get a variety of hull, mechanical and engineering upgrades to the ship to extend its service life out to the expected 35 years. In addition to that, we're getting some C4I upgrades, from the Navy Multiband Terminal to the CANES installation.

Q: Can you tell me about the CANES installation?

A: The CANES installation is going to replace our legacy ISNS (Integrated Shipboard Network System) architecture for our local area network, and [it] gives us increased capability from an administrator standpoint. It will also refresh all our PCs and brings some increased effectiveness and efficiencies for the crew with the better PC load-outs we're going to get.

Q: Upgrading a network aboard a Navy ship is not like upgrading your network at home. Can you explain what the differences are?

A: The biggest difference in doing a PC or network upgrade at home as compared to a ship is the extensive industrial work that needs to go on throughout the ship. You can imagine the ship has numerous cableways throughout that we have to restring — all of the network cable, Cat 5 and fiber needs to be strung from scratch. We have ripped out all the old stuff, then we have to redo foundations for all the cabinetry and the racks that have to go in their place. In addition, we're also doing work to some ventilation units to increase our cooling capacity in a couple key spaces to accommodate the updated server racks.

Q: Isn't an updated Internet café also being planned?

A: Many ships are configured differently

throughout the Navy, and it depends on how they have gone through other availabilities and utilize spaces. Milius is unique because, several years ago, an Internet café was created out of one space and it's been a tremendous benefit to Sailors for quality of life. So in this space on the ship we have five computer workstations and the crew is able to go in their off-time and they're able to log in, using their normal network log-in, and do what they need to do from Facebook to off-ship email.

And I tell you what, we went on an eight-month deployment last year and the connectivity we had with home was absolutely phenomenal. The ability for my crew to communicate back home gives peace of mind, makes them happy and more productive on-station.

Q: What benefits do you see when CANES is on the ship?

A: I am excited about a couple of aspects that PMW 160 (Tactical Networks Program Office, Navy Program Execu-

tive Office C4I) has briefed us on. The first thing I'm excited about is our thin clients, or multidomain computer workstations, we're getting. That is a huge boost because I go from a workstation where I have three desktops to one desktop that will allow me to log-in to NIPRNET, SIPRNET and CENTRIXS (Combined Enterprise Regional Information Exchange System, the network for coalition communications), all from the same workstation. And that is real estate reduction, which on a ship is a key and essential because you don't have a lot of real estate for desktop computers.

Getting the toughbook laptops is a good thing because walking around a steel ship, up and down ladders with unprotected laptops, is not good for laptop survivability.

Another benefit is the ability to support non-governmental organizations by using virtual private networks to give NGOs access to the Internet without touching our LAN. That is a huge win for increased operational capability, and potentially we might be able to use that feature for quality of life aspects.

Lastly, I'm looking forward to having wireless connectivity within the skin of the ship to expand our LAN. We're limited in the number of LAN drops we can have, which can be frustrating. So having wireless access points where we can expand LAN usage does nothing but increase productivity on the ship, which is a win.

Q: How do you view the addition of the Navy Multiband Terminal?

A: NMT is the replacement of our existing EHF (extremely high frequency) antenna. It combines SHF (super high frequency), EHF and the Global Broadcasting System, so it brings us an increased ability to combine three separate antennas into one. This is also a real estate win with the limited space we have up on our superstructure.

Having one antenna in the place of three is certainly advantageous. With



SAN DIEGO (Jan. 23, 2013) Cmdr. Steve Shedd, left, commanding officer of the Arleigh Burke-class guided-missile destroyer USS Milius (DDG 69), discusses CANES installation on the Milius with Capt. D.J. LeGoff, the CANES program manager at Program Executive Office, Command, Control, Communications, Computers and Intelligence (PEO C4I). Milius is the first ship to receive the Navy's next generation tactical afloat network. U.S. Navy photo by Mass Communication Specialist 3rd Class Karolina A. Martinez.

that capability at sea, it appears we'll have a lot of functionality that we didn't have with our legacy EHF system; so we're excited to get that too.

Q: What would you tell other COs about where you're at in the CANES installation process right now?

A: Being the first ship to get CANES comes with responsibility on my part. My message to the rest of the fleet and fellow COs is that I've got their back. With any installation there will be some challenges, and I want to make sure that SPAWAR (Space and Naval Warfare Systems Command), with PMW 160 and PEO C4I, have looked at all the angles from an operator perspective. It's important for operators like me [to] provide good feedback about the CANES install, to capture those lessons learned so that we keep the warfighter's best interest in mind as we get this program going. I'm looking to positively impact future installations.

Q: Have there been any surprises thus far?

A: So far there have been no major surprises, but I want to explain the two separate phases. Number one, we have the industrial phase, and then we have the testing and integration phase. The industrial work is going on right now.

The second phase we're going to enter is in the June–July timeframe for the testing and integration, and I'm certainly concerned [about] how that goes. I'll be looking at that with great interest as we light the system off, incorporate other onboard systems and make sure we can operate like we did before. I know a lot of COs may be reticent to be the first ship for a new system install, but I'm all-in on being the first one. I enjoy the dialogue with the shore side and I want to ensure the operators' input is being heard early in the process. We'll ride the challenges through so the last installation down the road in 2020 or 2023 is just as good as the second installation based on our lessons learned.

Q: Is there anything you'd like to add?

A: The teamwork between SPAWAR and PMW 160 has been excellent. Milius has been afforded a lot of support from the right levels, and by the right levels, I mean at the O-6 level and up, to make sure we're afforded a voice to make this process work. The teams have been receptive to our requests, from small things like LAN drop locations to some larger things like VTC capability locations. So we're working through those minor issues, and the teamwork is absolutely critical. I think the worst thing a ship can do with a first install is to develop an adversarial relationship and assume that the shore-side isn't thinking about the best interest of the warfighter. Sometimes there might be a translation issue, but everybody has a common goal. That's to get this ship back out on station with increased capability, and CANES is certainly [a] multiplier in making that happen. ●



SAN DIEGO (Jan. 23, 2013) Cmdr. Steve Shedd, left, commanding officer of the Arleigh Burke-class guided-missile destroyer USS Milius (DDG 69), discusses blueprints for the Consolidated Afloat Networks and Enterprise Services (CANES) program with Capt. D.J. LeGoff, center, the Consolidated Afloat Networks and Enterprise Services (CANES) program manager at Program Executive Office, Command, Control, Communications, Computers and Intelligence (PEO C4I) command, and engineers. CANES seeks to streamline operations and reduce overall costs by using standardized technologies. U.S. Navy photo by Mass Communication Specialist 3rd Class Karolina A. Martinez.

CANES Keeps Pace with Technology Advances

Technology changes constantly. The hottest, latest, most innovative computer can become obsolete before the average user has even figured out all the bells and whistles. If the average user decides to upgrade, it's a fairly straightforward process: back up your data, unplug the old system and plug in the new system, load your data and you are all set.

According to Bart Lankard, a Space and Naval Warfare Systems Command ship superintendent, the process for upgrading Navy networks is a much more involved process.

"There is only so much real estate on a ship," explained Lankard, who is overseeing installation of the Navy's next generation tactical afloat network, CANES, or the Consolidated Afloat

Network and Enterprise Services, aboard USS Milius (DDG 69). While describing the intricate industrial work required to modernize a network aboard a Navy vessel, Lankard said, you have to disconnect the old system, unbolt it and remove it from the ship. Then a welder is brought in to cut out the existing foundation, which is a piece of metal in the deck that holds the rack to the deck of the ship.

"You have to transport [the new] rack through very tight spaces, without damaging it or the ship to get it to its space. Then you have to put the rack on its foundation and build what is called a swaybrace at the top of the rack. Then, you have to run all the cabling through the ship, from a power panel to the rack, or from workstations or a switch or a hub," he continued. "This is a very detailed process and if you multiply this by 17 or 18 racks it can be very difficult.

This is the first installation of its kind," Lankard said.

Lessons learned are being carefully collected to ensure that future installations are performed faster and more efficiently.

The guided missile destroyers USS McCampbell (DDG 85) and USS Chafee (DDG 90) are the next ships in class scheduled to receive the CANES installation. USS John C. Stennis (CVN 74) is the first aircraft carrier scheduled to receive CANES.

FOR MORE INFORMATION

To view a video of Cmdr. Shedd discussing the CANES installation on the USS Milius, visit: <https://www.facebook.com/PEOC4I#!/photo.php?v=582351821775816>

PEO C4I
WWW.PUBLIC.NAVY.MIL/SPAWAR/PEOC4I/

Storage of Paper Records Containing Personally Identifiable Information

THE FOLLOWING IS a recently reported personally identifiable information (PII) data breach involving the storage of paper documents containing PII. Incidents such as this one will be reported in each edition of CHIPS to increase PII awareness. Names have been changed or omitted, but details are factual and based on reports sent to the Department of the Navy Chief Information Officer Privacy Office.

The Incident

A Navy recreational office was burglarized after it was secured for the evening. The perpetrator broke into a locked file cabinet containing membership applications for 180 Navy personnel. The applications contained Social Security numbers and either a copy of a person's passport or birth certificate, which was used to verify citizenship.

Actions Taken

No files or personal property were stolen during the burglary. However, a breach report was submitted because of the potential compromise of personal information, and written notifications were sent to the 180 people who were affected. Further, leadership requested sample application forms from similar offices and reviewed all application processes to ensure conformance to Department of the Navy policy for safeguarding PII and improve application handling.

Lessons Learned

There are a number of lessons that others can learn from this incident and that apply to handling paper records and forms that collect PII. Paper records containing PII must only be accessible to those with an official need to know. In this example, the office and file cabinet were properly secured.

However, the form used by the office

was not an official Navy form. All forms that commands use to collect PII must be an official form. This means commands must follow procedures established by the DON CIO, as the Senior Military Component Official for Privacy. Forms must be reviewed by a forms manager and privacy official, and if approved they are assigned a form number. The form must include a Privacy Act Statement and the specific authority that allows PII to be collected. Finally, the form must be registered and posted to the Naval Forms Online website (<https://navalforms.documentservices.dla.mil/>). For additional information, please contact your command forms manager or OPNAV DNS-51 at (703) 614-7585.

There are other considerations as well. The collection of PII may require

collection of SSNs is required, then a document justifying the collection must be developed and signed by a flag officer, a civilian senior executive or an individual given by direction authority. More information on the DON SSN reduction process is available at www.doncio.navy.mil/contentview.aspx?id=1912.

Minimize the collection of PII wherever possible. The Navy office in the example was collecting SSNs and verifying citizenship for members by maintaining a file copy of either their passport or birth certificate. The Department of Defense ID number or other unique identifier should be used in place of SSNs whenever possible. And while passport or birth certificate information should be confirmed, there is no need to keep a copy on file.

BREACH NOTIFICATIONS NOT ONLY COST THE DEPARTMENT SCARCE RESOURCES ... BUT ALSO HAVE THE POTENTIAL TO UNDERMINE MORALE AND TRUST IN THE ORGANIZATION.

a System of Records Notice (SORN). Please contact your command privacy official or the OPNAV DNS-36 Privacy Act Branch at (202) 685-0412 to determine if a SORN is required.

If you are collecting personal information on 10 or more members of the public in a 12-month period, the form may also require Office of Management and Budget approval and an OMB control number. To determine if an OMB control number is required, contact OPNAV DNS-51 at (703) 614-7585.

If the form collects SSNs, it must go through the SSN reduction review process established by the DON CIO to reduce the use of SSNs in business processes under the department's control. If it is determined that the continued

Finally, paper copies of the application could be scanned and filed electronically, eliminating the need to keep hard copy documents in file cabinets.

PII breaches not only cost the department scarce resources, such as time and money, but also have the potential to undermine morale and trust in the organization. Additional privacy resources can be found at www.doncio.navy.mil/privacy. ●

STEVE MUCK is the Department of the Navy privacy lead.

STEVE DAUGHETY provides support to the DON Chief Information Officer privacy team.



DON'T GET CAUGHT

BY

SPEAR PHISHING



BY STEVE MUCK

PHISHING IS A CRIMINAL ACTIVITY in which an adversary attempts to fraudulently acquire sensitive information by impersonating a trustworthy person or organization. A rising cyber threat called spear phishing takes this email threat to a new level.

Instead of sending thousands of emails to random recipients hoping a few will respond, spear phishing targets select groups of people with something in common. For example, they may work at the same organization, bank at the same financial institution, attend the same college, or order merchandise from the same website. The fraudulent emails are supposedly sent from organizations or individuals that the potential victims would normally receive emails, which make them even more alarming because the perpetrators already know specific information about the potential victims.

Spear phishing emails may contain personal data such as a person's name, phone number, address or work-related information. For cyber thieves, the ultimate goal is to extract personal information to commit identity fraud.

How spear phishing works

First, cyber criminals need some inside information about their targets to convince these potential victims the emails they are sent are legitimate. The criminals often obtain this information by combing through websites, blogs and social networking sites where unsuspecting users reveal personal details of their lives.

Once they have obtained enough information, the criminals send emails that look legitimate to the recipients, requesting personal data by offering urgent and realistic explanations as to why they need it. Finally, the victims are told to click a link in the email that takes them to a phony but realistic-looking website, where they are asked to provide passwords, account numbers, usernames, access codes and personal identification numbers. Once criminals have this type of personal data, they can access bank accounts, use credit cards, and create a new identity using the stolen information.

Spear phishing can also trick victims into downloading malicious code or malware after they click on a link embedded in the email. This is an especially useful tool in crimes such as economic espionage where sensitive internal communications can be accessed and trade secrets stolen. Malware can also hijack computers, which can then be organized into enormous networks called botnets that can be used for denial of service attacks. The most commonly used files in spear phishing attempts are: .RTF, .XLS and .ZIP.

Do not become a spear phishing victim

Take these precautions:

- Most companies, banks, agencies and other legitimate businesses do not request personal information via email. If in doubt, contact the business, but do not use the phone number provided in the email.
- Never click a link embedded in an email. Enter the URL manually in a browser.
- Never open attachments from strangers.
- Tell friends and co-workers to notify you before they send an attachment. This will reduce your risk of becoming an identity theft victim.
- Never assume that because you know the address from which the email was sent that it is safe.
- Always monitor personal financial accounts and check credit reports.

Report spear phishing

It is important to report incidents of spear phishing attempts and successes to the Federal Trade Commission (FTC) at www.ftc.gov/complaint. The FTC maintains a secure online database that is used by law enforcement authorities worldwide. Such reports help authorities determine patterns of behavior, which lead to investigations and prosecutions.

The Navy Marine Corps Intranet email exchange servers have anti-spam filters to keep spear phishing to a minimum. However, when a suspected spear phishing message is received, send it with the word "SPAM" in the subject line, including the original header information, to: NMCI_SPAM@navy.mil for Navy users or usmc_anti-spam@nmci.usmc.mil for Marine Corps users.

Spear Phishing Resources

The following list of resources provides additional information about spear phishing:

- Federal Bureau of Investigation news article regarding spear phishing: www.fbi.gov/news/stories/2009/april/spearphishing_040109.
- FBI newsletter regarding electronic scams: www.fbi.gov/scams-safety/e-scams.
- Federal Trade Commission news article on phishing: www.onguardonline.gov/articles/0003-phishing. ●

STEVE MUCK is the Department of the Navy privacy lead.

Rear Adm. David G. Simpson

Vice Director, Defense Information Systems Agency

As vice director of DISA, Rear Adm. Simpson helps lead a worldwide organization of military and civilian personnel responsible for planning, developing, and providing interoperable, global net-centric solutions that serve the needs of the president, secretary of defense, Joint Chiefs of Staff, the combatant commanders, and other Department of Defense components.

CHIPS spoke with Rear Adm. Simpson March 29, 2013.



Rear Adm. David G. Simpson

Q: Reaching the one-million users mark for DoD enterprise email is quite an achievement. Is the process of moving users to Enterprise Email going more smoothly now? I understand that there were some issues in the early stages of roll-out.

A: Thanks for asking, this is a good opportunity. Let me start with talking a little bit about what Enterprise Email is. It's just passed the one-million mark — we actually flew right through it and we're at 1.1 million unclassified users. About 18 months, after we started the unclassified system, we started the classified system and are providing service for over 60,000 SIPRNET users. We will deploy an enterprise mobility capability that is part and parcel with the Enterprise Email capability. [It includes] 80,000 BlackBerry mobile devices, 700 smart devices — those are Apple and Android tablets and smart phones. Next week we deliver the first of 500 secret SIPRNET mobile phones that can actually be accredited up to the top secret level.

The first classified mobility device goes to Deputy Secretary of Defense Ashton Carter. So, it's important that

we really get a sense of the universe of enterprise services to appreciate the synergy from their deliberate integration. This integration allows users to communicate, not just via email, but via calendaring (ability to share calendars across the DoD), collaboration, via identity management, global directories and unified capability (VoIP and video). Users have mobile access to those capabilities as well as applications that have only, at this point, been available in the fixed environment.

When we first rolled out enterprise email, we had a very good product, and a good team that understood how to implement the product. We had organized around running networks for tens of thousands of users. When we got to about 60 or 70,000 users, we recognized that the team was not structured to optimize for the full scale of the endeavor.

Navy information professionals understand how critically important IT service management is, and DISA employs ITIL v.3 (Information Technology Infrastructure Library version 3) for our DoD enterprise security management framework, so while we had the right framework in mind, we had not task organized to our own target framework.

So we took a two-month pause in the creation of new accounts. In that two months, we did a deep dive focused on process improvement, and what we recognized is that we had not implemented our own ITIL objectives.

So we needed to break up our processes that had co-mingled, incident management and problem resolution, capacity management, change management, and really define workflow associated with each of the process lanes and the process owners. So in doing that, DISA greatly improved the service.

We also recognized that our partner organizations were a key part of the service framework. There's an element of tier one that is a partner organization responsibility; similarly at the high end, tier four, (problem resolution) there is an element of service that periodically requires our vendor partners to be engaged. We worked with all of our partners to align our enterprise service management framework so that we had one incident management process between us and systematically addressed process definition and implementation.

We worked to develop service level agreements and operational level agreements together so that expectations were clear and execution was

This mission first and foremost is to ensure that we provide a service to meet warfighter needs. It's got to be there with the right information at the right time in a reliable, robust and resilient manner. It has to be defensible against committed adversary attack.

crisp. That two-month pause allowed us to resume migrating users right out of the gate; in some months, 80,000 to 90,000 users a month.

Currently the Army, Joint Staff, EUCOM (U.S. European command), AFRICOM (U.S. Africa Command), Navy recruiters, and several other agencies have switched to Enterprise Email. We are working to onboard additional services and agencies. I think it's also important to recognize that we built this service in a way that did not repeat some of the shortfalls of previous DoD enterprise intranets. Specifically, an important core tenet was to maintain government command and control over all aspects of the service. The agency must be able to assess risk to prioritize corrective action based on that risk, to recognize opportunity, and to be able to direct the activities of the entire team even while under a committed adversary attack. So not only did we need to get the service management framework optimized for service levels, we also needed to build the kind of command and control commensurate with the level of adversary threat we expect in the future.

Q: What is the response of the users once they migrate to the Enterprise Email System? It sounds like things have been going very well.

A. They have; it's been very positive. First on the Navy side, let's just pick a niche here. Rear Adm. Earl Gay, who leads Navy Recruiting Command, had a real issue facing him in that his workforce — the recruiters — are a very

mobile workforce. They were regularly being locked out of their email capabilities on the road because of limitations in storage and aspects of the service that weren't as mobile as they needed to be. When he looked at what the NMCI (Navy Marine Corps Intranet) contract line items would cost to upgrade the services for all the recruiters, it wasn't in his budget. He heard about DoD Enterprise Email and found that the cost of the entire Enterprise Email account would be less than the cost to increase the NMCI memory capacity for each of the recruiters. He was able to switch them to [DoD] Enterprise Email and achieve lower cost and increased capabilities. The recruiters have been very well supported by that.

I spoke to Rear Adm. Gay when we went over 1 million users; I wanted to make sure that there wasn't any degradation in his service level. His 5,000 recruiters have been on it now for seven or eight months meeting all missions. We get that same response from all levels of the department.

DISA is responsible for DoD's communications for the President through the White House Communications Agency. We also provide enterprise email today to the Chairman of the Joint Chiefs of Staff, the Vice Chairman and all of the Joint Staff users. We are quite sure that the chairman wouldn't be shy if the service didn't meet his expectations. Similarly, the Secretary of the Army, Chief of Staff of the Army, deployed forces in Korea, Japan and Southwest Asia have all given us high marks. They enjoy the flexibility to access the same service anywhere around the world.

We also work closely with AFRICOM and EUCOM as we bring the Joint Information Environment together. Enterprise Email is providing organizations that were strapped for money and people a cost-effective way [for] addressing the continuously increasing computer network defense requirements.

Q: What is the vision for the DoD Enterprise Email System for continued deployments and what are the projected cost savings and efficiencies for continued deployment? How does DEE fit in with the DoD Chief Information Officer's and DISA's plans for the development and deployment of enterprise services across the department?

A. This mission first and foremost is to ensure that we provide a service to meet warfighter needs. It's got to be there with the right information at the right time in a reliable, robust and resilient manner. It has to be defensible against committed adversary attack. We will continue to work under U.S. Cyber Command to make sure that Enterprise Email has the very best our nation has to offer in the way of cyber security. We must be able to spot anomalous activity and correlate that activity to identify a potential attack so that we can contain and prevent its lateral spread. Then we must bring to bear the whole weight of our operations and intelligence communities to characterize those attacks, and when appropriate, generate active responses to those attacks.

Second, DEE will be the linchpin for bringing the department's collaborative

capabilities together. I believe that as we go forward, there will not be an appetite for continuing to have multiple enterprises within DoD. We will be providing a service that the world is increasingly comfortable with — having email as a part of the cloud.

Many of us are familiar with Gmail and other kinds of cloud-based email systems. They're very reliable. Shifting the resiliency for our military email system, from a server that has to go with you wherever you are and maintained in a building where you're at because you're potentially disconnected at times to one in which we regularly engineer route diversity and the ability to work around outages in the transport layer because we've designed it with the 99.99 percent of network access that many missions truly require, has enabled a whole new way to look at email in the future.

So instead of doing multiple enterprises at scale — one for the Army, one for the Air Force, one for the Marines, one for the Navy and then once again for the DoD components and COCOMs, I absolutely believe the right thing to do is to do it once for DoD so that each of the services can optimize their resources around their tactical information environment. The tactical edge is where we really want to be focusing Navy and Marine Corps dollars, around our unique tactical platforms.

We have already achieved significant cost savings for the department. The charge for Enterprise Email since we first started the project has been \$39 dollars per user, a year. Thirty-nine dollars per user a year! And it hasn't changed since we began. DISA is a working capital funded organization. We have to abide by the statute in the way we're set up and that is to recover all the costs that we spend. We're in a very good position to hold that pricing. I know that as we continue to add volume, we'll continue to lower the cost of running the service.

DoD Chief Information Officer Ms. Terri Takai has set a very progressive agenda which takes advantage of the latest technology for the department. It centers around things like cloud services, data center consolidation,



Rear Adm. David G. Simpson at Joint Test and Evaluation, Suffolk, Va., Jan. 12, 2012.

enterprise mobility and unified capabilities (eliminating legacy telephony and video services). Enterprise Email is very well-suited to multiply the advantage from all of those initiatives.

Enterprise directory services is an example where the move to Enterprise Email automatically adds value for other enterprise service offerings. Our mobile devices (BlackBerry, Android, Apple iOS and Windows 8) utilize the same directory as our email system, phone and video system and our portals. Pulling together the same directory for all of these areas enables additional collaborative capabilities that weren't there before in directories built independently by each organization.

Under the fully realized joint information environment, the ability now to have your phone be the computer on your desk, and have phone calls made to your organization, recognize that you're not there, see where the device is and then route the phone call to wherever you might be throughout the battlespace is a very important capability.

If you're not there, the message that the system takes in unified capabilities then becomes email accessible from Enterprise Email or enterprise mobility and is archived within the connected

portal structure. That's part of the CIO's vision in the Joint Information Environment, that we multiply the advantage from each of these capabilities to gain synergy from the investments while improving the defense.

We're able to now see and correlate anomalous activity across each of these lanes. The value isn't just in the single product, Enterprise Email, for example, it is in the synergy between each of the different products and services of the JIE and the ability to defend in a much more effective and efficient manner.

Q: The DoD Mobile Device and Commercial Mobile Device (CMD) Implementation Plan encompasses three goals to achieve: improve infrastructure, implement mobile device management (MDM) policies and develop mobile Web-based applications. There are 16 ongoing component mobility pilot programs; can you talk about how the pilots are progressing?

A. I think that the pilots are progressing well. Each of our partners had specific goals in wanting to understand how mobility would better advance their missions in a specific area. They're op-

The charge for Enterprise Email since we first started the project has been \$39 dollars per user, a year. Thirty-nine dollars per user a year! And it hasn't changed since we began. DISA is a working capital funded organization. We have to abide by the statute in the way we're set up and that is to recover all the costs that we spend. We're in a very good position to hold that pricing. I know that as we continue to add volume, we'll continue to lower the cost of running the service.

erating the pilots in a way that informs the entire group with best practices and observations to the operational environments for the 16 different pilots. Next steps include stand up of enterprise mobile device management and its mobile applications store. Many of the pilots will then join the enterprise, bringing best practices with them.

A couple of the pilots really are oriented toward how we ultimately expect to bring enterprise mobility into the tactical information environment. A good example of that is Navy's (Long-Term Evolution) LTE pilot on the USS Kearsarge and the USS San Antonio. Imagine setting up a cellular network (4G) afloat that connects to all of those capabilities I just described — unified capabilities, cloud services, mobile app store and email — collaborative products. That's a huge capability that will revolutionize the way that we communicate. I think we'll see the number of pilots reduced in the upcoming months to years and the remaining pilots will really focus on the tactical edge.

Q: What are you learning from the pilots?

A. Some of what we're learning is important. First, let me talk about the challenges. There are a number of

competitors in mobility in the commercial sector. BlackBerry, Apple, and iOS products, Android and Windows 8 on the Microsoft side are competing vigorously, and all are working to roll in technology to gain advantage over one another. That's one of the reasons why when we pulled together enterprise mobility, we established, from the very beginning, the principle that we would be establishing a management platform that is vendor agnostic so we would not have a big competition for any one vendor only to later regret that we missed out on the next technological improvement. Instead, we defined the platform in a way where the onus is on the vendors to upgrade their products into that single departmentwide mobile ecosystem.

That's been very successful, and we've got all four product lines up and running. We are surprised, frankly, about how much interest there has been from each of the vendors. When we first started out, there were some critics that said, 'Well, DoD is such a small market, commercial providers of public technology won't want to change anything they're doing to accommodate a DoD-run enterprise.'

The exact opposite has happened, and we have mobile companies really seeking to partner with DoD mostly

because of the security challenges that their non-DoD customers are facing. In working with NSA (National Security Agency) and DISA at the early stages of their product lines, they're finding they're able to work on capabilities with DoD in a manner that improves their products — improves the industry in a mutually satisfying way.

Q: Is there anything else you'd like to talk about with us?

A. I always like to talk about the opportunity for Navy to improve collaboration across the joint force; to improve the Navy's leverage of 'purple' joint investments, to benefit from the defensive cyber orientation that is designed at DISA from the beginning with CYBERCOM, NSA and our service partners. There's great potential for Navy to benefit from DOD-wide services, and optimize Navy work in IT around our unique platforms and the maritime information environment. ●

DOD ENTERPRISE EMAIL

<http://www.disa.mil/Services/Enterprise-Services/Applications/DoD-Enterprise-Email>

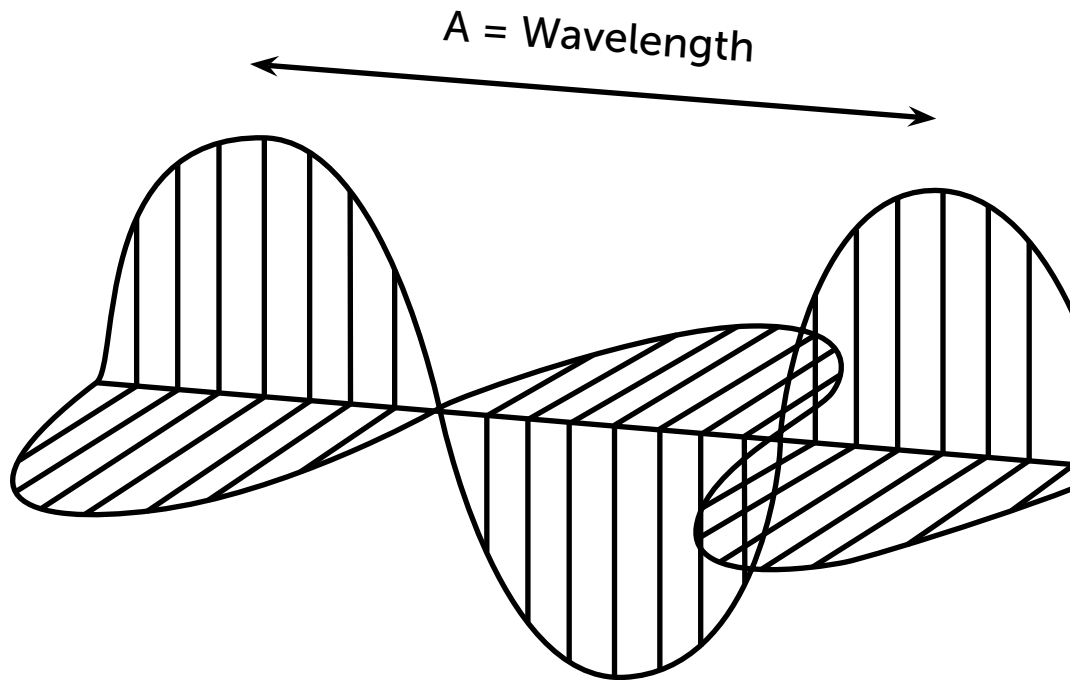
Making Waves: Radio Spectrum a Vital Resource for Mission Success

W E LIVE IN a radiant world. Natural cosmic and man-made radio waves flood the atmosphere around the world on a daily basis. These invisible and quiet waves are an important and integral part of our lives. Most people are heavily dependent on them to communicate with others, access electronic devices, and operate remote-controlled technology.

The entire electromagnetic spectrum cannot be seen by the human eye — only visible light is detectable. An electromagnetic field is generated when an alternating current is input into an antenna. Created by vibration or oscillating electric and magnetic fields, electromagnetic radiation consists of a stream of photons traveling silently in the form of waves moving at the speed of light. The electromagnetic spectrum cannot be heard. A wave is called electromagnetic because it is made up of two parts: an electric field and a magnetic field.

The only difference between the various types of electromagnetic radiation is the amount of energy generated. Radio waves have photons with low energies, microwaves have a little more energy than radio waves, and infrared light has still more energy. Moving up in energy level is visible light, ultraviolet light, X-rays, and the most energetic of all, gamma rays. The higher the radio wave frequency, the shorter its wavelength and the greater its energy.

As energies travel, they produce a unique wavelength with a frequency that can be identified and measured. Frequency is measured in hertz while wavelength is measured in meters. A wavelength is the distance from crest to crest between two peaks of a wave. A frequency is the time interval between passing peaks. The greater the



Electric and magnetic fields traveling at right angles form an electromagnetic wave.

length of the wave, the lower its frequency and energy will be. The shorter the wave, the higher the frequency and energy will be.

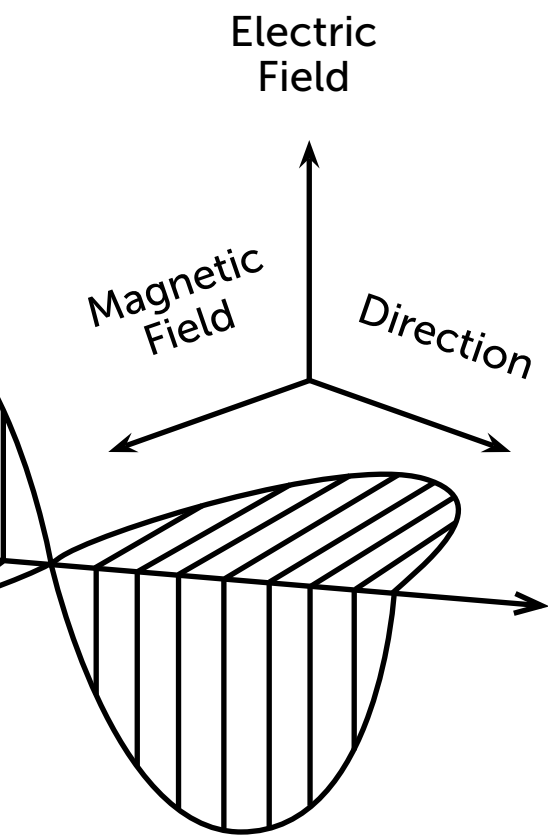
Radio waves have the longest wavelengths in the electromagnetic spectrum. These waves can be longer than a football field. The longest waves are several kilometers in length. The shortest radio waves are millimeters long while gamma rays measure less than the diameter of an atom. The radio frequency (RF) spectrum has several unique properties.

- ➔ It is free; it does not cost anything to use it.
- ➔ It is finite; there is a great deal of competition and demand for it.

- ➔ It is not consumed or destroyed when used.
- ➔ It is wasted when it is not being used.

RF spectrum is a vital and limited national resource, and the U.S. federal government makes extensive use of it for electronic communications and transferring data and information.

The use of the RF spectrum is regulated. Access is controlled and rules for its use are enforced because of the possibilities of interference between uncoordinated uses. Managing the RF spectrum can be a great challenge. Internationally, it is allocated by the International Telecommunication Union (ITU)



RADIO WAVES HAVE PHOTONS WITH LOW ENERGIES, MICROWAVES HAVE A LITTLE MORE ENERGY THAN RADIO WAVES, AND INFRARED LIGHT HAS STILL MORE ENERGY.

to various classes of service according to different regions of the world. Within the United States, the RF spectrum is further allocated between nonfederal government and federal government users.

The Federal Communications Commission (FCC), acting under the authority of Congress, is responsible for the allocation and assignment of frequencies to nonfederal government, civil and commercial users, as well as state and local government agencies. The FCC decides who is able to use specific frequencies for specific purposes, and it issues licenses to stations for specific frequencies.

The National Telecommunications and Information Administration (NTIA), which is an operating unit of the

Department of Commerce and an Executive Branch agency that is principally responsible for advising the president on telecommunications and information policy issues, administers the allocation and assignment of frequencies to departments and agencies of the federal government such as the Department of the Navy, Federal Aviation Administration and the Federal Bureau of Investigation.

Coordination between nongovernment and government users of the RF spectrum is accomplished by joint meetings of the FCC and the NTIA. The NTIA is also responsible for maintaining the National Table of Frequency Allocations. The NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management is the guidebook for frequency authorization in the United States, its possessions and territories.

The use and access of the radio spectrum are fundamental to the government, military and warfighter to accomplish core missions across all functional and operational areas. The military is heavily dependent on the RF spectrum to communicate essential and urgent

information and data instantaneously.

The government and military are required to manage the spectrum by planning, coordinating and managing the use of the RF spectrum through operational engineering and administrative procedures, policies, standards and directives. The objective is to enable spectrum-dependent equipment and capabilities to perform their functions in the intended electromagnetic operational environment while avoiding harmful RF interference.

The future role of the United States as a superpower and its assured victory in conflicts are dependent on how it makes use of the electromagnetic spectrum, and how it commands and controls this valuable, finite, congested and contested natural resource. ●

ZAID YACU is the electromagnetic spectrum manager for SPAWAR Systems Center Atlantic.

THOMAS KIDD is the lead for strategic spectrum policy for the Department of the Navy.

Rear Adm. Brian B. Brown Commander, Naval Meteorology and Oceanography Command

In August 2012, Rear Adm. Brian B. Brown assumed duties as commander of the Naval Meteorology and Oceanography Command (NAVMETOCOM).

Operational oceanography enables the safety, speed and operational effectiveness of the fleet by illuminating the risks and opportunities for naval and joint forces posed by the present and future natural environment.

Operational oceanography includes: oceanography, bathymetry, hydrography, meteorology, geophysics, astrometry and precise time.

Rear Adm. Brown responded to questions in writing in late February.



Rear Adm. Brian B. Brown

Q: Can you discuss how operational oceanography enables the warfighter?

A: The Navy's operational oceanography program focuses on generating competitive advantage across the physical maritime warfighting domain by providing our commanders a deep understanding of the current and future conditions of the battlespace to enable force maneuver, effective platform, sensor and weapon systems employment, and operational safety. As the Navy's physical science team, our highly educated Sailors and civilians measure and collect meteorological, oceanographic, hydrographic and other data relevant to the physical battlespace. They use the data to analyze and determine current conditions, forecast the future state, and provide mission-focused impacts that enable commanders to make well-informed operational decisions across the entire spectrum of warfare.

Operational oceanography operates along eight distinct lines of operations: maritime operations, aviation operations, fleet operations, navigation, precise time and astrometry, expeditionary warfare, anti-submarine warfare,

and mine warfare. Maritime operations enable the safe operation of ships and submarines at sea through individualized forecasts, monitoring of their movement relative to hazardous weather, and alternate route advisories as warranted. Aviation operations are similar, but focus on the safe navigation of aircraft. Fleet operations represent our oceanography forces deployed on aircraft carriers, amphibious assault ships, independent deployers and task forces. Navigation enables safety of surface and subsurface navigation through hydrography.

Precise time and astrometry are foundational to the battlespace framework we use and support the Global Positioning System, networks, communications, and space-based systems. Expeditionary warfare (amphibious warfare, riverine warfare and special operations), anti-submarine warfare, and mine warfare (offensive mining and defensive countermeasures and clearance), as their names imply, support their respective warfare areas via a mixture of forward-deployed and reach-back capabilities.

Q: I understand that operational oceanography is

multidisciplinary, incorporating physical oceanography, meteorology, hydrography, geophysics and precise time and astrometry. Could you discuss how each discipline is important to naval operations?

A: Yes, operational oceanography encompasses a number of scientific disciplines that are based in the physical sciences. To understand and predict the future state of the physical battlespace, expertise in physical processes from the sub-atomic level to the entire expanse of the universe is required, with specific focus on geophysical and fluid processes in the maritime domain.

Since the Navy operates globally under, on, and above the world's oceans, from blue water to the littorals, operational oceanography maintains expertise in geophysics (sea floor sediments and morphology), hydrography (ocean depths, navigation hazards), physical oceanography (ocean properties and motion to include currents, tides, waves, sea ice formation, and underwater acoustics), and meteorology (atmospheric properties and motion to include severe weather, tropical cyclone forecasting, and the electromagnetic

Naval oceanography is a key enabler of the Navy's information dominance strategy ... The strategic tenants of ID concentrate on providing the warfighter with assured command and control capabilities, enhanced cyber and electromagnetic kill capabilities integrated with more traditional kinetic kill capabilities to broaden warfighting options, and to provide predictive, battlespace awareness across all warfighting areas.

spectrum). These disciplines are underpinned by our precise time (precision atomic clocks), astrometry (celestial reference frame mapping), and earth orientation (the time-varying alignment of the Earth's terrestrial reference frame with respect to the celestial reference frame) missions that enable our geospatial reference framework and support our national and Department of Defense space-based environmental collection capability (electro-optical and infrared weather satellites, altimetry, sea surface temperature, radar imagery for sea ice).

Additionally, our time, astrometry and Earth orientation missions directly support national and DoD networks, communication systems, navigation, targeting, platforms and weapon systems. We tie these disciplines together to provide the Navy and joint forces with an unparalleled view of the current and future maritime battlespace so our commanders can make better operational decisions regarding force maneuver and employment faster than the adversary.

Q: NAVMETOCCOM employs a concept called Battlespace on Demand to aid in operational decision making. I discussed the concept briefly with your PAO; she said graphically, the concept is depicted as a pyramid with a base (0) and three tiers. Can you describe how the BonD concept aids warfighters and operational commanders?

A: Battlespace on Demand is an operational concept that we use to describe how the Navy operational oceanography program is aligned to provide the warfighter with superior knowledge of the physical maritime battlespace. Through our work with our warfighting partners, we have developed a deep understanding of the decisions they are required to make based on the physical environment to ensure the effective and/or safe employment of their capabilities. These decisions serve as the basis for BonD.

We describe BonD as a pyramid (or value chain) and with the decision space at the top with distinct layers or tiers that move us from data to decision. Briefly, these tiers are described below:

- Tier 0, the foundational data layer, in which data from various sources are collected, assimilated and fused to provide initial and boundary conditions that accurately describe the current ocean and atmosphere environment, as well as the celestial and temporal reference frames.
- Tier 1, the environmental layer, where the data from Tier 0 is quality controlled, analyzed and processed using our unique high performance, scientific computing capabilities. It is in this tier where we run world-class atmospheric and oceanographic numerical models to continually forecast and verify the future state of the ocean and atmosphere.
- Tier 2, the performance layer, takes into account how the environment

modeled in Tier 1 will impact sensors, weapons, platforms and people. Tier 2 incorporates the influences of planning, force structure, targeting, timing, maneuver, tactics, techniques and procedures. The result is a 'performance surface' that accounts for both the predicted environment and the capabilities and behaviors of the force — both allies and adversaries.

- In Tier 3, the decision layer, performance surfaces are applied to specific decision-making processes to quantify risk and opportunity at strategic, operational and tactical levels to provide timely and mission-specific courses of action for the warfighter. We strive to rapidly transition technology into operational capabilities that enable the decision layer.

In application, we work closely with our warfighting customers to understand their decision space and then execute our operational oceanography program using the BonD construct to give the customer the best courses of action and ensure mission success. BonD helps us ensure the highest return on investment for every dollar invested in the program.

Q: NAVMETOCCOM has some unique collection capabilities at the BonD Tier 0 level. Can you describe some of them?

A: Certainly! We leverage national and international data sources like satellites,

oceanographic buoys, expendable bathythermographs, surface observing systems/networks, and other sources of critical environmental data. In addition, we maintain world-class, and in some cases, unique capabilities to collect oceanographic, meteorological, hydrographic and astrometric data.

In consonance with the Military Sealift Command (MSC), we execute the scientific mission of six multimission military oceanographic survey vessels designated as T-AGS. The six ships of the USNS Pathfinder (T-AGS 60) class (with a seventh currently under construction) are continuously forward deployed and conduct hydrographic, oceanographic and acoustic surveys in all the oceans of the world. Their science teams are comprised of civilians and military from the Naval Oceanographic Office and are operated by civilian mariners under contract to MSC. These ships have modern full ocean depth multibeam and single-beam sonar systems for accurately measuring bottom depths and features, towed side-scan sonar systems for acoustic imaging of bottom features and navigation hazards, ocean current profilers, sub-bottom profilers for measuring stratification of seabed sediments, and over-the-side devices that collect physical ocean parameters such as temperature and salinity with depth.

These ships are capable of hosting a number of roll-on/roll-off systems, including systems for collection of seismic data and unmanned underwater vehicles. The ships are also equipped with C-band communications to send data directly back to the Naval Oceanographic Office for immediate processing and use in BonD. Three of the ships are complemented with hydrographic survey vessels — smaller craft for shallow water hydrographic collection.

We have been operating unmanned underwater vehicles (UUVs) for well over a decade. Our inventory consists of propelled vehicles, such as various models of the Remote Environmental Monitoring Units (REMUS) UUV for collection of sonar, sub-bottom and optical data, in addition to buoyancy controlled, high endurance UUVs, such as the Slo-



The Navy DoD Supercomputing Resource Center (DSRC) is home to three IBM iDataPlex supercomputers with a total theoretical peak performance exceeding 954 teraflops (trillion calculations per second). This world class scientific computing environment provides the capability for DoD scientists and engineers to accelerate delivery of new technologies and for the Naval Meteorology and Oceanography Command to deliver oceanographic products that support the safety, speed and operational effectiveness of the fleet. Photo courtesy of Navy DSRC by Lynn Yott.

cum glider and wave-powered Sensor Hosting Autonomous Remote Craft (SHARC) vehicles, which collect and transmit ocean and atmospheric data in real time for satellite transfer back to our operational production centers. In addition, we use UUVs for direct support to operation missions, like mine countermeasures, where we not only characterize the battlespace but conduct mine hunting/find and fix missions as part of the warfighting team.

As part of our hydrographic capability, we also employ unique jet ski variants we call 'expeditionary survey vehicles' or ESVs. Outfitted with single-beam and side-scan sonar, in addition to accurate Global Positioning System navigation, ESVs can be rapidly deployed and conduct hydrographic survey into the surf zone, to places where traditional systems can't go. This data is extremely useful for supporting expeditionary warfare and enabling missions like humanitarian assistance and disaster relief. ESVs proved extremely useful for getting supplies to the beach in the aftermath of the Haiti earthquake in 2010.

Lastly, we also employ a unique

airborne hydrographic survey capability called the Coastal Zone Mapping and Imagery LIDAR (CZMIL) system. Using laser technology, in the right water conditions, CZMIL can rapidly survey the near-shore region, both topographically and hydrographically to safety of navigation specifications in water depths of up to 50 meters.

Q: NAVMETOCCOM is headquartered at the Stennis Space Center, which is home to the Navy Department of Defense Supercomputing Resource Center that Navy, Army and Air Force scientists and researchers use to design tools and weapons systems that support DoD's global mission. I understand the DSRC recently completed a significant upgrade. What is NAVMETOCCOM's role with DSRC, and can you talk about what the new systems will mean to the Navy and DoD?

A: The Navy DSRC is a premier provider of high performance computing services and support to DoD scientists and engi-

neers. It is one of five supercomputing centers established under the DoD High Performance Computing Modernization Program (HPCMP). CNMOC maintains oversight of the Navy DSRC systems that have been operational since 1997.

The Navy DSRC provides a high-performance computing capability with primary emphasis on support of the largest, most computationally-intensive HPC applications. Our center leads the way for numerous HPCMP-wide initiatives and provides our users with in-depth computational expertise and support.

While the HPCMP is primarily focused on DoD research and development programs, the Navy DSRC is unique in that approximately 15 percent of its total capability is apportioned for operational use by naval operational oceanography. Today, the Navy DSRC enables, on a daily basis, operational, global, regional and port scale ocean circulation, [and] wave and sea ice forecast numerical models supporting worldwide Navy and DoD operations. Of note, our global ocean forecast capability only became a reality a few years ago as the Navy DSRC's computational capacity reached the 200 trillion floating point operations per second (teraflops) level.

This year, the Navy DSRC's total computational capacity reached over 950 teraflops. This affords us computational space to not only improve our ocean models, but to bring online world-class atmospheric models within the DSRC and begin to more tightly couple ocean and atmospheric physics and energy exchange to provide a more accurate, longer range future state of the atmosphere. It is truly exciting times to be in our business.

Q: It is astonishing what NAVMETOCCOM can accomplish given its small footprint, forward robust reach-back and a combined military-civilian workforce. How is the command organized and what are its contributions to the Navy, DoD, the nation and the international community of nations?

A: Operational oceanography delivers our products and services through a small embedded footprint forward with the fleet and robust reach-back capability ashore through our highly educated, professional civilian and military workforce.

Under the guidance of the Naval Oceanography Operations Command and its subordinate commands, small teams of aerographers' mates (AGs) and oceanography officers embed forward with the mission commanders in units, such as aircraft carriers, destroyer squadrons, Navy Special Warfare Teams and mine countermeasures squadrons, and provide the essential link between our capabilities and operations. They also leverage reach-back to operational production centers, like the Naval Oceanographic Office or Fleet Numerical Meteorology and Oceanography Center, for obtaining products. This allows our forward-deployed teams to effectively employ the expertise of our CONUS-based, largely civilian scientific workforce and our high-performance scientific computing capabilities. Our civilian team contributes Ph.D. level expertise to warfighting problems while our military professionals contribute their operational forecasting experience and an insight into Navy operations, platforms and weapons systems. It's a great pairing.

Q: Your command has more than 40 cooperative agreements with nations around the world, and the Navy partners with other U.S. federal agencies, the National Oceanic and Atmospheric Administration, National Geospatial-Intelligence Agency, and the U.S. Army Corps of Engineers, for example. What do these partnerships bring to the table?

A: As a small organization with a global requirement, we find our partnerships essential to sustaining our operations. They provide access to data sources key to our operational support, insight into emerging science and technology, and help all parties leverage limited budgets

by reducing redundancy and pooling capabilities. Being a part of the national and international science team really has its advantages in enabling naval operational oceanography to meet our warfighter's requirements.

Naval operational oceanography has a long history of executing cooperative military hydrographic and oceanographic surveys, as well as data, product and subject matter exchanges with our international partners. Our ability to provide emerging partners with improved capabilities in the areas of meteorology, oceanography and hydrography is unique and is highly regarded by combatant commanders and naval component commanders as an outstanding tool for strategic engagement. In turn, our partners provide access to information vital to our forward-deployed naval operations.

We also maintain strong interagency partnerships. The National Unified Operational Prediction Capability (NUOPC) initiative exemplifies how naval operational oceanography interagency partnerships contribute to enhanced capabilities. [With] the integration of modeling efforts among the Navy, National Oceanic and Atmospheric Administration (NOAA), and U.S. Air Force, NUOPC provides an unparalleled global modeling capability that can be adapted by individual agencies for specific applications, like warfighting support. Another strong example is our partnership with NOAA and the U.S. Coast Guard in operating the U.S. National/Naval Ice Center, providing ice analysis and forecasts to support safety of navigation for public, commercial and DoD use in the Arctic, Antarctic, Great Lakes, and all other large bodies of water affected by ice.

Q: The NAVMETOCCOM traces its ancestry to the Depot of Charts and Instruments. What can you tell me about the history of the command?

A: Yes, the Depot of Charts and Instruments was established in 1830 with a primary mission to care for the U.S. Navy's

chronometers, charts and other navigational equipment. In the 1840s, the superintendent of the Depot of Charts and Instruments was Lt. Matthew Fontaine Maury, who created and published a revolutionary series of wind and current charts. This information, which is still resident in modern computer models of ocean basins and the atmosphere, laid the foundation for the sciences of oceanography and meteorology.

In 1854, as its mission evolved and expanded, the depot was reestablished as the U.S. Naval Observatory and Hydrographic Office. The Hydrographic Office became its own entity in 1866 and ultimately became the Naval Oceanographic Office. Both of these organizations are now part of NMOC.

Atmospheric science was further developed with the birth of naval aviation early in the 20th century. During World War I and the following decades, naval aerological specialists applied the fledgling concepts of air masses and fronts to warfare, and provided forecasts to the first transatlantic flight.

The Navy's weather and ocean programs contributed greatly to Allied victory in World War II. In the Pacific, Navy forecasters cracked the Japanese weather code. Hydrographic survey ships, often under enemy fire, collected data along foreign coastlines for the creation of critical navigation charts.

In 1978, the Navy's meteorology and oceanography programs were integrated in a single organization reflecting nature's close interaction of sea and air, which today is the Naval Meteorology and Oceanography Command.

Q: Is there anything else that you would like to discuss?

A: Naval operational oceanography is a key enabler of the Navy's information dominance strategy and a member of the Information Dominance Corps. The strategic tenants of ID concentrate on providing the warfighter with assured command and control capabilities,



NORTH SEA (Sept. 17, 2010) Naval Oceanographic Office surveyors John Suslavage and David Small prepare to launch autonomous underwater vehicle, REMUS 600 aboard the Military Sealift Command oceanographic survey ship USNS Henson (T-AGS 63). They are in search of the remains of John Paul Jones' Revolutionary War ship Bonhomme Richard, which was lost off the coast of England in 1779 after a decisive battle with HMS Serapis. Jones won the battle and seized HMS Serapis as Bonhomme Richard was heavily damaged and sank 36 hours later. U.S. Navy photo by Rebecca Burke.

"Naval oceanography is the key contributor to providing the predictive, physical maritime battlespace awareness capability ..."

enhanced cyber and electromagnetic kill capabilities integrated with more traditional kinetic kill capabilities to broaden warfighting options, and to provide predictive, battlespace awareness across all warfighting areas. In this sense, the battlespace includes the physical as well as the cyber and electromagnetic domain.

Naval operational oceanography is the key contributor to providing the predictive, physical maritime battlespace awareness capability. But that is only part of the answer. We continue to strengthen our ties with the intelligence and cryptology/signals intelligence communities, which provide the human-influenced part of the maritime battlespace, to deliver fused battlespace information relevant to the warfighter. This partnership existed prior to the IDC

but has been enhanced in many areas due to the Navy's focus on ID.

In the future, vital information from both intelligence and oceanography professionals will be fused into the same common operational picture afloat, providing a view of the battlespace we can only imagine today, ensuring better and faster warfighting decisions. ●

FOR MORE INFORMATION

COMMANDER, NAVAL METEOROLOGY AND OCEANOGRAPHY COMMAND
www.public.navy.mil/fltfor/cnmoc

CNMOC PUBLIC AFFAIRS OFFICE
STNS_CNMOC_paoweb@navy.mil

Navy Leaders Announce Plans for Deploying Cost-Saving Laser Technology

Citing a series of technological breakthroughs, Navy leaders announced plans Apr. 8 at the Sea-Air-Space exposition to deploy for the first time a solid-state laser aboard a ship in fiscal year 2014.

“Our directed energy initiatives, and specifically the solid-state laser, are among our highest priority science and technology programs. The solid-state laser program is central to our commitment to quickly deliver advanced capabilities to forward-deployed forces,” Chief of Naval Research Rear Adm. Matthew Klunder said. “This capability provides a tremendously affordable answer to the costly problem of defending against asymmetric threats, and that kind of innovative approach is crucial in a fiscally constrained environment.”

The announcement to deploy the laser onboard USS Ponce (AFSB[II] 15) comes as Navy researchers continue to make significant progress on directed energy weapons, allowing the service to deploy a laser weapon on a Navy ship two years ahead of schedule. The at-sea demonstration in FY14 is part of a wider portfolio of near-term Navy directed energy programs that promise rapid fielding, demonstration and prototyping efforts for shipboard, airborne and ground systems.

“Our conservative data tells us a shot of directed energy costs under \$1,” Klunder said. “Compare that to the hundreds of thousands of dollars it costs to fire a missile, and you can begin to see the merits of this capability.”

The Office of Naval Research (ONR) and Naval Sea Systems Command recently performed demonstrations of high-energy lasers aboard a moving surface combatant ship, as well as against remotely piloted aircraft. Through careful planning of such demonstrations and by leveraging investments made through other Department of Defense (DoD) agencies, researchers have been able to increase the ruggedness, power and beam quality of lasers, more than doubling the range of the weapons.

“The future is here,” said Peter A. Morri-



SAN DIEGO (July 30, 2012) The Laser Weapon System (LaWS) temporarily installed aboard the guided-missile destroyer USS Dewey (DDG 105) in San Diego, Calif., is a technology demonstrator built by the Naval Sea Systems Command from commercial fiber solid state lasers, utilizing combination methods developed at the Naval Research Laboratory. LaWS can be directed onto targets from the radar track obtained from a MK 15 Phalanx Close-In Weapon system or other targeting source. The Office of Naval Research's Solid State Laser (SSL) portfolio includes LaWS development and upgrades providing a quick reaction capability for the fleet with an affordable SSL weapon prototype. This capability provides Navy ships a method for Sailors to easily defeat small boat threats and aerial targets without using bullets. U.S. Navy photo by John F. Williams.

sion, program officer for ONR's Solid-State Laser Technology Maturation Program. “The solid-state laser is a big step forward to revolutionizing modern warfare with directed energy, just as gunpowder did in the era of knives and swords.”

Officials consider the solid-state laser a revolutionary technology that gives the Navy an extremely affordable, multi-mission weapon with a deep magazine and unmatched precision, targeting and control functions. Because lasers run on electricity, they can be fired as long as there is power and provide a measure of safety as they don't require carrying propellants and explosives aboard ships.

Lasers complement kinetic weapons to create a layered ship defense capability, providing improved protection against swarming small boats and unmanned aircraft at a fraction of the cost of tradi-

tional weapons. The advancing technology gives sailors a variety of options they never had before, including the ability to control a laser weapon's output and perform actions ranging from non-lethal disabling and deterrence all the way up to destruction.

“We expect that in the future, a missile will not be able to simply outmaneuver a highly accurate, high-energy laser beam traveling at the speed of light,” Klunder said.

Following the USS Ponce demonstration, the Navy and DoD will continue to research ways to integrate affordable laser weapons into the fleet.

Video of the demonstration of the high-energy laser aboard a moving surface combatant ship and against remotely piloted aircraft can be seen here: <http://youtube/OmoldX1wKYQ>. ●

DoD's Commercial Mobile Device Implementation Plan

Enabling the mobile workforce

By CHIPS editors, Sharon Anderson and Heather Rutherford

Recognizing increasing end-user dependence on mobile devices, the Defense Department released a comprehensive enterprise management plan in February to ensure secure mobile device operation and maintenance in a cost efficient manner. The Commercial Mobile Device (CMD) Implementation Plan focuses on three key areas: mobile devices, the information enterprise infrastructure to support mobile devices and a Mobile Application Store. The plan emphasizes flexibility as a top priority to keep pace with fast-changing technology.

Plan development is in response to a Joint Requirements Oversight Council Capability Gap Assessment, Office of the Secretary of Defense guidance, and strong user demand for secure classified and unclassified mobile solutions. The plan outlines goals to provide data and voice services at the unclassified, secret and top secret levels for CONUS and OCONUS users, but does include provisions for use in combat.

Mobility solutions will leverage the enterprise capabilities within DoD's Joint Information Environment and will also be codified in the department's Information Enterprise Architecture.

Vision

The vision is to equip 600,000 DoD mobile-device users with secure classified and protected unclassified devices. The CMD Implementation Plan uses a phased structure, allowing small-scale pilot programs so that lessons learned can be incorporated and the plan refined as implementations



scale up. The plan executes the goals of the Mobile Device Strategy released in June 2012 by establishing a framework to advance and evolve the DoD enterprise information infrastructure to support mobile device policies and promote the development and use of mobile apps for DoD. The goal is to provide a cost management process that permits mobility solutions across the Defense Department but not to implement a specific mobile technology.

The CMD Implementation Plan opens the door for Android, Apple and BlackBerry devices enabling a device-agnostic approach. The plan includes directives to establish wireless voice, video and data capabilities

across the department by October 2013. It also calls for a 90-day approval cycle for mobile devices and operating systems, and includes guidance for the use of personal devices within the DoD environment due to ongoing security concerns. Under the plan, a bring-your-own-device option is not permitted.

Acquisition contracts for CMD carrier services (e.g., mobile voice and data via cellular) will be consolidated to the greatest extent practical. Department and governmentwide contracts are preferred to promote efficient use of government resources, in accordance with the Digital Government Strategy released May 23, 2012.

Mobile Application Store

Recognizing the increasing power, popularity and productivity advanced by mobile apps, DoD users will be able to download required applications from the department's Mobile Application Store. The DoD Chief Information Officer's aim is to develop a centralized library of mission-capable apps and an organizational process and development framework that keep pace with technology improvements where applications can be quickly developed, certified, purchased and distributed to users.

"This is not simply about embracing the newest technology — it is about keeping the department's workforce relevant in an era when information accessibility and cybersecurity play a critical role in mission success," said DoD CIO Teri Takai, in a release Feb. 26.

Governance

According to the plan, mobility capabilities will be guided by a continuous process of requirements evaluation and business case analyses to determine the mission and cost effectiveness of developing an enterprise solution. The approach calls for the procurement of CMDs via the Defense Information Systems Agency, DoD components and the General Services Administration. Mobile applications will be acquired and managed by each component, as a service managed by GSA, and as an enterprise service managed by DISA.

At the same time, DoD will take into account mobile application development across DoD and other federal agencies to leverage lessons learned. The DoD CIO will make the final decision on enterprise apps with input from each of the components to ensure enterprise applications meet mission requirements and achieve best value for the department. Under the direction of the DoD CIO Executive Board, department components will participate in the CMD Working Group. The CMDWG will review and approve standards, policies and

processes for the management of mobility solutions and mobile applications on an ad hoc basis. The DoD CIO will conduct a semiannual audit that determines the total cost of mobility implementation, operation and management.

First Responder Network and Security Features

The plan also addresses security and interoperability standards with the First Responder Network Authority (FirstNet) Radio Access Network since DoD is often called upon to partner with other federal agencies and civil authorities when responding to significant local, regional or national emergencies. The DoD CIO foresees the ability to leverage CMDs to augment, enhance or replace existing communication capabilities as a total force enabler that will empower a new generation of digital collaboration technology. Developing networks that can simultaneously integrate DoD and public safety networks will widen the circle of actors who can support a given operation, allowing diverse stakeholders to contribute insights and expertise in real time.

The DoD mobility capability will integrate into established cyber-situational awareness and information assurance policies and procedures and computer network defense. Advances in technology may permit additional security features to strengthen the overall information assurance posture of DoD networks. Technologies to be examined include, but are not limited to, encrypting all voice traffic via Voice over Secure Internet Protocol (VoSIP), implementing 1024-bit encryption and biometric techniques. The Commercial Mobile Device Implementation Plan will deliver compelling benefits to DoD organizations and individual users; it is a strategy that incorporates long-term objectives as well as near-term capabilities.

According to Ms. Takai, the plan is a "key capability enabler for joint force combat operations, the application of mobile technology into global operations, integration of secure and non-secure communications, and development of portable, cloud-enabled capability [that] will dramatically increase the number of people able to collaborate and share information rapidly." ●

FOR MORE INFORMATION: Department of Defense Mobile Device Strategy: www.defense.gov/news/dodmobilitystrategy.pdf and Commercial Mobile Device (CMD) Implementation Plan: www.defense.gov/news/DoDCMDImplementationPlan.pdf.

DOD COMPONENT MOBILITY PILOTS

Unclassified CMD Capability

Army App Store (<http://www.army.mil/mobile/>)

Connecting Soldiers to Digital Apps

Navy - Digital Sea Bag

Air Force Warfighter's Edge

Air Force Electronic Flight Bags

U.S. Northern Command ONE Mobile Application

Telemedicine and Advanced Training Research Center mCare Initiative

Defense Advanced Research Projects Agency Fixed Wireless at a Distance

Unclassified CMD Capability

Navy - 4G Long-Term Evolution (LTE) Sea Trial

Special Operations Command - SECRET BlackBerry

Marines Corps - Trusted Handheld

DARPA - Secure iPad

Defense Information Systems Agency - Multi-Level Security Joint

Capability Technology Demonstration (JCTD)

DISA - JO-LTE-D TACTICS JCTD (broadband to the tactical edge)

National Security Agency - TIPSPIRAL

Cmdr. Sean O'Brien

Deputy Chief Information Officer, Naval Education and Training Command

The Naval Education and Training Command (NETC) has implemented a Virtual Desktop Initiative, a five-year plan to deploy the VDI to more than 36,000 daily users which will replace 80 percent of about 23,000 desktop computers in 2,500 classrooms at 68 learning sites around the world. Desktop virtualization provides multiple student and instructor workstations from a centralized server environment which eliminates physical workstations residing in an electronic classroom. CHIPS asked NETC's Deputy Chief Information Officer Cmdr. Sean O'Brien to discuss VDI and its impact on training, as well as other innovations that the training command is implementing to develop fleet readiness. O'Brien responded in writing in mid-March.



Cmdr. Sean O'Brien

Q: Can you explain what the VDI is and how it works? Is the VDI considered cloud computing? How do you see it evolving?

A: Desktop virtualization is the simulation of a computer and its resources within software. This process drives the separation of the operating system and applications from the underlying physical asset. VDI is a form of cloud computing, and is really the first step towards establishing a true NETC private cloud.

Q: Does the VDI run on Navy Marine Corps Intranet computers and is it part of the NMCI's limited deployment of the HVD, hosted virtual desktop?

A: Our implementation does not run on NMCI, but is very similar to HVD. The difference is our desktop virtualization stack is a VMware solution and NMCI's is provided by Citrix.

Q: Can you talk about the benefits of the VDI? Can it be accessed from mobile devices?

A: Our goals are: refresh outdated electronic classroom (ECR) workstations and operating systems by (1) standard-

izing the processes and technology that deliver training; (2) providing a solution that supports a streamlined, centralized information technology workforce; (3) improving the enterprise security posture; and (4) providing continued mission support with existing resources in light of reduced funding over the FYDP (Future Years Defense Program).

Centrally hosting the desktop environment on a server enables us to provide: (1) a common desktop configuration; (2) a uniform electronic classroom experience for the Sailor; (3) central management of patches, software upgrades and operating systems; and (4) a standardized solution for student and application loads.

VDI reduces operating costs: virtualization reduces information assurance (IA) risks and requirements [because] data never leave the virtual server; no Data At Rest [solution] is required for zero-base clients; and non-compliant applications are isolated and minimize IA risks reducing IT touch labor. Zero-clients have no local operating system or disk drives to fail; no refresh requirements driven by protocol updates [or] new applications; and media, graphics or memory restrictions.

Right now, we are only servicing users that log in from a NETC electronic class-

room, instructor prep station or an electronic resource room. At NETC activities at Keesler Air Force Base, we were able to serve up all instructor-led and self-paced courses. In the future, once we have a proof of concept and can identify and address security concerns, we see great training value to servicing NETC students no matter where they are and on any device they want, to include mobile devices.

During the planning process, the integrated project team determined VDI should be phased in throughout the domain because of diverse training environments and multiple stakeholders with varying requirements. At each site we are employing a rigorous pre-deployment process because several training applications are learning-site specific, and the team needed to consider each site and decided which workstations, programs and applications could be delivered as a service to the student.

At Keesler we were able to virtualize all seats and applications, but given the age of some of our content and associated applications we expect that as we prep each site we will find that there are some applications that are just not good candidates for visualization. Our goal is to replace 80 percent of our desktops, with the remaining 20 percent handling those applications that do not virtualize well.

Q: When was the initial deployment of the VDI at the Center for Naval Aviation Technical Training Unit, Keesler Air Force Base, and what is the students' response to how the VDI is performing?

A: We went fully operationally capable in January 2013. In this case, we went from 152 computers to three servers. Now when we need to update, we only have to do it three times instead of 152. It's a huge time and electricity saver and greatly reduces workload to a level commensurate with our manning. It's reliable, it's faster, and instructors now spend less time fighting technology and more time teaching. Our site technicians now spend more time on customer service — rather than compliance and configuration changes. Students and instructors are reporting a faster and richer learning experience on the new setup as latency and login times have been greatly reduced as well.

Q: Can you discuss any other information technology improvements that NETC is planning to improve the Navy learning environment?

A: The NETC CIO has chartered the Enterprise Training Management Framework (ETMF) initiative to apply industry best practices to increase efficiencies in developing, managing and delivering training. This effort represents a collaborative effort across functional subject matter experts (NETC N7), operational SMEs (NETC N6), technical SMEs (Sea Warrior Program under PEO EIS PMW 240), and Naval Education and Training Professional Development and Technology Center (NETPDTC) N6) to better define training and education requirements for training content and curriculum management and delivery.

The goal is to create a plan for IT development and spending that supports continuous business process improvements, meets required business needs, and in turn, improves the return on investment. ETMF is focused on



delivering the right training or training quality to our students. The current efforts are directed toward developing an enterprise roadmap that will help NETC prioritize its technology investments by assessing their impact to the business.

The ETMF team has held a series of workshops designed to identify and prioritize the business drivers and processes that make up NETC's mission. As we implement our strategy for transitioning those existing end-to-end processes, transition business rules and legacy systems into a data-centric, services-oriented architecture, collaboration and communication across our domain are critical.

The next steps will involve working with technology teams to evaluate how meeting the business needs impacts our training support systems. The end result will be an integrated IT strategic goal of efficiently capturing, aligning, storing and delivering training content and data to enable effective and agile decision making, and improve information sharing and knowledge management capabilities across all our lines of business and between all our business systems. This strategy is a key to ensuring the right people receive the right training (content) at the right time through efficient and effective use of the right resources (instructors, classes and equipment).

The objective is to provide access to training anytime, anyplace, and the Navy

began a phased roll-out of the modernized Learning Management System (LMS) platform Feb. 22 at the Naval Technical Training Center Meridian, Miss. Developed under a modernization effort called the Enterprise Training Management Delivery System (ETMDS), a subsystem in ETMF, it uses AtlasPro as the replacement technology for the current LMS that is at the end of its life. Navy eLearning (NeL) uses the LMS as the technology backbone enabling the delivery, administration, documentation, tracking and reporting of online educational courses and training programs. The new system will be phased in throughout shore-based training facilities only.

Since 2001, Sailors afloat and ashore have depended on NeL to help advance their careers and stay current with training requirements. Courses range from information assurance awareness training — required of all Sailors, Marines, civilians and contractors — to hull-specific training for individual afloat units. NETC relies on NeL for use in schoolhouses for individual skills and skill refresher training. ●

FOR MORE INFORMATION

New LMS for NeL: <https://ile-help.nko.navy.mil/ile/index.aspx> and click on ETMDS. A CAC is required for access.

Naval Education and Training Command public website: <https://www.netc.navy.mil>.

The Unmanned Combat Air System Demonstrator X-47B

By Heather Rutherford and the Deputy Chief of Naval Operations for Information Dominance

Imagine AN AIRCRAFT THAT can launch with just the click of a mouse. While that capability has yet to be realized, the Navy is one step closer with the development and testing of the X-47B Unmanned Combat Air System (UCAS) demonstrator X-47B.

The X-47B was born of the Defense Advanced Research Projects Agency's Joint Unmanned Combat Air Systems program and developed by Northrup Grumman. The unmanned air vehicle (UAV) took its first flight in early February 2011 at Edwards Air Force Base in California and completed its first test at sea in December 2012 aboard the USS Harry S. Truman (CVN 75) off the coast of Virginia.

The unmanned aircraft's specifications are impressive; shaped like a bat, tailless, and bearing a wingspan of 62 feet, the X-47B was designed to be a long-range vehicle that could operate at a ceiling of 40,000 feet at a speed classified as high subsonic — that's more than 600 miles per hour. The purpose of the X-47 is to demonstrate UAV carrier suitability so it is only flight cleared for 15,000 feet and 220 knots for testing. There are currently no plans to operationalize X-47B, but the information garnered and the lessons learned will directly transition into the follow-on operational Unmanned Carrier-Launched Airborne Surveillance and Strike (UCLASS) system under development.

"I'm a believer that this is only the beginning," said Don Blottenberger, deputy program manager for the Navy UCAS Program Office (PMA-268). "We're taking UCAS-D into next year with what we learned aboard [USS] Truman. We are planning to get it back on a carrier to complete catapult launches, arrested landings and aerial refueling tests. There is a lot ahead for our program and a lot of hard work behind us. I look at Truman as the beginning of future unmanned integration with the fleet."

The UAV was subjected to a battery of tests that included carrier-based tractors towing the aircraft and taxiing on



ATLANTIC OCEAN (Dec. 11, 2012) An X-47B Unmanned Combat Air System (UCAS) demonstrator aircraft is transported on an aircraft elevator aboard the aircraft carrier Harry S. Truman (CVN 75). U.S. Navy photo courtesy of Northrup Grumman by Alan Radecki.



ATLANTIC OCEAN (Dec. 13, 2012) An X-47B Unmanned Combat Air System (UCAS) demonstrator aircraft is transported on an aircraft elevator aboard the aircraft carrier Harry S. Truman (CVN 75). U.S. Navy photo courtesy of Northrop Grumman by Alan Radecki.

the flight deck by its arm-mounted control display unit (CDU). Among the most striking results of the testing was X-47B's performance when exposed to electromagnetic fields. The aircraft withstood electromagnetic and environmental testing in an anechoic chamber, on the ramp and pier-side, successfully demonstrating that its command and control links, including the wireless link to the CDU, are effectively protected.

"We proved that the X-47B air system is mature and can perform flawlessly in the most hostile electromagnetic environment on Earth — a Nimitz-class Navy aircraft carrier," said Mike Mackey, UCAS-D program director for Northrop Grumman Aerospace Systems.

Crew members were responsible for directing the X-47B during its stay aboard the Truman. Although X-47B is

nearly 17 feet wider than the Navy's F/A-18 Super Hornet, which has a wingspan of almost 45 feet, the crew was able to comfortably maneuver the aircraft on the flight deck and into the hangar bays. As with guiding a traditional aircraft aboard a carrier, the flight deck director used standard hand signals and issued instructions to the deck controller. The major difference? The deck controller carried out the flight director's commands using a wireless handheld control. The exercises demonstrated the ability to maneuver the strike-fighter-sized aircraft quickly and precisely on the flight deck.

"I believe our Sailors integrated with the system very easily," said Lt. Cmdr. Larry Tarver, Truman's aircraft handling officer. "Getting Sailors to help out and participate was very easy as everyone was curious and excited to work with

it. Apart from those minor differences, the aircraft moved much like any other carrier-based aircraft while taxiing under its own power."

While X-47B itself is a prototype and will not become a permanent fixture in the fleet, similar aircraft may someday be found aboard ships.

"There are a lot of people aboard Truman that will take this experience with them," Blottenberger said. "I think that all of this interest will help different programs both manned and unmanned. Hopefully, its impact will benefit future technologies."

What's next for X-47B? According to Chief of Naval Operations Adm. Jonathan Greenert, the UAV will conduct catapult operations this spring. "I would submit to you we're going to get all wound up when we see this thing ... I'm pretty excited about it," he said. ●

Advances in Synthetic Aperture Sonar Transform Mine Countermeasures and Undersea Warfare

By Dr. Daniel D. Sternlicht, Jose E. Fernandez and Dr. Timothy M. Marston

ACTIVE SYNTHETIC APERTURE SONAR (SAS) IS A POWERFUL IMAGING TECHNIQUE THAT COHERENTLY COMBINES ECHOES FROM MULTIPLE PINGS ALONG THE TRAJECTORY OF A SURVEY PATH TO CONSTRUCT A LONG VIRTUAL ARRAY OF HYDROPHONES, WHICH ARE MICROPHONES DESIGNED TO BE USED UNDERWATER FOR RECORDING OR LISTENING TO UNDERWATER SOUND.

When synthetic aperture techniques are applied at sufficiently low acoustic frequencies, where sound absorption in the ocean medium is minimized, a modest-sized side-scan sonar can generate imagery with a constant azimuth resolution comparable to that of higher frequency sonar systems, but with a longer range potential, as shown in Figure 1.

Side-scan sonar is a category of sonar system that is used to efficiently create an image of large areas of the seafloor. It may be used to conduct surveys for maritime archaeology; in conjunction with seafloor samples it is able to provide an understanding of the differences in material and texture type of the seabed. Side-scan sonar imagery is also a commonly used tool to detect debris and other obstructions on the seafloor that may be hazardous to navigation, as illustrated in Figure 2. Side-scan data are frequently acquired along with bathymetric soundings and sub-bottom profiler data, thus providing a glimpse of the shallow structure of the seabed. Bathymetry is the study of underwater depth of lake or ocean floors. (See Figure 3.)

Synthetic aperture technology originated in the radar community in the mid-20th century, and was adapted by

the sonar community approximately 20 years later. For some time, SAS was not practical because of the limitations associated with enabling technologies, such as underwater platforms, suitable motion measurement instrumentation, accurate motion estimation techniques, and the storage and processing components needed to meet the computational requirements associated with SAS beamforming. This has changed over recent years and SAS systems are now being fielded in a wide range of military and commercial applications such as geological mapping, telegraph and pipeline surveys, environmental remediation, marine salvage and archeology and mine countermeasures. Beamforming is a general signal processing technique used to control the directionality of the reception or transmission of a signal on a transducer array. A transducer is a device that converts a signal in one form of energy to another form of energy. Energy types include electrical, mechanical, electromagnetic (including light), chemical, acoustic or thermal energy.

Small Synthetic Aperture Minehunter

Since the 1980s, the U.S. Office of Naval Research (ONR) has developed advanced synthetic aperture sonars for detection, localization, and classification (DLC) of mines, for protection of sea lines of communication and naval operating areas, and for support of amphibious operations. The range of activities required by these sensors includes: intelligence preparation of the operational environment (IPOE), search-classify-map (SCM) operations,

and reacquisition-identification (RI) of mine-like objects for subsequent neutralization.

Recently developed SAS systems have been designed to operate over a wide range of wavelengths and aspects. Centimeter-scale wavelengths (with acoustic frequency typically greater than 100 kilohertz) are used for fine-detail imaging of seabed texture and of small man-made objects. Longer wavelengths, which propagate deeper into the sediment volume, are used for imaging and spectroscopic analysis of buried objects that lay proud on the seabed. Spectroscopic analysis refers to the measurement of electromagnetic radiation intensity as a function of wavelength.

The Small Synthetic Aperture Minehunter (SSAM), developed by the Naval Surface Warfare Center Panama City Division (NSWC PCD) and the Applied Research Laboratory, Penn State University (ARL-PSU), is a multi-scale frequency design that exploits all of these advantages. It consists of two SAS systems: a high frequency (HF) synthetic aperture sonar and a long-wavelength broadband (BB) synthetic aperture sonar, wherein two separate projectors share a common hydrophone array, as shown in Figure 1. The SSAM is deployed on a Woods Hole Oceanographic Institution Remote Environmental Monitoring UnitS 600 (REMUS 600), commonly referred to as the 12.75, because of its hull diameter. It may be operated to a depth of 600 meters.

Presently, two generations of the SSAM concept exist, both of which operate in strip-map mode: monostatic and utilizing broadside beams. A

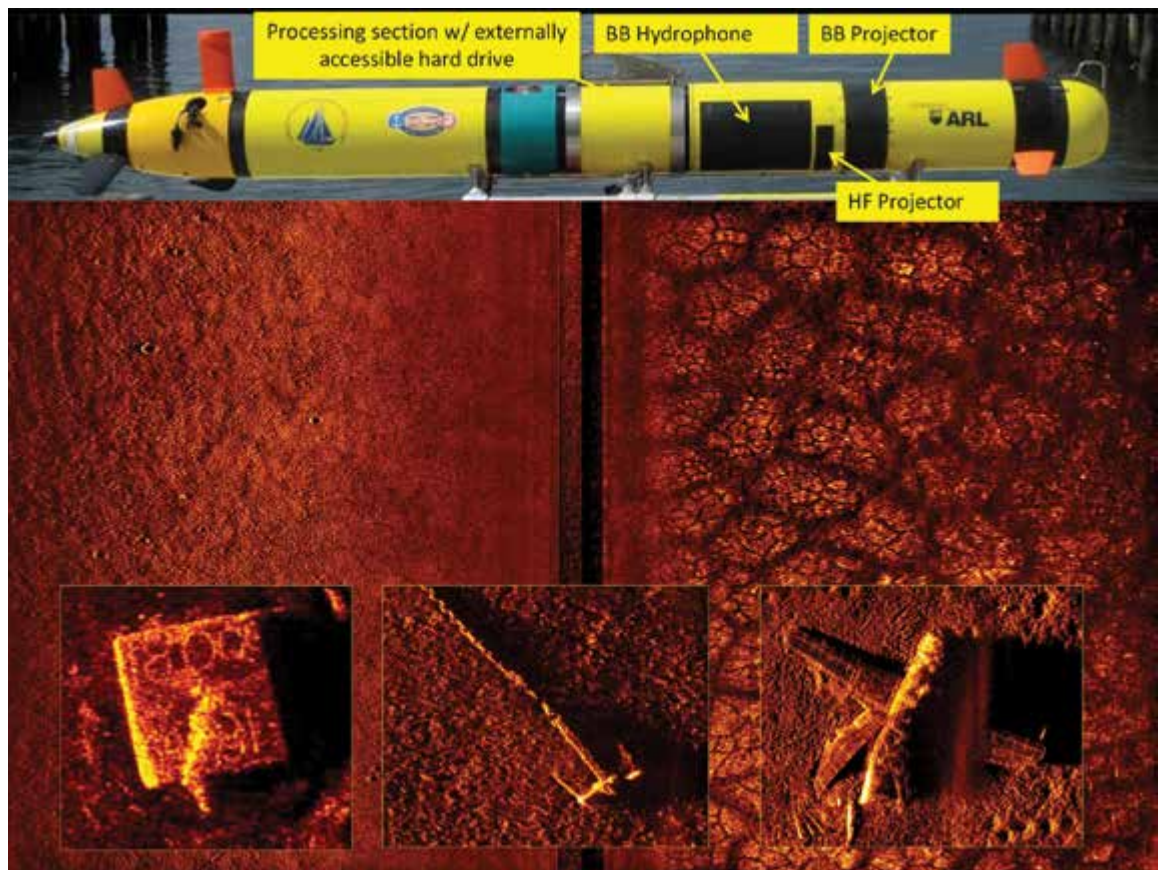


Figure 1. The SSAM system and example imagery showing engravings on a mooring and high resolution detail of objects at maximum range. The background displays a mirrored high-frequency and broadband image, with subsurface geology evident in the latter. U.S. Navy courtesy photos.

conventional SAS strip mapping mode assumes a fixed pointing direction of the hydrophone array broadside to the platform track. A strip map is an image formed in width by the swath of the SAS and follows the length contour of the flight line of the platform itself. The first generation SSAM system was fielded from 2005 through 2009 and participated in 11 events surveying more than 23 square nautical miles of seabed. The second generation system (SSAMII) has been fielded since 2010, and is designed for hunting proud and heavily scoured objects in shallow water and near-shore environments. New features include an improved hydrophone array and projectors that effectively reduce interference from surface multipath reflections, thus extending the range of the system in shallow water

environments. To accomplish this, the hydrophone array has a multichannel vertical aperture that allows beam steering to reject energy scattered from the sea surface. This new design houses the receiver electronics in an oil-filled cavity behind the array, and is used for enhanced motion estimation and generation of high resolution bathymetry maps.

The HF projector was redesigned in an asymmetric curve to reduce surface ensonification further improving signal to reverberation ratio. As in the previous generation, the SSAMII can accommodate storage and processing components for real-time SAS image formation and implementation of automatic target recognition (ATR) for initial generation of a sortie report that can be transmitted by a RF link or acoustic communications.

Tomographic and Interferometric SAS Processing

A recently developed modality exploiting tomographic processing (taking measurements around the periphery of an object) has been demonstrated with the SSAM system. This modality, referred to as "circular synthetic aperture imaging" (CSAS) in technical literature, is capable of very high fidelity image generation. CSAS is similar to conventional strip-map SAS in the sense that the sonar trajectory is exploited to synthesize a much larger array than that of the physical sonar.

Unlike strip-map SAS systems operating on a linear trajectory, CSAS, as implied by the name, circumnavigates and repeatedly ensonifies the area to be imaged. Signal processing techniques similar to those applied by

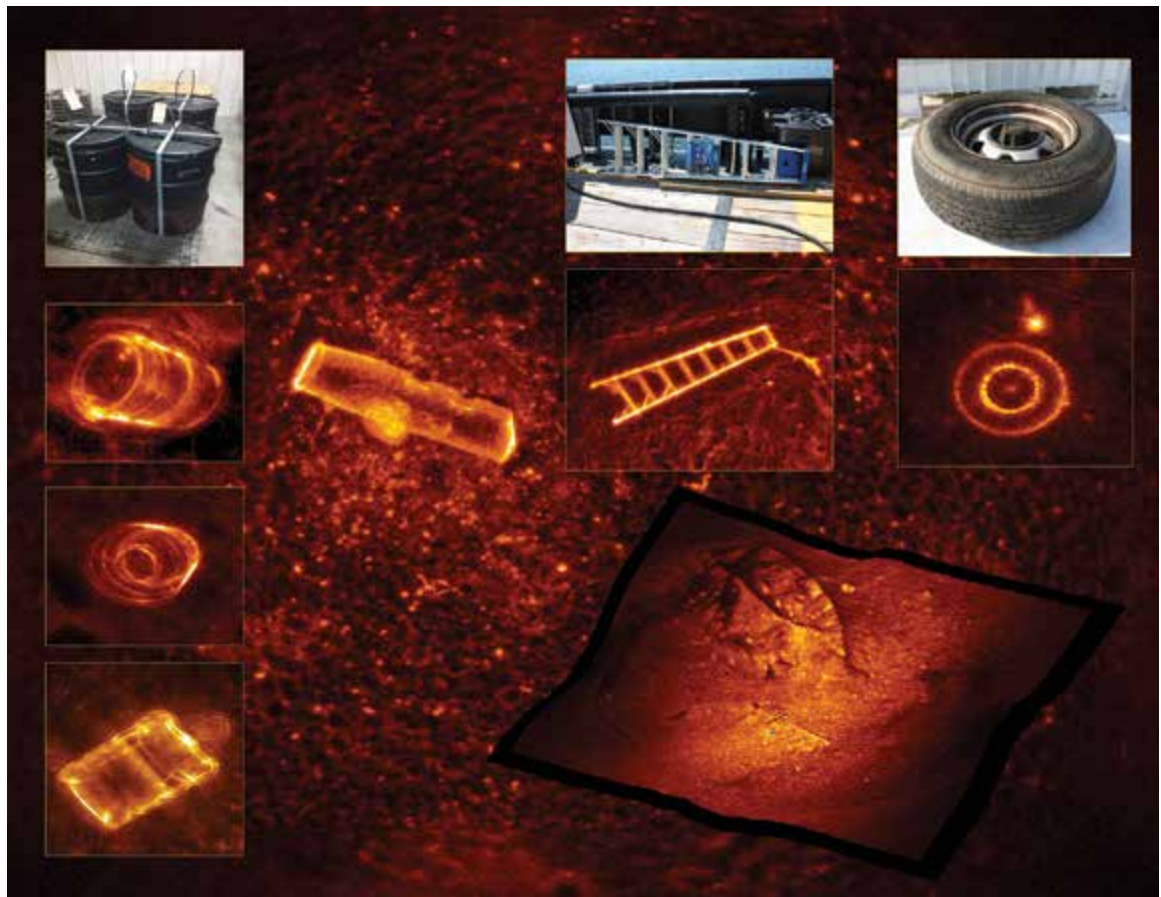


Figure 2. CSAS imagery generated using SSAM. Insets show a ladder, car tire, barrels, and a boat overlaid on topography. The background image shows a beveled training cylinder.

medical computerized tomography (CT) scanners are used to reconstruct a very high resolution image from the back-scattered acoustic information. Though neither strip-map nor circular SAS need to operate on their ideal linear and circular paths to form high resolution imagery, the platform position must be precisely known. Position estimation has historically been a primary cause of SAS image degradation and the major handicap preventing field usage of the tomographic imaging modality. Powerful motion estimation and data-driven focusing techniques are now capable of making high quality linear and tomographic SAS images in a consistently robust manner.

The photographic quality of circular scans provides images that an opera-

tor could use to identify objects with high confidence. The resulting information content in the digital data is extremely rich, appropriate for use by a variety of scene analysis and target recognition algorithms. In undersea warfare, a canonical minehunting procedure comprises target detection and classification, with a wide-swath seafloor imaging sonar (SCM phase), followed by confirmation using divers or a short-range identification sensor (the RI phase). The processing techniques described in this article demonstrate the possibility of combining the SCM and RI phases within a single sortie; where the AUV first maps an area using strip-map SAS processing, produces a contact list via in-vehicle beamforming and automatic target recognition; and then returns to circle

the object for target identification.

The Small Synthetic Aperture Minehunter system contains vertically spaced rows of hydrophones for interferometric (technique to extract arrival angle of acoustic waves) data processing. Interferometric processing exploits timing differences in received signals to estimate bathymetry.

The interferometric data channels on the SSAMII can be used to generate bathymetric estimates that are co-registered with the output SAS images. The capability of generating centimeter-scale resolution in all three spatial domains should provide significant performance improvements in the classification and identification of small objects. Additionally, interferometric data can be used to aid the coherent beamforming process making a

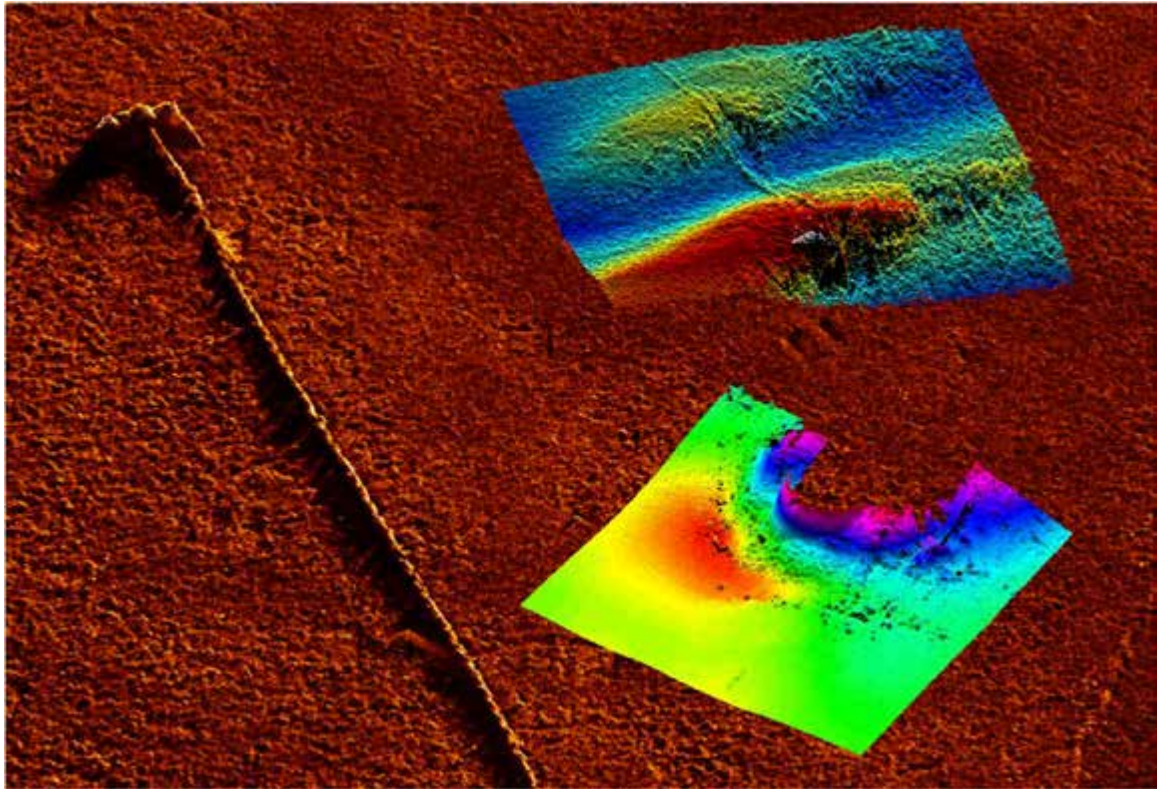


Figure 3. Bathymetry for snippets of scenes containing a cable, a bridge-supporting column, and an anchor. The SAS intensity image has been overlaid on the anchor bathymetry.

SINCE THE 1950S, NAVAL SURFACE WARFARE CENTER PANAMA CITY DIVISION HAS BEEN A LEADER IN THE DEVELOPMENT OF SIDE-SCAN SONAR SYSTEMS FOR THE U.S. NAVY.

more reliable and robust system.

TRANSITION AND FUTURE INNOVATIONS

SSAM technology is transitioning into the acquisition phase for use in autonomous search-classify-map operations and intelligence preparation of the operational environment missions. It is also being used for site inspection and detection of unexploded ordnance in active and formerly used military test ranges, with successful 2012 deployments in the waters off Naval Air Station Patuxent River, Md., and Naval Support Activity, Panama City, Fla. Further deployments are being planned for a variety of sites along the Gulf Coast and Eastern Seaboard.

The next generation of the SSAM, in the early stages of development, is

being designed to improve detection, localization, and classification capabilities against fully buried objects. Here, spectroscopic techniques (multi-aspect, broadband measures of target strength) for the broadband synthetic aperture sonar will be combined with image-based processing from the high frequency synthetic aperture sonar to substantially reduce false alarm rates.

Since the 1950s, Naval Surface Warfare Center Panama City Division (NSWC PCD), then called the Mine Defense Laboratory, has been a leader in the development of side-scan sonar systems for the U.S. Navy. Over the last three decades NSWC PCD, working with its partners in government, industry and academia, has pioneered development of synthetic aperture sonars, with system designs, signal and

information processing, platform innovation, and concepts of operation that have had a transformational effect on mine countermeasures and undersea warfare, with commensurate effect in the commercial marketplace.

The mission of NSWC PCD is to conduct research, development, test and evaluation, and in-service support of mine warfare systems, naval special warfare systems, diving and life support systems, amphibious/expeditionary maneuver warfare systems, and other systems that operate primarily in coastal regions.

Today, NSWC PCD employs more than 1,300 employees of whom more than 880 are scientists and engineers serving at the only U.S. Navy RDT&E laboratory located on the Gulf of Mexico. ●

DR. DANIEL STERNLICHT is the head of the sensing sciences division at NSWC PCD, which specializes in development of advanced sensors and processing for Navy and Marine Corps missions. He received a Ph.D. in electrical engineering and applied ocean science from the University of California, San Diego, and Scripps Institution of Oceanography.

JOSE FERNANDEZ is the senior sonar engineer for the sensing sciences division at NSWC PCD. He has worked in the design, testing and data analysis of several sonar systems. Most of his recent work has been related to the development of synthetic aperture sonar (SAS) technology.

DR. TIMOTHY MARSTON, a research scientist in the field of signal processing at NSWC PCD, received a Ph.D. in acoustics from Penn State University in 2009. Since 2010, his primary focus has been the development of robust algorithms for synthetic aperture data processing.

Acknowledgments

The authors gratefully acknowledge the support of the Office of Naval Research, Ocean Engineering and Maritime Systems (Code 321), Dr. Jason Stack and Dr. Thomas Swean for development of the sensor, vehicle, and signal and information processing associated with the SSAM system.

For More Information

- ➔ [NAVAL SURFACE WARFARE CENTER PANAMA CITY DIVISION \(NSWC PCD\): WWW.NAVSEA.NAVY.MIL/NSWC/PANAMACITY/DEFAULT.ASPX](http://WWW.NAVSEA.NAVY.MIL/NSWC/PANAMACITY/DEFAULT.ASPX)
- ➔ [NSWC PCD PUBLIC AFFAIRS OFFICE NSWCPCPAOWEBMANAGER@NAVY.MIL](mailto:NSWCPCPAOWEBMANAGER@NAVY.MIL)
- ➔ [OFFICE OF NAVAL RESEARCH WWW.ONR.NAVY.MIL](http://WWW.ONR.NAVY.MIL)
- ➔ [ONR OCEAN ENGINEERING AND MARINE SYSTEMS WWW.ONR.NAVY.MIL/EN/SCIENCE-TECHNOLOGY/DEPARTMENTS/CODE-32/ALL-PROGRAMS/OCEAN-SYSTEMS-321/OCEAN-ENGINEERING-MARINE-SYSTEMS.ASPX](http://WWW.ONR.NAVY.MIL/EN/SCIENCE-TECHNOLOGY/DEPARTMENTS/CODE-32/ALL-PROGRAMS/OCEAN-SYSTEMS-321/OCEAN-ENGINEERING-MARINE-SYSTEMS.ASPX)



Dr. Timothy M. Marston, a Naval Surface Warfare Center Panama City Division (NSWC PCD) research scientist, receives the prestigious Meritorious Civilian Service Award Feb. 1, 2013 for his technical achievements in synthetic aperture sonar (SAS) signal processing. Standing from left to right are: Science, Technology, Analysis and Simulation Department head Dr. Kerry Commander; Hilary Marston (wife of Dr. Marston); Dr. Timothy Marston; Prof. Philip Marston (Dr. Timothy Marston's father); and NSWC PCD Technical Director Mr. Ed Stewart. Photo by Ray Lim/NSWC PCD.

For Further Reading

- D. Sternlicht and J. F. Pesaturo, Synthetic Aperture Sonar: Frontiers in Underwater Imaging, *Sea Technology*, 45(11), pp. 27-32. November 2004.
- D. Brown, D. Cook, and J. Fernandez, Results from a Small Synthetic Aperture Sonar, *Proceedings MTS/IEEE OCEANS*, September, 2006.
- D. D. Sternlicht, J. E. Fernandez, R. Holtzapple, D. P. Kucik, T. C. Montgomery, C. M. Loeffler. Advanced Sonar Technologies for Autonomous Mine Countermeasures, *Proceedings MTS/IEEE OCEANS*, September 2011.
- T. M. Marston, J. L. Kennedy, P. L. Marston, Coherent and Semi-Coherent Processing of Limited-Aperture Circular Synthetic Aperture (CSAS) Data - Applications for Target Field Analysis and Object Classification, *Proceedings MTS/IEEE OCEANS*, September 2011.
- T. Marston, A Correlation Based Autofocusing Algorithm for Coherent Circular Synthetic Aperture Sonar, *Proceedings of the European Conference on Synthetic Aperture Radar (EUSAR)*, April 2012.
- T. R. Clem, D. D. Sternlicht, J. E. Fernandez, J. L. Prater, R. Holtzapple, R. P. Gibson, J. P. Klose, T. M. Marston. Demonstration of Advanced Sensors for Underwater Unexploded Ordnance (UXO) Detection, *Proceedings MTS/IEEE OCEANS*, October 2012.

New Department of the Navy IT Policies Signed

By DON IT Enterprise Communications Team

Cloud Computing Memo Signed

On April 1, 2013, the Department of the Navy Chief Information Officer signed the memo, "Department of the Navy Approach to Cloud Computing." The memo (www.doncio.navy.mil/ContentView.aspx?id=4518) states that to increase efficiency and achieve necessary cost savings, the department is moving forward to employ capable cloud computing solutions that meet mission and security requirements and provide best value. Unless a more cost-effective solution is identified, the first step will be moving DON systems that host publically releasable information to commercial cloud service providers that meet all requirements.

The policy follows a recent pilot sponsored by the DON CIO with Amazon Web Services to move publicly accessible data to a commercial hosting environment. The Secretary of Navy's public-facing information portal (www.secnav.navy.mil/default.aspx) is now hosted in the Amazon Web Services cloud infrastructure. The innovative decision to host the data in a commercial cloud environment resulted from an analysis of several factors, the most important being the type of data stored in the portal, hosting costs and security requirements.

The new policy will enable the department's systems that host publically releasable information to move to commercial cloud service providers, as long as all requirements are met at the best value. The experience the DON gains through initial application of cloud computing, in conjunction with security requirements, will inform future decisions on how to best apply this technology.

The National Institute of Standards and Technology defines cloud computing as: "A model for enabling ubiquitous, convenient, on-demand network access

to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

In the simplest terms, cloud computing focuses on storing and accessing data and programs over the Internet instead of on your computer's hard drive. End users access cloud-based applications through a Web browser or a lightweight desktop or mobile app while the software and user's data are stored on servers at a remote location.

As a business model, cloud computing can help the DON achieve economies of scale with improved manageability and ability to adjust resources to meet end user demand, improve system performance and reduce infrastructure costs.

DON Policy for Electronic Record Keeping Systems and Applications

The purpose of the memorandum (www.doncio.navy.mil/ContentView.aspx?id=4508) is to delineate records management (RM) policy for electronic information systems (EISs) and records management applications (RMAs) within the Department of the Navy. This policy pertains to new, updated and existing DON EISs and RMAs. Enclosures (1) through (4) provide detailed information essential to policy compliance.

In addition to complying with Department of Defense (DoD) and DON policies and Federal statutes and regulations, effective EIS RM facilitates information discovery and visibility, which improves information sharing. Additionally, effective EIS RM facilitates removal of obsolete data, improves security, and helps maintain current, authoritative information sources. The new policy was

signed by the DON CIO Terry Halvorsen, March 21, 2013.

DON Certification and Accreditation Pilot

This memo (www.doncio.navy.mil/ContentView.aspx?id=4493) outlines the certification and accreditation pilot of information technology systems within the Department of the Navy.

DoD Instruction 8500.2, Information Assurance (IA) Implementation, of Feb. 6, 2003 and DoD Instruction 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), of Nov. 28, 2007 require certification and accreditation (C&A) of information technology systems within the Department of Defense. Flexibility within the policies allows the Department of the Navy to explore process changes that may reduce costs yet maintain a secure environment. The DON plans to investigate these possibilities by piloting a streamlined C&A process. In this pilot, the DON will prepare for transition to the Risk Management Framework, employ security measures focused on mission impact and real threat information, eliminate duplicative and unnecessary efforts, and reduce the overall cost of C&A. The pilot will employ mission-based approaches to system accreditation. It will investigate alternatives for interim approval timelines and conditions for specialized environments. The pilot will also evaluate prioritized security controls and increased C&A reciprocity between the Navy and Marine Corps. The DON Chief Information Officer and the Service Designated Accrediting Authorities will supervise the pilot to ensure acceptable security is maintained. ●

DON CIO
WWW.DONCIO.NAVY.MIL

Rear Adm. Terry B. Kraft

Commander, Navy Warfare Development Command

Navy Warfare Development Command links tomorrow's ideas to today's warfighter through rapid generation and development of innovative solutions to operational challenges. NWDC's unique synergies and capabilities help move the fleet forward through the 21st century. NWDC is home to the Navy Center for Advanced Modeling and Simulation, a 10,000 square-foot, state-of-the-art modeling and simulation facility which supports the Navy Continuous Training Environment, experimentation, concept generation and concept development. As the Navy's executive agent for concept development and generation, NWDC harvests concept proposals and innovative ideas and hosts the Navy Center for Innovation. Rear Adm. Kraft talked about the NWDC mission and fleet innovation in mid-March.



Rear Adm. Terry B. Kraft

Q: Since you assumed command of NWDC in October 2011, the command has taken on increased responsibilities in the areas of concept development and experimentation and support of innovation in the Navy. Can you talk about these changes?

A: I really appreciate the opportunity to talk about Navy Warfare Development Command. We have been going through a lot of changes over the past 15 months, and it is exciting to talk about some of the things we are involved in right now.

Concept development and fleet experimentation used to be split between NWDC and our parent command, Fleet Forces Command. Early last year, we absorbed the concept and experimentation teams at Fleet Forces and are really driving both concept generation and fleet experimentation now at NWDC. What this gives us is a 'virtuous cycle' of concept generation and experimentation and then turning that into tactical memoranda and eventually doctrine. We call that our cycle of life here — spanning from concept generation to experimentation and war gaming and into doctrine. These things are right in our wheelhouse, allowing us to deliver what Adm. Gortney and the CNO are looking for in fleet innovation.

Q: Adm. William Gortney, commander, U.S. Fleet Forces, approved the FY 13 Fleet Experimentation execution plan in fall 2012. Can you talk about the experiments that NWDC and NCAMS will be hosting?

A: Fleet experimentation, or FLEX as we call it, includes 12 different campaigns and up to 30 experiments in a single campaign, including Trident Warrior 2013 which is a large experimentation event. We are also hosting a war game which will look at how a MEU (Marine Expeditionary Unit) is going to fit and operate in the new ARG (amphibious ready group) which will obviously include the new LHA-6 (amphibious assault ship USS America), LPD-17 (amphibious transport dock USS San Antonio), the V-22 (Osprey) and the F-35B aircraft.

Another war game looks at the integration of both manned and unmanned systems in mine warfare and how to conduct force protection for some of these unmanned systems if you decide they are important enough to protect.

NCAMS hosts or enables about 330 training events a year, including Fleet Synthetic Training events. These fall under the Navy Continuous Training Environment or NCTE network. So you can think of us as a master node that is

able to push synthetic training out to the fleet. If you look to the future, delivering synthetic training to ships, not just ships that are pierside or simulators for aviation, but getting training to ships underway is going to be the next step in the process as we look at compressed local schedules. Ships may or may not get as much underway time, at least in the near future, so that puts pressure on our ability to do synthetic training and that's where NWDC comes in.

Q: With the Navy's current budget shortfall in maintenance accounts, will that have any bearing in the experimentation and synthetic training at NWDC?

A: The main impact of maintenance is that the ship is unavailable to do the kind of tactical training that you may want to do. Maintenance is a requirement and how you build in all the other things you want to do around that maintenance piece is where Fleet Synthetic Training comes in. You know you are going to have to maintain the ship, what do you do with the rest of the time around the maintenance period?

Q: Can you explain what the Carrier Strike Group (CSG) Advanced Tactics Initiative is?



Space and Naval Warfare Systems Center Pacific scientists and engineers hosted an Ideation Workshop Jan. 29 for members of Navy Warfare Development Command's (NWDC) Navy Center for Innovation Cell. The workshop provided an opportunity for an in-depth review of warfighter requirements. Military personnel from NWDC, Office of Naval Intelligence, Naval Postgraduate School, and the fleet attended as part of the Chief of Naval Operations' Rapid Innovation Cell (CRIC). The group's mandate is to generate ideas that lead to "disruptive innovation"; to propose radical new ways to solve problems; focus on prototypes, reviews, and alternate uses of technology; conduct virtual and live workshops; and expand a network of experts. The collaborative effort with CRIC began following SSC Pacific presentations to NWDC leadership at the Pacific Rim Symposium. U.S. Navy photo by Alan Antczak.

A. We call it CATI. CATI integrates rapid development of CSG training and tactics with fleet-identified capability gaps, tactical level doctrine and training solutions for the CSG. This really came about when I came into this job. When I was commander of the Enterprise Carrier Strike Group, I didn't feel we had a good system to really push high-end advanced tactics, as well as our newer capabilities that were coming down the line, to our CSG commanders and make them aware of them. So we are now an intermediate stop before prospective CSG commanders go to their next command. We fill their heads, if you will, with these advanced tactics that are available to them as they prepare their strike group for deployment. We also make them aware of the last five years' worth of carrier strike group debriefs to pass on tactics and best practices from one CSG to the next.

We have also built a war game called CSG 360° that is rolling out now. CSG 360° takes all these things that we have been talking about and puts them into a future warfighting scenario that is

very challenging. We had great support from the Naval War College developing CSG 360°. In a nutshell, it's really about getting the strike group commanders to think tactically again above and beyond the things we are facing today.

Q: Are you working with the surface warfare and air warfare communities?

A. We do. Besides interfacing with strike group commanders, we've pushed a lot of these initiatives out to the Commander, Strike Force Training Atlantic and Pacific, and also to Tactical Training Group Pacific and Atlantic. The tactical training groups have taken on a lot of these things. We make it part of their work-ups and training. The Naval War College has been a great partner in this effort.

Q: Is CATI training or the CSG 360° war game a prerequisite for deployment?

A. It is not in the official pre-deployment work-up syllabus but

elements of it have already been included in that syllabus. It is not a stand-alone syllabus event at this time, although I could see how it could turn into how we train strike groups in the future.

Q: With the certainty of reduced defense budgets, the importance of fleet innovation is more urgent than ever since some are predicting the Navy's fleet will shrink in size. So increased capabilities and innovative warfighting concepts are more important than ever. NWDC has been able to do an amazing job with jumpstarting fleet innovation in such a short time.

A. Thank you very much for the compliment; it is by far the most fun thing that we do here. When I came into this job in October 2011, [former Commander of Fleet Forces] Adm. Harvey made it clear to me that the CNO was interested in rebuilding a culture of innovation across the fleet. We had it before as we looked at the



Chief of Naval Operations Adm. Jonathan Greenert with the CNO's Rapid Innovation Cell — or CRIC. The CRIC is made up of some of the Navy's most innovative junior leaders who look at specific fleet warfighting needs and how commercial solutions might be brought to bear on these issues.

interwar years and the innovation history and the General Board (advisory panel of senior admirals credited with bringing creativity and innovation in the fleet — dissolved in 1951). They came up with some great things they were experimenting with at the time. The (World War II) island-hopping campaign, floating drydocks, and how to use detached aircraft carriers. They were war gaming these ideas to such a point that after the war Adm. Chester Nimitz said the only aspect [of the Pacific War] that surprised him was the kamikazes; we had evaluated everything else. So this idea of innovation in challenging times was really driven home when we looked at the interwar years, and we had to decide now how we can adapt it for modern times. We teamed with SPAWAR (Systems Center) Pacific on a West Coast event and brought in junior leaders (junior officers and mid-grade enlisted) to pick their brains and stimulate this idea of fleet innovation. One of the results of that is the Innovator's Guide that we published

Every warfighter needs to know how to operationally use information, and we need to bring that knowledge level into everything that we do.

for innovators of all ranks, and it has become popular in industry as well.

We also recently completed a three-phase online war game; the acronym is MMOWGLI, or Massive Multiplayer Online War Game Leveraging the Internet. It's a crowdsourcing environment, and it is an interesting look at how crowdsourcing works in this process of innovation. The game explored electromagnetic (EM) maneuver in three specific areas: Understanding EM Energy; C2 in the EM Environment; and Tactical Employment of EM Weapons. We put

people through a lot of scenarios over the course of the three phases to pull ideas. At one point, we had over 500 players across the globe, and we are taking the results and putting them into something leadership can use.

The idea behind our innovation campaign is to develop a process that the CNO can use to make sure that important ideas get to people that matter. Two groups were established to do this. One is the CNO's Advisory Board (CAB) which is a small group of nine people, including active-duty three-stars, and industry and

The CNO's Rapid Innovation Cell – or CRIC – is a group of what the CNO calls 'free radicals.' These are mostly junior officers at the grade of lieutenant (we also have an E-6 and a few O-4s) and they are given a small budget to look at things they want to prototype and experiment with in the fleet.

academic professionals, to be kind of our window on the world to see what events outside of the military could be important for the Navy. During the interwar years a lot of innovation was driven inside the military, but as we look at society today a lot of innovation is happening in industry and in other places. The question is who can be a lens for the CNO on all the things that are going on and that's what we envision the CAB doing for this process.

The CNO's Rapid Innovation Cell – or CRIC – is a group of what the CNO calls 'free radicals.' These are mostly junior officers at the grade of lieutenant (we also have an E-6 and a few O-4s) and they are given a small budget to look at things they want to prototype and experiment with in the fleet.

This has been very exciting for me because junior officers look at the world much differently than I do. Frankly, their viewpoints are refreshing. They sat down with the CNO in mid-March to talk about their ideas. So all these things roll up into a process to build a channel for innovation.

Q. Do you have any pilots in the fleet based on ideas that were generated?

A. The CRIC has about six ideas that we made a decision to move on that will be introduced to the fleet within

the next year. I don't want to steal their thunder because we will be publicizing them as they roll out to the fleet. They are all interesting ideas and several have very little investment for what could possibly be a high payoff.

Q. Would you like to talk about anything else?

A. One last thing I would like to talk about is building on the Navy's information dominance capability – building the 4-D (air, surface, subsurface, space) or 5-D (air, surface, subsurface, space, cyberspace) warfighter. How do we do that? Right now, we have 3-D (air, surface, subsurface) warfighters. But we need to bring in information or cyber knowledge. Using EW (electronic warfare) or cyber is how we fight today. We developed the Capstone Concept for Information Dominance to support the implementation of The Navy Information Dominance Vision and The Navy Information Dominance Strategy. We need ideas and discussion [to keep building on the Navy's capabilities]. Every warfighter needs to know how to operationally use information, and we need to bring that knowledge level into everything that we do.

We also just published a lessons learned report about the Navy's response to Hurricane Sandy. Usually, a warfighter would come back from a

mission or deployment and he would sit down and type a report [but that information would be lost]. During the relief efforts in New York and New Jersey, we deployed a team to do a live collection to capture lessons learned. This is a case where we turned a report into real knowledge. We are turning knowledge into TACMEMOs and doctrine. A Lessons Learned Guidebook from Sandy will be passed out at a gathering of flag officers in April.

A meta-analysis of Carrier Strike Group deployment lessons learned is a popular focus right now with the Fleet Training Integration Panel (FTIP) and Readiness Requirements Review Board. What are the major trends and gaps in capabilities? CATI will forward tactics and training recommendations to the FTIP and Fleet Commanders Readiness Council for prioritization and resourcing. ●

FOR MORE INFORMATION

NAVY WARFARE DEVELOPMENT COMMAND
<https://www.nwdc.navy.mil/>

NAVY CENTER FOR INNOVATION
<https://www.nwdc.navy.mil/ncoi/>

Play the game, Change the Game

Crowdsourcing to solve some of the Navy's toughest problems

By Heather Rutherford

The Massive Multiplayer Online War Game Leveraging the Internet (MMOWGLI) is an online game designed to crowdsource ideas and strategies that may provide insight into some of the Navy's toughest problems.

With the help of multimedia and Web 2.0 technology, the joint effort between the Office of Naval Research (ONR), the Naval Postgraduate School (NPS) and the Institute for the Future creates an environment where players are asked to share new ideas and collaborate with others to earn innovation points and win the game. The platform is designed to support large numbers of distributed global players working together on idea generation and action planning, with an eye toward surfacing innovative outlier strategies.

MMOWGLI can be used for virtually any topic. Previous MMOWGLI games focused on Somali piracy, energy and business innovation. The most recent game was sponsored by the Navy Warfare Development Command's (NWDC) Navy Center for Innovation and explored electromagnetic maneuver (em2).

Electromagnetic Maneuver Massive Multiplayer Online War Game Leveraging the Internet — or em2 MMOWGLI — was played in three one-week phases:

- ➔ Move 1: "Know the EM Environment: Understanding EM Energy";
- ➔ Move 2: "Be Agile: C2 in the EM Environment"; and
- ➔ Move 3: "Change Our Paradigm: Consideration for EM Capabilities Employment."

em2 MMOWGLI had more than 625 players from across the globe.

"This is a great way to reach a lot of people and save money," said Rebecca



Law, a MMOWGLI subject matter expert based at NPS. With today's budget constraints, MMOWGLI makes good economical sense. While the first games were open to a more general audience, access to em2 MMOWGLI was limited to holders of a .mil address. Players could sign up, register, and log in from the MMOWGLI players' portal page using screen names of their choice so they could remain anonymous, if desired. The em2 MMOWGLI was also the first time that this unclassified game system was coupled with a NWDC-hosted SIPRNET discussion site to allow for full discussions of some pressing electronic warfare and cyber issues at the appropriate level of classification.

According to Steve Rowe, director of

NWDC's innovation campaign division, players were able to join the game during any phase.

Playing a MMOWGLI game is not unlike solving a puzzle in a group setting; players provide input, seek out the best ideas and brainstorm to reach a collaborative solution. "Seed" cards were planted at the beginning of each phase to spark ideas without bias, which allowed players the opportunity to think freely.

Using questions on the seed cards as prompts, players entered their ideas, which displayed on virtual sticky notes called idea cards. Depending on the game, ideas were geared toward either innovation (future ideas) or defense (status quo).

Because MMOWGLI's developers

sought to create an environment that has similar aspects to social networking, players' idea card responses were limited to 140 characters (just like Twitter). Despite that, players had a lot to say: more than 5,600 idea cards were generated during em2 MMOWGLI.

Players received points based on their input and could also receive exclusive icons and badges if they reached special achievements such as playing cards in every category – which sometimes stoked the fires of competition.

For the most part, MMOWGLI players appeared to take the game seriously – and they wanted recognition. “There are times when it is about getting points out there and getting on the leaderboard,” Law said. “But based on the 41 action plans the players collaboratively generated, they were clearly focused on helping the Navy move electronic warfare forward.”

While the game essentially drove itself, MMOWGLI was moderated – presided over by behind-the-scenes game masters on both the East and West coasts of the United States. Not only did the game masters monitor game play for potential technical issues, they also interacted with the players by “liking” players' ideas to link related concepts or illuminate specific areas of interest. If a game master clicked a player's card, that player received extra points.

Idea generation is key to the success of the war game. As Law said, “Good ideas naturally float to the top.”

The good ideas eventually led to actionable items, which in turn were incorporated into action plans addressing the 5 W's – who, what, when, where and why. Action plans were generated in two ways; from game masters, who could ask for an action plan development, or by players, who could request action plans. Players also had the ability to vote on action plans to propel the best plans forward.

Although traditional action plans are text-based, players were welcome to embellish their plans using images, charts – and even videos. For example, rather than filling out a form, a player might record a video and post it on

MMOWGLI is designed to support large numbers of distributed global players working together on idea generation and action planning, with an eye toward surfacing innovative outlier strategies.

YouTube. While it may seem unusual to “watch” an action plan, using this sort of technology is in keeping with the Navy's initiative to appeal to the younger generation.

At the end of the game, winning players received the honor of being recognized on the MMOWGLI players portal for their input; namely, number of cards played, participation in action plans, and helpful feedback.

At press time, NWDC was still conducting detailed analysis of the thousands of ideas discussed in em2 MMOWGLI to identify recommendations for em2 capabilities development, and for future crowdsourcing events on this and other topics. The most interesting crowd-generated themes that have emerged so far include:

- The need to aggressively train to, and be prepared to operate with agility in, an environment where our command and control (C2) and communications systems are threatened.
- Enhancing EW and cyber training from accession onward, including

curricula at NPS, the Naval War College and the U.S. Naval Academy, and improved troubleshooting training in “A” School to reduce distance support reach-back requirements.

- Innovative ideas for engagement with the civilian sector, such as a DoD surge capability through a cyber/EM reserve “militia” force and a program in which civilians could volunteer to donate bandwidth and spectrum for military operations.
- Changes in doctrine, tactics and equipment to reduce reliance on vulnerable networks and communications paths. This discussion included some “back to the future” ideas like using lights for ship-to-ship signaling and use of pre-GPS navigation systems. Another “retro” suggestion was a renewed emphasis on emissions control (EMCON) and min-RAD (minimizing radiation signals) practices during the Cold War. ●

HEATHER RUTHERFORD is the CHIPS assistant editor. She can be reached at chips@navy.mil.

For More Information

MMOWGLI Players Portal: <https://portal.mmowgli.nps.edu/welcome>
Navy Warfare Development Command: <https://www.nwdc.navy.mil/>
Navy Center for Innovation: <https://www.nwdc.navy.mil/ncoi/default.aspx>,
NWDC_NRFK_INNOVATIONS@navy.(smil.)mil



THE DEPARTMENT OF THE NAVY
and DEFENSE LOGISTICS AGENCY

PARTNER TO DELIVER SAVINGS

BY THE DON AND DLA PRINT
AND IMAGING SOLUTIONS TEAM

A **NEW CRADLE-TO-GRAVE APPROACH** to manage unclassified networked and stand-alone copiers, printers, fax machines and scanners (CPFSSs) and multifunctional devices (MFDs) was established Jan. 25, 2013, in a policy signed by the Department of the Navy Chief Information Officer (DON CIO).

The policy, which applies to all DON commands and activities, is effective immediately. It improves how the department manages and uses its CPFSSs and MFDs, resulting in substantial savings for the DON. The enterprisewide contracts will include related consumables and support services.

The overall objective is to achieve cost savings by leveraging the efficient procurement and managerial capabilities of the Defense Logistics Agency (DLA) Document Services, according to the memo signed by DON CIO Terry Halvorsen.

The new policy is "a low risk, high payoff opportunity," Halvorsen said. "We are getting great support from senior leadership who have been willing to give up their own printers and walk the extra steps to a shared printer or look at data on the screen."

Halvorsen's initiative lead, Don Reiter, confirmed a dual focus of the policy.

"This DON-wide effort is a good example of how we can partner together with a well-established team of subject matter experts," Reiter said. "These SMEs will leverage their tools, experience and economic order of quantity agreements to improve how the DON acquires and manages its copiers, printers, scanners and multifunctional devices, and more importantly, [it will] save dollars."

Best Practices

Departmentwide savings are achieved by reducing the number of total devices and implementing best practices procedures in addition to cultural change management. These changes include making smart choices about what is printed and how it is printed.

Paper and color toner and inks contribute greatly to an organization's overall printing cost. To optimize the cost savings in this area, documents should be printed in black and white and on both sides of the paper. Typically, organizations print in black and white 70 percent of the time and in color 30 percent of the time. The Federal Strategic Sourcing Initiative for Print Management Commodity Team has set new printing targets at 90 percent black and white and 10 percent color printing. Standardizing printer settings will help the DON to achieve this performance goal. DLA will ensure all CPFSSs/MFDs are installed with these default settings already established. Users may override these settings for the occasional single page and color prints.

DLA Document Services will also help the DON implement best printing practices by ensuring all appropriate devices are set at the factory, and are monitored in offices, to print two-sided and in black ink to achieve additional savings, explained Steve Sherman, director of DLA Document Services.

Assessment

Assessments help an agency manage resources by first identifying current requirements and assets and then performing an in-depth analysis. The analysis matches the current staff and its printing requirements to an optimal shared-resource environment. DLA Document Services offers three assessment models — a physical on-site inventory, a Web-based data collection, and a customer-assisted inventory. The model employed is matched to the organization's structure, size and preference.

DLA Document Services plans to execute strategies to enable DON cost-savings, according to Michele Spiro, deputy director of operations for DLA Document Services. A significant part of the DON's savings will be achieved by eliminating and consolidating costly single-function desktop devices and replacing them with fewer, more-capable networked multifunctional devices.

DLA Document Services' expertise in conducting assessments will be used to determine the near optimal device configuration for DON commands and component organizations. This will ensure requirements are met, noted Spiro, who is responsible for the equipment management solutions program. The assessment process provides a benchmark of the existing device inventory and operating costs, identifies the organization's document equipment needs, and delivers a set of recommendations on the optimal mix of devices.

"Multifunctional devices help an organization do more with less by providing more functionality at a significantly lower total cost of operations," Spiro said. "The transition from single-function devices to multifunctional devices is a low-risk money saver that increases capacity and capability."



Contracting: Improving Competition

The policy also shifts the responsibility of contracting, supplying and managing office equipment from the DON to DLA Document Services, where it is one of DLA's core functions. Additionally, the necessary experience and support infrastructure are already available within DLA to achieve the savings goal, explained John Peterson, director of business for DLA Document Services.

"Our managed print services approach includes a professional and experienced staff, contracts that are leveraged Department of Defense-wide and competitively awarded, and a highly refined assessment process to determine the optimal device fleet solution," Peterson said. "We also integrate requirement fulfillment with on-demand print options and provide automated accounting, funding and billing."

Tracking Cost Savings

DLA Document Services will provide an easy to track cost savings capability to the DON CIO to ensure all savings are captured by command, organization and Echelon II command.

"This initiative capitalizes on DLA Document Services' core capabilities and infrastructure, as well as over 30 years of experience in managing office equipment for the DoD," Sherman said. "DLA Document Services has refined its expertise and skills over many years to become an effective life-cycle manager of all required services to deliver cost-efficient office devices across the DoD."

This policy will bring virtually all the DON's estimated 70,000 unclassified devices under the joint management of DON leadership and DLA Document Services. Together, the DON and DLA Document Services will provide centralized

management which will facilitate a complete capture of total annual costs.

Identifying Obstacles to Achieving Cost Savings

DLA Document Services has provided equipment management solutions services to the DON and DoD communities for decades. Based on this extensive experience, DLA Document Services has identified common obstacles. The primary obstacle is behavior-based preferences, including what is printed and how it is printed.

Challenges that are specific to the DON include the significant scope of the effort, which spans the entire department and the amount of time it will take to implement these changes – estimated at one to two years. Additional challenges include controlling the use of the government purchase card for CPFs, MFDs and associated services and consumables, and increasing competition by having more devices certified.

Transition

DLA Document Services, working closely with Navy and Marine Corps leadership, will prepare a final report identifying the optimal configuration of more capable and networked



equipment at the conclusion of the assessment. Assessments by DLA Document Services are vital to the transition; they provide current equipment inventories and proposed optimal fleet configurations for execution. The transition is dependent on current contract expiration dates, mission, availability of certified devices and delivery requirements. Transition timelines, including assessments, depending on scope, could range from 60 to 180 days.

The partnership between the DON and DLA Document Services to provide efficient procurement and management of unclassified networked and stand-alone copiers, printers, fax machines and scanners and multifunctional devices will help the DON achieve substantial savings, enhance device performance and improve customer service.

The partnership between the DON and DLA Document Services to provide efficient procurement and management of unclassified networked and stand-alone copiers, printers, fax machines and scanners and multifunctional devices will help the DON achieve substantial savings, enhance device performance and improve customer service.

For More Information:

Mandatory Guidance Regarding Management of Depart-

ment of the Navy Copiers, Printers, Fax Machines, Scanners, and Multifunctional Devices: <http://www.doncio.navy.mil/uploads/0130XQE94885.pdf>

DLA Document Services: <http://www.documentservices.dla.mil/>

The Federal Strategic Sourcing for Print Management Program (<https://strategicsourcing.gov/about-print-management>) is a national commodity management approach that will reduce the amount of printing equipment in use, minimize spending on paper and toner supplies across federal agencies, and brings the government closer to the current print management best practices exhibited in private industry. ●

THE NEWLY FORMED DON PRINT AND IMAGING SOLUTIONS TEAM is responsible for leading and overseeing the implementation of the DON CIO memo, "Mandatory Guidance Regarding Management of Department of the Navy Copiers, Printers, Fax Machines, Scanners, and Multifunctional Devices." The policy objective is to achieve cost savings by working closely with and leveraging established efficient procurement and managerial capabilities and processes of DLA Document Services.

A Night of Honor and Grace ... *A Tribute to Rear Adm. Grace M. Hopper*

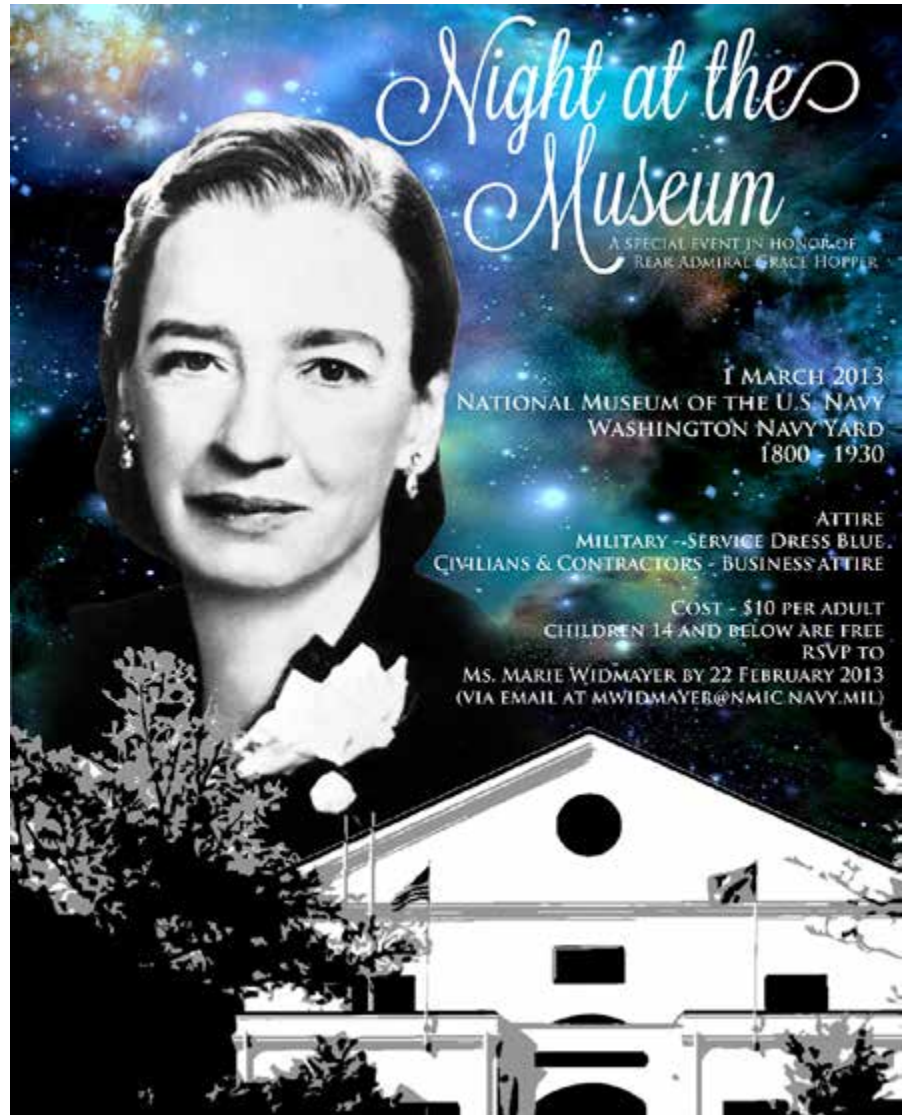
By Jennifer Ralston

On March 1, 2013, the first day of National Women's History Month, the Hopper Information Services Center, Office of Naval intelligence, celebrated the life and legacy of Rear Adm. Grace Hopper. Hopper's life embodied this year's theme: "Women Inspiring Innovation through Imagination." The tribute was held where the Navy honors its heritage's best — the National Museum of the United States Navy located on the Washington Navy Yard.

The event was called "Night at the Museum" and brought together more than 200 Hopper Information Services Center employees, their families, and members of the Navy Historical Foundation. Senior Information Dominance Corps leaders attended and included Vice Adm. Kendall Card, Deputy Chief of Naval Operations for Information Dominance (OPNAV N2/N6) and Rear Adm. Sam Cox, Director of the National Maritime Intelligence-Integration Office and Commander of ONI. It was a special night on many levels.

Key features of the official event included guest speaker and historian retired captain Dr. Dave Rosenberg, who provided colorful highlights from Hopper's life, a journey that spanned seven decades and produced long-lasting advances for the Navy and the nation. Dr. Rosenberg described Grace Hopper as the "Charles Lindbergh" of the computer age. Hopper earned a bachelor's degree in mathematics and physics (with honors) from Vassar College in 1928 and earned a Ph.D. in mathematics from Yale University in 1934, the first woman to do so.

She was a member of the Vassar faculty from 1931 to 1943, when she joined the Naval Reserve. Commissioned a lieutenant (junior grade) in 1944, she was assigned to the Bureau of Ordnance



and immediately became involved in the development of the then-embryonic electronic computer. Over more than four decades to follow, she was in the forefront of computer and programming language progress working in both academia and industry. She retained her Naval Reserve affiliation, attaining the

rank of commander before retiring at the end of 1966. Hopper was recalled to active duty in August 1967 and retired involuntarily at the age of 80 in 1986 as a rear admiral.

Hopper was a driving force behind the development of COBOL, or Common-Business-Oriented Language,

an innovative computer language that enabled computers to respond to words rather than just numbers. She served as a Navy spokesperson on computer technology around the nation and ultimately earned a staggering 37 honorary doctorate degrees from around the country. In addition to the Hopper Information Services Center, the Navy commissioned a destroyer, USS Hopper (DDG 70), in her honor.

Dr. Rosenberg described how Rear Adm. Hopper brought the Navy into the digital age through sheer intellect, grit and strength of personality. Her unique ability to make computers understandable to Sailors, admirals and service secretaries alike ensured the Navy was on the forefront of developing combat systems and command and control capabilities that gave the U.S. Navy a technological edge over the Soviets during the Cold War.

One of Grace Hopper's most famous teaching techniques involved handing out salvaged Bell telephone cables cut into 11.8-inch lengths that represented the distance light travels in one nanosecond. The demonstration was meant to show that one should not waste time, not even one nanosecond. Hopper was an exemplary mathematician, but an even more persuasive visionary, communicator and teacher. Despite her frail physical stature, she was a giant in her achievements, famous for speaking truthfully and guiding the Navy forward to meet its future.

After Dr. Rosenberg's remarks, Naval History and Heritage committee members played a video clip featuring Grace Hopper. The six-minute montage, which was produced by the Hopper team in concert with ONI's video reproduction staff, excerpted highlights from 360 minutes of video that had been digitized from analog tapes. The tapes were presented by Hopper's family members to the Naval Computer and Telecommunications Station San Diego. Some of the interviews were 35 years old. It was fortunate the Hopper team borrowed the tapes when they did because technicians indicated they would not have survived much longer in storage.



Sailors from the Hopper Information Services Center, Office of Naval intelligence, celebrated the life and legacy of Rear Adm. Grace Hopper at a special event for National Women's History Month March 1, 2013 at the National Museum of the United States Navy located on the Washington Navy Yard.

The clips culminated with a CBS "60 Minutes" special featuring Hopper. At the show's conclusion, clad in a Navy bridge coat, Hopper said, "I've received many honors and I'm grateful for them; but I've already received the highest award I'll ever receive, and that has been the privilege and honor of serving very proudly in the United States Navy."

History came alive in other ways during the event. Tables displaying Grace Hopper memorabilia, probably one of the largest collections in the world, were featured. Many of the items, such as commemorative plaques, gifts, certificates, a graduation hood, and a gold coin were on loan from NCTS San Diego. Also on display were rare photographs. Grace Hopper's alma mater recently gave the center almost all Hopper's student holdings, including her handwritten university grade sheets and a class of 1928 yearbook. It was a treasure trove of artifacts, most of which had never been seen together in one place before. We thank the Vassar staff, the commanding officer of NCTS San Diego and the Navy Historical Foundation for making the unveiling possible.

Commanding Officer of the Hopper Information Services Center Capt. Mike

Studeman, and host for the evening, summed up Hopper's life in this way, "She inspired generations of computer scientists and information systems technicians, not just in the Navy, but across the nation. She has been called 'Grandma COBOL,' 'The Grand Lady of Software,' 'Admiral of the Cyber Sea,' or simply 'Amazing Grace.' She was a very special naval officer, a great American, and a woman for the ages."

The evening affair was a fitting tribute to Grace Hopper and re-inspired a new generation of information technology professionals to follow in her footsteps. Her legacy will live long into the Navy's information dominance future. ●

HOPPER INFORMATION SERVICES CENTER provides mission-related information technology and services to the Office of Naval Intelligence, its Echelon III commands and the fleet. Web link: www.oni.navy.mil/commands/Hopper.html.

JENNIFER RALSTON is the Hopper Information Services Center history and heritage leader.

Modernizing and Securing Navy's MPTE Environment ... and Winning a DON IT/IM Excellence Team Award

MPTE Enterprise Information Management (EIM) scores a hit for the Navy

By the EIM Team and Sharon Anderson

In AN INITIATIVE THAT began in 2006 to improve the quality of data for force shaping and critical decision making, the Manpower, Personnel, Training and Education (MPTE) Enterprise Information Management (EIM) team developed a data roadmap to transform data management and integration. Then in fiscal year 2012, MPTE formally set out to further improve the quality of military human resources (HR) data and establish better rules regarding its use in Navy business decisions. While much of the work is transparent to Sailors on the deck plates, according to the MPTE EIM team, it will also result in better safeguarding of Sailor personally identifiable information (PII), and improve human resources business processes.

The scope of the challenge is huge because data resides in every MPTE system across the Navy and affects every Sailor throughout his or her Navy career. To say the MPTE domain is complex — is a vast understatement. The MPTE domain consists of approximately 66 systems, 887 applications and an estimated 240,000 data elements that have evolved over 40 years, according to the Sea Warrior Program (PMW 240), the primary information technology acquisition agent for non-tactical business operations addressing MPTE systems across the Navy.

According to BUPERS Command Information Officer, Stephen Hubbard, BUPERS, Navy Education and Training Command (NETC) and PMW 240 are

full partners in the MPTE data transformation effort.

This MPTE effort organizes resources — people, processes and technology — to meet the goals associated with the following 10 data management functions, according to Hubbard:

- Data Governance;
- Data Architecture Management;
- Data Development;
- Database Operations Management;
- Data Security Management;
- Reference and Master Data Management;
- Data Warehousing and Business Intelligence Management;
- Document and Content Management;
- Meta-data Management; and
- Data Quality Management.

Because data management was not a core competency in the Enterprise Information Management program, the team leveraged Gartner Research and the Data Management Association (DAMA) to plan the project, according to Hubbard. DAMA International is a non-profit, vendor-independent, global association of technical and business professionals dedicated to advancing the concepts and practices of information and data management. The team used DAMA for training and certification of the EIM Team.

A data consolidation effort was vital to the success of the project because there was no one single authoritative data source. This situation evolved over time and was exacerbated by the promise of the Defense Integrated Military Human Resources System

(DIMHRS), a joint HR service delivery system that never fully materialized. The team initiated MPTE's Authoritative Data Environment (ADE) project to implement the new Navy data governance standards, which included gathering data definitions, researching laws, regulations and policy, and identifying authoritative data sources. The effort is focused on establishing a single operational environment of quality personnel data that is authoritative, verifiable, and easily accessible to authorized people and applications.

The EIM team also began standardizing data elements for various Personnel/Pay Modernization Business Process Initiatives, such as the Navy Performance and Appraisal Reporting System (NPARS), Record of Emergency Data/Dependency Application (RED/DA) and Enhanced Drill Management (EDM).

Additionally, the EIM team was instrumental in implementing the MPTE EIM data transfer and compliance program aimed at controlling access to Sailor data by revamping the request process and information system access to raw HR data.

One of the greatest challenges, according to Hubbard, was getting customers to understand the need to control who can access data, and once they have it, to be able to properly control and protect it, in accordance with Navy policy and statutory requirements.

This major shift in data management reduces access to the minimum data required. The EIM team has also established a review process for all data transfers from MPTE information



MPTE EIM Team (in BUPERS-07) front row, left to right: Cmdr. Arjay Nelson (Data Steward, BUPERS-3) Colby Ritter (BUPERS Enterprise Architect, BUPERS-072), Teppi Dixon (EIM Team, BUPERS-072), Mary Buchschacher (EIM Team Lead, BUPERS-072), Kendrick Brown (BUPERS Enterprise Architect, BUPERS-072), Lauren Rummel (BUPERS Deputy CIO, BUPERS-07). Second row, left to right: Victor Kethireddy (EIM Team Data Architect, BUPERS-072), Bradley Friesen (EIM Team Data Modeler, BUPERS-072), Rebecca Robbins (EIM Team Contractor Lead, BUPERS-07) and Cmdr. Michael Raymer (EIM Team, BUPERS-072), Joseph Gibson (EIM Team, BUPERS-072) and Stephen Hubbard (BUPERS Chief Information Officer, BUPERS-07).

MPTE EIM members not pictured: Scott Pavelec (MPTE EIM Chief Data Steward, BUPERS-072), Nuria Hernandez (Enterprise Architect, OPNAV-N15), Rich Sweetman (Technical Advisor, PMW240), MPTE EIM Data Stewards: Deane Halvorsen (Workforce Development, NETC-N5), Larry Hoehn (Distribution, PERS-4), Glenn Stubbs (Distribution, PERS-4), David Hessling (Fleet & Family, OPNAV-N135), Terry Eisenhour (Personnel, PERS-3), Leo Metoyer (Personnel, PERS-3), Stan Keller (BUPERS-072), Karen White (Reserve Personnel, PERS-9), Robert Albritton (Reserve Personnel, PERS-9), John Nickle (Position Management, NAVMAC), Cathy Mills (Position Management, NAVMAC), Mary Naifeh (Recruiting Accessions, CNRC-N-6), Jeffrey Keating (Recruiting Accessions, CNRC-N-6), Teresa Price (Recruiting Accessions, CNRC-N-6), Gail Lile (NPRST), Tate Brown (NPRST), James Stuart (BUPERS-3), Bill Ragatz (BUPERS-3), Mike Hollister (PMO), Linda Jardine (PMO), Linda Freeman (Financial Management, OPNAV-N10), Edward Timko (Financial Management, OPNAV-N10), Tom Bonanno (Training Management, NETC-N7), Angie McDonough (Training Management, NETC-N7). EIM Team (BUPERS-072): Larry Francis, Mary Kay Levie, Mary Beth Novack, James Murray, Sam Shamblyn, Thomas Curry, Wayne Hilburn, Robert Cross and Kathy Eisenhour.

systems, resulting in increased security of Sailor data.

Implementing large scale, complex data environments requires specialized skills.

"In June 2010, we were able to recall Navy Reserve Capt. Mike Rominski to active duty for three years to work on the project," Hubbard said. Capt. Rominski has experience as a civilian working with large scale data environments for a Blue Cross Blue Shield provider in the Midwest.

The cross-functional EIM team is made up 28 government and 12 contractor personnel supporting the data interest of each of the lines of business and cross-functional integrators. Deputy Chief of Naval Operations for Personnel, Education and Training (OPNAV N1), BUPERS, NETC, Navy Personnel Command (NPC), Commander, Navy Recruiting Command (CNRC), Navy Manpower Analysis Center (NAVMAC) and PMW 240 have all provided subject matter experts known as data stewards.

Data stewards work with a technical advisor; enterprise, business and data architects, data custodians and a team of 12 data analysts to execute the various activities of data management. Through monthly meetings and collaborative communication the team addresses data issues, projects and activities across the MPTE domain promoting a holistic point of view of the data requirements that support Navy HR business processes and decision making.



The Department of the Navy Chief Information Officer announced the winners of the 2013 DON IM/IT Excellence Awards in January. The EIM Board and Team was awarded a 2013 DON IM/IT Excellence Team Award and received the following citation.

Manpower, Personnel, Training & Education (MPTE) Enterprise Information Management Board & Team, Bureau of Naval Personnel (BUPERS): for proactively addressing enterprise management and governance of MPTE data assets, and controlling and protecting personally identifiable information while supporting business requirements. The team promoted data as an enterprise asset with assigned accountability and responsibility throughout its lifecycle. The team educated MPTE personnel and instilled a culture of collaboration throughout the organization, inspiring confidence in data quality that results in greater trust in MPTE data when making decisions.

These modernization efforts are actually shrinking the IT infrastructure and could reduce costs, according to Chief Data Steward and BUPERS Information Resources Management (IRM) Branch Head (BUPERS 072), Scott Pavelec.

Pavelec explained that the employment of an enterprise service bus will actually facilitate movement of data between the myriad pay and personnel systems. An enterprise service bus is a software architecture model used for designing and implementing the interaction and communication between mutually interacting software applications in a service-oriented architecture. As a software architecture model for distributed computing, it is a specialty variant of the more general client server software architecture model and promotes agility and flexibility with regard to communication and interaction between applications. Its primary use is in enterprise application integration of heterogeneous and complex landscapes — which exactly describes the Navy's MPTE environment.

"We are moving toward an enterprise service bus which will reduce the point-to-point interface [between systems, Pavelec said. "It improves interconnection between multiple systems to exchange data. It acts as a traffic manager between the systems and ensures the

quality of data and confidence in its authenticity and reuse."

In January, the Department of the Navy Chief Information Officer announced that the MPTE Enterprise Information Management Board and Team was awarded a DON IT/IM Team Excellence Award for proactively addressing enterprise management and governance of MPTE data assets, and controlling and protecting personally identifiable information while supporting business requirements. The announcement stated that the team promoted data as an enterprise asset with assigned accountability and responsibility throughout its life cycle. The team educated MPTE personnel and instilled a culture of collaboration throughout the organization, inspiring confidence in data quality that results in greater trust in MPTE data when making decisions.

The team is not resting on its laurels; however, and efforts to continuously improve the accessibility and security of data are ongoing. The team is establishing a formal program for data management and drafted several policies on the handling and transfer of data. They have implemented a meta data management tool/repository that will assist in the standardization of MPTE data assets and document authoritative data

sources. The team is also working on a data quality program that will establish standards and measurement of data quality in MPTE systems.

"We want the Navy to look to MPTE OPNAV N1 as the force provider of military HR data," Hubbard said. ●

Navy Personnel Command/BUPERS

www.public.navy.mil/bupers-npc/Pages/default.aspx.

Sea Warrior Program Office (PMW 240)

manages a complex portfolio of information technology (IT) systems to support Navy human resource management, criminal justice, Fleet Support, afloat business applications, Navy and DoD portfolio management, DON administration, and joint aviation aircraft scheduling.

The PMW 240 Program is part of the Navy Program Executive Office for Enterprise Information Systems (PEO-EIS), which develops, acquires, fields, and sustains enterprise network, business, and Fleet support IT systems for the warfighters of the Navy and Marine Corps. For more information, visit www.public.navy.mil/spawar/PEOEIS/SWP/Pages/default.aspx.

The National Initiative for Cybersecurity Careers and Studies

Online resources for training and education, scholarships and more

By CHIPS Magazine

The NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES (NICCS)

aims to be a single online resource for cybersecurity education and career information. With 556 million people per year becoming victims of cybercrime at a rate of 1.5 million per hour, 18 people per second, and with an annual price tag of \$110 billion, cybercrime costs the world significantly more than the global black market in illegal drugs. Securing cyberspace means we, as a country, must develop a technologically skilled workforce, a cyber-savvy public, and an effective pipeline of future employees. Billions of dollars are spent on new technologies to help secure the United States in cyberspace, but it will take a national strategy, similar to the effort to upgrade science and mathematics education in the 1950s, to meet the challenge of securing cyberspace today.

Now is the time to begin a coordinated national effort focused on cybersecurity awareness education, training and professional development. To address this need, the National Initiative for Cybersecurity Education was established. The mission of NICE is to enhance the overall cybersecurity posture of the United States by accelerating the availability of educational and training resources designed to improve the cyber behavior, skill and knowledge of every segment of the population — enabling a safer cyberspace for all.

To make cybersecurity materials more readily available, the government developed NICCS. NICCS underscores all four NICE components and intends to serve as a national resource for

government, industry, academia and the general public to learn about cybersecurity awareness, education, careers and workforce development opportunities.

The vision of NICCS is to build a national resource to elevate cybersecurity awareness and help the American public to adopt a culture of cyberspace security and to build a competent cybersecurity workforce.

To continue advancing the content and information provided on the NICCS portal, the NICCS Supervisory Office is working closely with its partners to provide the most up-to-date guidance, recommendations and best practices on cybersecurity awareness, education, careers and training programs. As part of that effort, NICCS houses a Cybersecurity Education and Training Catalog that allows users to find the training they need to advance their careers.

Everyone knows cyber is the hot field to be in right now. But now that you're in, how can you get the training you need? The National Initiative for Cybersecurity Careers and Studies can help. The catalog allows users to search for training or certifications by a variety of means, including keyword search, training provider and proficiency level. Later this year, the catalog will contain industry training that will make it a more robust and helpful resource. If you're interested in learning more about the catalog, please contact the NICCS Supervisory Office at niccs@hq.dhs.gov.

In the meantime, you are encouraged to explore the NICCS and the catalog at www.niccs.us-cert.gov.

Developed by the Department of Homeland Security, NICCS offers tools and training and creates awareness

for cyber competitions, camps and clubs. The cybersecurity career field is constantly growing and changing. There are an increasing number of cybersecurity degree programs that can lead to careers in the cybersecurity field. Many of these degree programs fall within the five traditional subdisciplines of computing: computer science, computer engineering, information systems, information technology and software engineering.

The government, colleges, and many corporations and non-profit organizations offer scholarships for students to attend college. In addition to the scholarships listed on the NICCS website (<http://niccs.us-cert.gov/scholarship-opportunities>), the Department of Homeland Security sponsors the Cyber Corps: Scholarships for Service program (<http://niccs.us-cert.gov/education/cybercorps@-scholarship-service-sfs>). The SFS program is a publicly funded scholarship co-sponsored by DHS and the National Science Foundation. This program provides scholarships that fully fund the typical costs that students pay for books, tuition, and room and board while attending an approved institution of higher learning. Additionally, participants receive stipends of up to \$8,000 for undergraduate and \$12,000 for graduate students. Scholarships are equivalent to years of service in the government.

In the future, scholarship opportunities will be integrated into a searchable database and aligned with the National Cybersecurity Workforce Framework.

For more information about the NICCS, go to <http://niccs.us-cert.gov/>. ●

Robert Scott Jack II

Deputy Director, Deputy Chief Information Officer (CIO) for Command, Control, Communications and Computers (C4) Headquarters, Marine Corps

As deputy director and CIO for C4, Mr. Jack formulates and provides broad policy guidance governing information technology, cyber security, and communications infrastructure and applications in support of the U. S. Marine Corps. Prior to his current assignment, Mr. Jack served as the Director of Communications and Information, Headquarters Air Force Global Strike Command, Barksdale Air Force Base, La. Mr. Jack was appointed to the Senior Executive Service in 2005 with 33-plus years of federal civilian service and six years of active duty with the U. S. Air Force. He entered the Air Force Reserve in July 1982, retiring from the Reserve in December 2000 with more than 24 years of service in various assignments at Wright-Patterson AFB, Ohio; Scott AFB, Ill.; and Seymour Johnson AFB, N.C. Mr. Jack responded to questions in writing in early April.



Robert Scott Jack II

Q. Can you discuss your communications work for the Air Force and how it may be similar or different in regard to your new position with the Marine Corps?

A. I would say that my 39-plus years of working across numerous Air Force, DoD, and other federal agencies gave me the universal skill sets to hit the ground running upon being assigned as the Deputy Director of Command, Control, Communications and Computers. The prime role of my position is to deliver information and communications capability to the warfighter. In this assignment, the warfighter is the Marine Air-Ground Task Force, or MAGTF, and the Marines assigned to its elements.

The nuance between my previous assignments and my current role is the MAGTF operates in an amphibious/expeditionary environment where bandwidth is a very constrained resource. This reality drives the need for every system, service, and application deployed forward with the MAGTF to have the ability to reach back to a garrison or enterprise authoritative data source. To achieve

this, our systems must be bandwidth lean, light in weight, and efficient in their power consumption.

One other factor that will define my tenure in this position is the extremely constrained fiscal environment. The measure of merit for the next few years will be to maximize the return on investment [for] every dollar we get allocated. With that said, we are also going to maximize those capabilities we already own. Lastly, our USMC C4/IT efforts will be focused on meeting the tenets of joint interoperability to achieve mission assurance across the spectrum of operations.

Q. The goals of Data Center Consolidation are to shift IT investments to more efficient computing platforms and technologies; reduce the operation and maintenance costs of data center hardware and software; reduce the overall energy and footprint of government data centers; and increase the overall IT security posture. Can you discuss the Marine Corps' progress in achieving these goals?

A. Improving the efficiency of our computing platforms is a top priority. Since May 2012, when the Marine Corps Private Cloud Computing Environment (PCCE) Strategy was published, the Marine Corps has been focusing on the benefits of developing a private cloud. One of the forces driving cloud development is Marine Corps Enterprise Information Technology Services (MCEITS), which provides enterprise IT services contained within an application and data hosting environment with supporting communications, computing network information assurance, and enterprise services infrastructure. MCEITS will be the catalyst for moving the Marine Corps toward an integrated, consistently managed enterprise hosting environment that complies with the Office of Management and Budget (OMB) Federal Data Center Consolidation Initiative (FDCCI).

One of the key tenets put forward in the Marine Corps Private Cloud Computing Environment Strategy focuses specifically on IT efficiencies and the concept of green IT. Some of the key selling points include servers and their

Improving the efficiency of our computing platforms is a top priority. Since May 2012, when the Marine Corps Private Cloud Computing Environment (PCCE) Strategy was published, the Marine Corps has been focusing on the benefits of developing a private cloud. One of the forces driving cloud development is Marine Corps Enterprise Information Technology Services (MCEITS), which provides enterprise IT services ...

processing power being better leveraged, promoting effective online collaboration, and utilizing storage virtualization technology, which allows the end user to pool storage resources and easily scale storage resources as needed.

Controlling access to data in the cloud will be a critical factor; however, the benefit of establishing a private cloud is that the network is a contained environment that enables seamless, secure command and control functions even in locations of constrained bandwidth.

Q: How has virtualization and system and application rationalization supported the Marine Corps' Data Center Consolidation efforts to achieve additional efficiencies?

A: The Marine Corps is focused on virtualization, as well as system application inclusion to the Marine Corps Enterprise Information Technology Services environment. Using an inclusion process and leveraging the capital planning and investment control (CPIC) process, the Marine Corps will develop relevant metrics and assess proposed services/applications for enterprise deployment onto MCEITS.

Q: Is the Marine Corps still using a regionalization strategy to consolidate and operate management of the Marine Corps Enterprise Network? This effort was designed specifically to support Marine Expeditionary Forces and

supporting establishment organizations — can you talk about how it works? Are the regionalized centers designed to be interoperable with the Defense Department enterprise using the Joint Information Environment (JIE) framework?

A: My Department, Command, Control, Communications and Computers (C4) is currently working on a Unification Campaign Plan that addresses specific objectives in support of the U.S. Marine Corps Regionalization Strategy. Executing the Marine Corps Regionalization Strategy will evolve the Marine Corps Enterprise Network (MCEN) into a tightly integrated, agile, defensible and survivable network capable of maintaining a superior security posture, supporting highly distributed operations for improved response to our warfighters, and operating the supporting establishment as an efficient and effective business enterprise.

Additionally, by executing the requirements of the Office of Management and Budget Federal Data Center Consolidation Initiative through the Regionalization Strategy, the Marine Corps will increase its operational efficiency and reduce total cost of ownership for IT Infrastructure assets. This will be achieved through the reduction of energy consumption, the real estate footprint, physical and IT security costs, and hardware maintenance costs. We will adopt JIE standards to ensure interoperability as they are developed and promulgated.

The MCEN is the Marine Corps'

network-of-networks and approved interconnected network segments. It comprises people, processes, logical and physical infrastructure, architecture, topology, and cyberspace operations.

Q: Can you talk about the progress in establishing the MCEITS framework which hosts an application and data hosting environment with supporting communications, computing network information assurance, and enterprise services infrastructure? Specifically can you discuss how many applications have been migrated and how much savings has been achieved?

A: Additional Marine Corps applications are scheduled to move onto the MCEITS environment during fiscal year (FY) 13. These include several applications that were previously hosted in the Defense Information Systems Agency Defense Enterprise Computing Centers. The current plan is to have up to 15 applications hosted on the environment by the end of FY13, and we expect this number to grow through FY17. The focus of MCEITS has always been on efficiency, consolidation and cost avoidance. Unfortunately, like many other programs across the Department of Defense, the MCEITS program is also facing the challenges associated with potential funding reductions across the Fiscal Year Defense Plan.

Q: I read that the Marine Corps is conducting an analysis of information and data requirements

to shape the information elements needed and then to apply appropriate resources to address these needs. Do you have the results of the analysis and plan of action yet? Does the Marine Corps have a data strategy and how does it relate to your application rationalization strategy?

A. The Marine Corps has started analyzing the information and data requirements for the Business Mission Area, which will continue in the foreseeable future. Marine Corps Order (MCO) 5231.3, published in 2009, brought forward a new data strategy that aligned to the DoD Net-Centric Data Strategy, which was intended to make data more visible, accessible, understandable, trusted, and interoperable. MCO 5231.3 complements other Marine Corps policies related to the application rationalization process by mandating the registration of authoritative data sources, while at the same time identifying and eliminating unnecessary data repositories.

Q. Can you describe any other initiatives the Marine Corps is working on to further reduce business IT spending and increase operating efficiencies?

A. Mobile Device Strategy — Historically, the ability to use mobile devices on Marine Corps IT networks has been limited to those individuals deemed as privileged or mission-essential users; however, with an increase in recent trends towards teleworking and mobile computing (see DoD Instruction 1035.01 that addresses using personally owned computers on unclassified DoD systems/networks), the DOD is starting to shift to an environment where mobile access to networks and information is no longer limited by this parameter.

In turn, the Marine Corps also recognizes the trend of evolving information needs, as well as the need to provide an agile method of



130321-M-OH054-015 (Left) Lance Corporals Nathaniel E. Winstead and Tony M. Chavez, both radio operators with 13th Marine Expeditionary Unit, log radio checks within the command operations center, set up aboard Marine Corps Base Camp Pendleton, March 21, 2013. From March 14-21, the 13th MEU set up their COC for a MEU Exercise to better train for their Western Pacific deployment this year. Official Marine Corps photo by Sgt. Christopher O'Quin.

meeting those needs. To align with recent DoD strategies and increasing mobile workforce requirements for IT consumerization, C4 has been leading the development of the Marine Corps Mobile Device Strategy. The strategy, which is currently in the final stages of approval, intends to establish a secure mobile framework that enables the Marine Corps to identify mobile device capability requirements, leverage existing resources, and promote the concept of using approved personally owned mobile devices.

In order to achieve the strategy, we have identified the following four goals: (1) Establish a Secure Mobile Framework; (2) Transition the Unclassified Mobile Device Infrastructure to a Cost Effective and Platform Agnostic Environment; (3) Collaborate with DoD and Industry Partners to Develop a Classified Mobile Device Capability; and (4) Incorporate Personally Owned Mobile Devices.

Hosted Virtualized Desktop —

C4 recognizes and understands its responsibility to make sure IT services are being distributed across the enterprise in a manner that is both

fiscally and operationally efficient. In recent years, C4 has demonstrated this through the development of strategies that focus on moving towards a more cost-effective organizational IT model. For example, the Marine Corps Private Cloud Computing Environment Strategy envisions a future where services can be accessed from anywhere across the Marine Corps information environment at any time, via the Marine Corps Enterprise Network to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can rapidly be provisioned and released with reduced management effort. As a result of this strategy, capabilities like desktop virtualization can be leveraged to employ a more effective way of managing user computers, provide users with the ability to access hosted desktops remotely, and generate savings in total cost of ownership from the consolidation of physical servers. We are currently in discussions with industry partners to establish a way-ahead on the implementation of this capability at the enterprise level. ●



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/.

Software Categories for ESI

IT Asset Management

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 Dec 16

CONTACT: CHESS Helpdesk (888) 232-4405 (peoeis.pdchess.helpdesk@us.army.mil)

WEB LINK: <https://chess.army.mil/Contract/Details/100083>

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

CONTACT: CHESS Helpdesk (888) 232-4405 (peoeis.pdchess.helpdesk@us.army.mil)

WEB LINK: <https://chess.army.mil/Contract/Details/100084>

DLT

BDNA ASSET MANAGEMENT: Provides asset management software 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 (Call for extension information.)

CONTACT: CHESS Helpdesk (888) 232-4405 (peoeis.pdchess.helpdesk@us.army.mil)

WEB LINK: <https://chess.army.mil/Contract/Details/100081>

Flexera

FLEXERA PRODUCTS: Flexera is a provider of of strategic solutions for application usage management. Flexera software helps application producers and their customers strategically manage application usage to achieve continuous compliance, optimized usage and maximized value.

CONTRACTORS:

Flexera DLT Solutions (N00104-12-A-ZF43); Small Business; (703) 584-3120

Flexera immixTechnology, Inc. (N00104-12-A-ZF44)

ORDERING EXPIRES: 21 Oct 15

WEB LINKS: Flexera DTL Solutions

www.esi.mil/contentview.aspx?id=319&type=2

Flexera Immix Group

www.esi.mil/contentview.aspx?id=320&type=2

Database Management Tools

Microsoft Products

MICROSOFT DATABASE PRODUCTS: See information under Office Systems on page 61.

Oracle (DEAL-O)

ORACLE PRODUCTS: Provides Oracle database and application software licenses, support, training and consulting services.

CONTRACTORS:

Affigent (W91QUZ-09-A-0001)

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

immixTechnology, Inc. (W91QUZ-08-A-0001);

Mythics, Inc. (W91QUZ-06-A-0003);

Small Business; (757) 284-6570

ORDERING EXPIRES:

Affigent: 29 Jun 16

DLT: 31 Mar 17

immixTechnology: 02 Mar 16

Mythics: 13 Aug 13

AUTHORIZED USERS: This has been designated as a DoD ESI and GSA Smart-BUY contract and is open for ordering by all U.S. federal agencies, DoD components and authorized contractors.

CONTACT: CHESS Helpdesk (888) 232-4405 (peoeis.pdchess.helpdesk@us.army.mil)

WEB LINK: https://chess.army.mil/CMS/A/SW_DEAL_O_HPG

SPECIAL NOTE TO NAVY USERS: See the information provided on page 62 concerning the Navy Oracle Database Enterprise License under Department of the Navy Agreements.

Sybase (DEAL-S)

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

CONTRACTOR: Sybase, Inc. (DAAB15-99-A-1003); (800) 879-2273; (301) 896-1661
ORDERING EXPIRES: 15 Apr 13 (Please phone for extension information.)

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/Contract/Details/100020>

Enterprise Application Integration and Architecture Tools

IBM Software

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) 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.

CONTRACTORS:

immixTechnology, Inc. (DABL01-03-A-1006); Small Business; (703) 752-0641 or (703) 752-0646

ORDERING EXPIRES: 02 Mar 16

WEB LINK:

immixTechnology, Inc.
<https://chess.army.mil/Contract/Details/100013>

Oracle/Sun Support

Total Warranty (SSTEWE2)

SUN SUPPORT TOTAL WARRANTY 2

(SSTEWE2): Offers Sun hardware and software support, extended warranty, maintenance, education, incidental hardware and software, and system engineering and support services.

CONTRACTORS:

Alliance Technology Group, LLC (HC1028-13-A-0005); (703) 307-5157

Dynamic Systems, Inc. (HC1028-13-A-0006); (801) 444-0008

Sterling Computers Corp. (HC1028-13-A-0007); (605) 242-4017

ORDERING EXPIRES: 27 Mar 14

WEB LINKS:

Alliance Technology Group
www.esi.mil/contentview.aspx?id=323&type=2
Dynamic Systems, Inc.
www.esi.mil/contentview.aspx?id=324&type=2
Sterling Computers Corp.
www.esi.mil/contentview.aspx?id=325&type=2

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/Contract/Details/100091>

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: 25 Jun 13

WEB LINK:

<https://chess.army.mil/Contract/Details/100040>

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/Contract/Details/100035>

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: 31 Mar 17

WEB LINKS:

Quest Software, Inc.

<https://chess.army.mil/contract/details/100038>

DLT Solutions

<https://chess.army.mil/contract/details/100045>

Enterprise Resource Planning

Oracle

ORACLE: See information under Database Management Tools on page 58.

RWD Technologies

RWD TECHNOLOGIES: Provides a broad range of integrated software products 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); (404) 845-3624

ORDERING EXPIRES: 14 Apr 15

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

SAP

SAP PRODUCTS: Provides software licenses, software maintenance support, information technology professional services and software training services.

CONTRACTORS:

SAP Public Services, Inc. (N00104-08-A-ZF41); Large Business; (202) 312-3515

Advantaged Solutions, Inc. (N00104-08-A-ZF42); Small Business; (202) 204-3083

Carahsoft Technology Corp. (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 Public Services, Inc.

www.esi.mil/contentview.aspx?id=154&type=2

Advantaged Solutions, Inc

www.esi.mil/contentview.aspx?id=155&type=2

Carahsoft Technology Corp.

www.esi.mil/contentview.aspx?id=156&type=2

Oakland Consulting Group

www.esi.mil/contentview.aspx?id=157&type=2

Information Assurance Tools

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 users.

ORDERING EXPIRES: 08 Sep 16

WEB LINK: <https://chess.army.mil/Contract/Details/100055>

Collaboration

Collaboration

COLLABNET: Provides CollabNet Licenses, CollabNet Support for TeamForge and Subversion, Consulting Services and Training Services at a discount up to 5 percent. CollabNet SourceForge Enterprise integrates software configuration management, issue tracking, project management, and collaboration tools into a single Web-browser based ALM platform that empowers distributed teams to deliver great software.

CONTRACTOR:

Carahsoft Technology Corp. (HC1047-11-A-0100)

ORDERING EXPIRES: 30 Mar 16

WEB LINK:

www.esi.mil/contentview.aspx?id=245&type=2

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, NI-ACAP, NIST or DCID processes. Xacta's AMHS provides automated, Web-based distribution and management of messaging across the enterprise. platform that empowers distributed teams to deliver great software.

CONTRACTOR:

Telos Corp. (FA8771-09-A-0301); (703) 724-4555

ORDERING EXPIRES: 24 Sep 14

WEB LINK:

www.esi.mil/contentview.aspx?id=205&type=2

Lean Six Sigma Tools

iGrafx Business Process

Analysis Tools

IGRAF: Provides software licenses, maintenance and media for iGrafx Process for Six Sig-

ma 2007; iGrafx Flowcharter 2007; Enterprise Central; and Enterprise Modeler.

CONTRACTOR:

Softchoice Corp. (N00104-09-A-ZF34); (416) 588-9002, x 2072

Softmart, Inc. (N00104-09-A-ZF33); (610) 518-4192

SHI (N00104-09-A-ZF35); (732) 564-8333

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: A DoD-wide blanket purchase agreement was established non-competitively with Minitab, Inc. to provide 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-AZF30); (800) 448-3555

AUTHORIZED USERS: This BPA is open for ordering by all Department of Defense (DoD) authorized 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:

immix Group, Inc. ((N00104-08-A-ZF31); Small Business; (703) 663-2702

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 Digital Media Product

ADOBE DIGITAL MEDIA PRODUCTS: The Department of the Navy IT Umbrella Program and the Naval Supply Systems Command, Weapon Systems Support, Mechanicsburg, Pa., have established multiple Enterprise Agreements for Adobe software products on behalf of the DoD ESI. This agreement expires 6/30/2016 (inclusive of BPA option ordering periods). Products include licenses, upgrades and maintenance. The Adobe BPAs were awarded non-competitively against GSA schedule. 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).

DOD contractors are encouraged to use the ESI agreements when approved by their contracting officer in accordance with FAR 51. Note: Ordering under this vehicle is not limited to the products listed on the BPA Price List (Attachment A). Any Adobe Software product that is on the vendor's GSA schedule may be procured using this vehicle at a discount below GSA pricing, including the Acrobat Suite, InDesign and Web Premium, Fireworks, Lightroom, ColdFusion Standard, etc. Go to www.esi.mil/agreements.aspx?id=301.

CONTRACTORS:

Carahsoft Technology Inc. (N00104-12-A-ZF31); (703) 871-8577

CDW-G. (N00104-12-A-ZF32); (800) 808-4239

Dell (N00104-12-A-ZF33); (224) 543-5314

Emergent, LLC (N00104-12-A-ZF34); (757) 493-3020

GovConnection, Inc. (N00104-12-A-ZF35); (800) 800-0019 x78007

Insight (N00104-12-A-ZF36); (800) 862-8758

SHI International Corp. (N00104-12-A-ZF37); (732) 868-5926

Softchoice (N00104-12-A-ZF38); (877) 333-7638 x323260 or x323228

Softmart (N00104-12-A-ZF39); (800) 628-9091 or (610) 518-4375

ORDERING EXPIRES: 30 Jun 16

WEB LINKS:

Carahsoft Technology Inc.

www.esi.mil/contentview.aspx?id=301&type=2

CDW-G

www.esi.mil/contentview.aspx?id=302&type=2

Dell

www.esi.mil/contentview.aspx?id=303&type=2

Emergent, LLC

www.esi.mil/contentview.aspx?id=304&type=2

GovConnection

www.esi.mil/contentview.aspx?id=305&type=2

Insight

www.esi.mil/contentview.aspx?id=306&type=2

SHI International Corp.

www.esi.mil/contentview.aspx?id=307&type=2

Softchoice

www.esi.mil/contentview.aspx?id=308&type=2

Softmart

www.esi.mil/contentview.aspx?id=309&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); (703) 871-8556

ORDERING EXPIRES: 14 Jan 14

WEB LINK:

www.esi.mil/contentview.aspx?id=186&type=2

Autodesk

AUTODESK: Provides software licenses for more than two dozen AutoCAD and Autodesk products.

CONTRACTOR: DLT Solutions (N00104-12-A-ZF30)

ORDERING EXPIRES: 20 Nov 14

Web Link: www.esi.mil/contentview.aspx?id=266&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); (312) 705-1889 or (703) 621-8211

Dell (N00104-02-A-ZE83); (224) 543-5306 or (512) 728-2277

EnPointe Gov., Inc. (N00104-12-A-ZF42); (310) 337-5200 x2640 or (310) 337-5200 x5496

GovConnection (N00104-10-A-ZF30); (301) 340-3407 or (800) 998-0019

GTSI (N00104-02-A-ZE79); (703) 502-2112 or (703) 502-2156

Hewlett-Packard (N00104-02-A-ZE80); (800) 727-5472 or (402) 758-3304

Insight Public Sector, Inc. (N00104-02-A-ZE82); (800) 862-8758 or (443) 534-6457

SHI (N00104-02-A-ZE86); (800) 527-6389 or (732) 564-8333

Softchoice (N00104-02-A-ZE81); 312-655-9002 x323260 or (312) 655-9002 x323228

Softmart (N00104-02-A-ZE84); (800) 628-9091 or (610) 518-4192

ORDERING EXPIRES: 01 Jul 13

WEB LINKS:

CDW Government, LLC

www.esi.mil/contentview.aspx?id=177&type=2

Dell

www.esi.mil/contentview.aspx?id=176&type=2

EnPointe Gov., Inc.

www.esi.mil/contentview.aspx?id=318&type=2

GovConnection

www.esi.mil/contentview.aspx?id=229&type=2

GTSI

www.esi.mil/contentview.aspx?id=235&type=2

Hewlett-Packard

www.esi.mil/contentview.aspx?id=114&type=2

Insight Public Sector, Inc.

www.esi.mil/contentview.aspx?id=173&type=2

SHI

www.esi.mil/contentview.aspx?id=178&type=2

Softchoice

www.esi.mil/contentview.aspx?id=174&type=2

Softmart

www.esi.mil/contentview.aspx?id=175&type=2

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 De-

fense 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 following websites 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).

CONTRACTOR: August Schell Enterprises (www.augustschell.com)

Download Site: <http://redhat.augustschell.com>

GCSS users: www.disa.mil/gcssj

ORDERING EXPIRES: Nov 13; All downloads provided at no cost.

WEB LINK: www.disa.mil

Red Hat

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 Corp. (HC1028-09-A-2004)

DLT Solutions, Inc. (HC1028-09-A-2003)

Ordering Expires:

Carahsoft: 09 Feb 14

DLT Solutions, Inc.: 17 Feb 14

WEB LINKS:

Carahsoft Technology Corp.

www.esi.mil/contentview.aspx?id=201&type=2

DLT Solutions, Inc.

www.esi.mil/contentview.aspx?id=200&type=2

Research & Advisory

Gartner Inc.

GARTNER INC.: 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. The BPA Ordering Period commences 12/01/2006 and is effective for the term of the GSA FSS Schedule. The BPA will be reviewed annually and is contingent upon the Contractor maintaining or renewing GSA Schedules GS-35F-5014H.

CONTRACTOR:

Gartner Inc. (N00104-07-A-ZF30); (703) 387-5676 or (703) 387-5704;

ORDERING EXPIRES: 31 Mar 18

WEB LINK:

www.esi.mil/contentview.aspx?id=171&type=2

Forrester Research

FORRESTER RESEARCH: Forrester Research is an independent technology and market research company which focuses on delivering research-based services to their customers. They align research, data, advisory and consulting services to their customer agendas and help customers understand existing and potential impacts of technology. The DoD ESI BPA contract with Forrester is available to all DoD components including the Intel community and offers discounts of up to 5% from GSA prices. Forrester will work with the various DoD components to create a customized package that fits each components' needs and is based specifically on their requirements. The BPA will be reviewed annually and is contingent upon the Contractor maintaining or renewing GSA Schedules GS-35F-4900H.

CONTRACTOR:

Forrester Research (N00104-12-A-ZF41); (703) 584-2626 or (703) 584-2628

Ordering Expires: 10 Aug 2013

WEB LINK: www.esi.mil/contentview.aspx?id=314&type=2

Department of the Navy Agreements

Oracle (Deal-O)

Database Enterprise License

for the Navy

On Oct. 1, 2004 and May 6, 2005, the Navy established the Oracle Database Enterprise License, effective through Nov. 1, 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 (SPAWAR/SCEN) 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:

www.esi.mil/agreements.aspx?id=139

Microsoft Enterprise Licensing

The Department of the Navy signed an enterprise licensing agreement July 5, 2012. All procurement of Microsoft brand software licenses including software assurance (SA), SA only, and subscriptions and SA-step up (SASU) for desktop and server based products must be acquired through the Microsoft DON enterprise licensing agreement (ELA) if that product is offered by the DON ELA.

This agreement, valid through 2015, consolidates previous Microsoft enterprise licenses; and, therefore, optimizes cost savings by leveraging the full purchasing capacity of the department. Acquired licenses and SA must be compatible and interoperable with existing DON hardware and technology equipment. The maximum dollar value, including the base period and two option periods, is \$700 million.

Ordering guidance: All Navy and Marine Corps procurement actions for information technology software must go through their respective processes identified at the Program Executive Office for Enterprise Information Systems PMM-110 portal page: <https://www.peois.portal.navy.mil/pmm110/default.aspx>. Since this is a dynamic environment, other policies may be added with little notice. Information about ordering products via DON ELAs can also be found at this site.

Use of DON ELAs, where available, is mandatory by all DON organizations and programs per the joint memo "Mandatory Use of DON Enterprise Licensing Agreements," which was signed Feb. 22, 2012, by the Department of the Navy Chief Information Officer, the Assistant Secretary of the Navy for Research Development and Acquisition, and the Assistant Secretary of the Navy for Financial Management and Comptroller.

WEB LINKS:

DON CIO

www.doncio.navy.mil/PolicyView.aspx?ID=3777

www.doncio.navy.mil/ContentView.aspx?ID=3778



www.esi.mil

FLEXERA SOFTWARE NOW AVAILABLE THROUGH ESI

On behalf of the DoD Enterprise Software Initiative (DoD ESI), the Department of the Navy SPAWARSCEN Pacific Code 55390 and the Naval Supply Systems Command, Weapon Systems Support, Mechanicsburg, Pa., have awarded blanket purchase agreements (BPAs) with DLT Solutions and Immix Group for Flexera IT Asset Management Software. Flexera Software provides technology that supports application producers and enterprises in increasing application usage and the value they derive from their licensed software. Among the products available through the DoD ESI BPAs are the FlexNet Publisher license manager and the InstallAnywhere and InstallShield installation packages. The DoD ESI BPAs for Flexera software are available to all DoD components including the Intel Community and offer 20 percent minimum discount off GSA pricing for all product purchases. Maintenance, training and professional services discounts will be less. For more information, go to www.esi.mil/agreements.aspx?id=319. ●

Who Can Use ESI?

- DOD ESI'S AGREEMENTS MAY BE USED AS ORDERING VEHICLES BY ALL DOD ORGANIZATIONS AND AUTHORIZED DEFENSE CONTRACTORS, WHICH INCLUDE:
- OFFICE OF THE SECRETARY OF DEFENSE (OSD)
- CHAIRMAN OF THE JOINT CHIEFS OF STAFF
- UNIFIED COMBATANT COMMANDS
- INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE (DOD IG)
- DEFENSE AGENCIES, THE DOD FIELD ACTIVITIES
- U. S. COAST GUARD
- NATO
- INTELLIGENCE COMMUNITY
- FOREIGN MILITARY SALES (FMS) WITH A LETTER OF AUTHORIZATION.
-

Government contractors performing work for a DoD end user (as defined above) may place Delivery Orders under ESI BPAs on behalf of and for the benefit of the DoD entity if authorized by their cognizant Contracting Officer in accordance with the requirements of FAR 51 and/or DFARS 251 as appropriate.

ESI Agreements that have been designated as a DoD ESI and GSA SmartBUY Contract are open for ordering by all United States Federal Agencies, Department of Defense (DoD) Components, and authorized contractors.

GSA or other applicable ordering organizations/agencies are authorized to place orders under this BPA on behalf of DoD end users and must comply with DFARS 208.7400. ●

JOIN US ONLINE FOR A **VIRTUAL** EXPERIENCE

DON IT Information Series

The DON IT Conference, East Coast 2013 will not be held in Virginia Beach this year due to budget and travel restrictions. Several information sessions will be offered through Defense Connect Online (DCO).

The AFCEA-USNI Joint Warfighting Conference, scheduled for May 14-16, 2013, at the Virginia Beach Convention Center will still take place. Several senior DoD and DON leaders are scheduled to appear as speakers and panel participants. Local commands are encouraged to attend, with appropriate command approval, if no travel costs will be incurred.

More information on the available DON IT sessions, as well as DCO access information, will be posted to the DON CIO website, www.doncio.navy.mil, in the upcoming weeks.

*PACIFIC OCEAN (Feb. 22, 2013)
The littoral combat ship USS Freedom (LCS 1) is underway conducting sea trials off the coast of Southern California. Freedom, the lead ship of the Freedom variant of LCS, is expected to deploy to Southeast Asia this spring. (U.S. Navy photo by Mass Communication Specialist 1st Class James R. Evans/Released)*

