

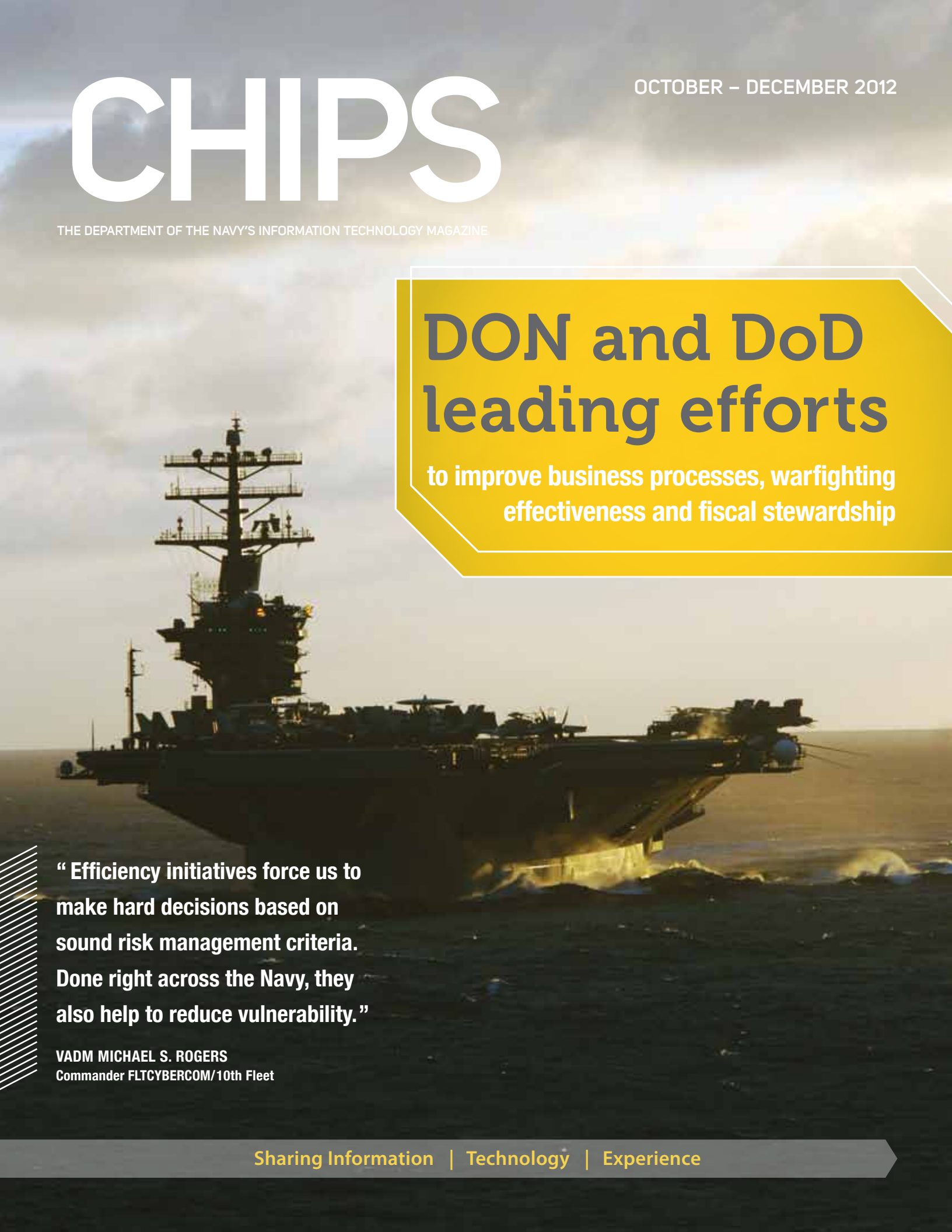
# CHIPS

OCTOBER – DECEMBER 2012

THE DEPARTMENT OF THE NAVY'S INFORMATION TECHNOLOGY MAGAZINE

## DON and DoD leading efforts

to improve business processes, warfighting effectiveness and fiscal stewardship



**“Efficiency initiatives force us to make hard decisions based on sound risk management criteria. Done right across the Navy, they also help to reduce vulnerability.”**

VADM MICHAEL S. ROGERS  
Commander FLTCYBERCOM/10th Fleet

Sharing Information | Technology | Experience

# CHIPS

OCTOBER – DECEMBER 2012, VOL. XXX ISSUE IV

**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, TERRY HALVORSEN, THOMAS KIDD,  
STEVE MUCK, STEVE WARD

**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 SPAWARSCEN PACIFIC. CHIPS IS PUBLISHED QUARTERLY BY SPAWARSCEN ATLANTIC, 1837 MORRIS ST., SUITE 3311, NORFOLK, VA 23511.

REQUESTS FOR ASSISTANCE SHOULD BE DIRECTED TO EDITOR, CHIPS, SPAWARSCEN 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.



52



## DEPARTMENT

### In Every Issue

- 04 Editor's Notebook
- 05 A Message from the DON CIO
- 13 Hold Your Breaches!
- 36 Full Spectrum
- 63 Enterprise Software Agreements

### Highlights

- 16 Fleet Cyber Command Establishes Enterprise Information Technology Service Management Governance  
*By Eric Markland*
- 24 Mailbox Storage and Security Improvements  
Coming Soon for NMCI Users  
*By Michelle Ku*
- 38 Stop Reinventing the Wheel  
Knowledge Management in the Department of the Navy  
*By Jim Knox*
- 52 NAVY 311: Your Single Entry Point for Service and Support  
Ask any question about any topic, anytime, from anywhere  
*By Sea Warrior Program Public Affairs*

## Q&A

- 08** Vice Adm. Michael S. Rogers  
Commander, U.S. Fleet Cyber Command/U.S. 10th Fleet
- 10** Kevin C. Cooley  
Command Information Officer, U.S. Fleet Cyber Command/U.S. 10th Fleet
- 20** Robert J. Carey  
Principal Deputy Chief Information Officer,  
Department of Defense
- 28** Matthew H. Swartz, Director, Communications and  
Network Division, Deputy Chief of Naval Operations for  
Information Dominance (N2/N6)

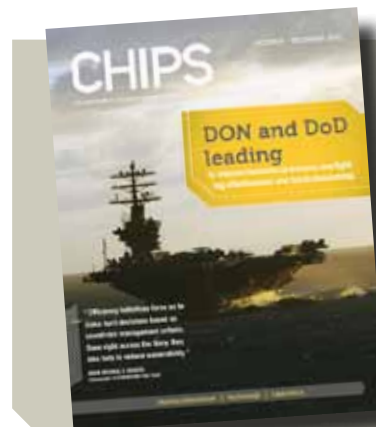


- 32** U.S. Navy Cmdr. James B. "Jamie" Gateau, Combined  
Endeavor 2012 Strategic Plans and Canadian Army  
Lt. Col. TS McLean, CE12 Officer-in-Command,  
Combined Joint Communication Control Center
- 60** Lisa Sexauer, Fitness, sports and deployed forces support  
program manager, Commander, Navy Installations  
Command

## FEATURES

- 06** DON Policies Set Stage for Future IT Efficiencies  
*By DON Enterprise IT Communications Team*
- 14** SPAWAR Single Technical Authority for IT Systems  
*By Rear Adm. Patrick H. Brady*

- 15** Information Technology Acquisition Approval Process  
*By Capt. Scott J. Hoffman*
- 19** The Joint Enterprise Information Environment  
*By Deputy Chief of Naval Operations for Information  
Dominance*
- 26** It's Time to Change the Way We Refer to  
SHF Satellite Communications  
*By Lt. Jason J. Hughes*
- 43** Cloud Computing Coming Soon  
*By Heather Rutherford*
- 44** We Want You to Submit Your Good Ideas  
*By Don Reiter and Sharon Anderson*
- 46** Attention: All Hands on Deck!  
Department of the Navy needs your help to be audit-ready  
*By Sharon Anderson*
- 48** Rear Adm. Jonathan White — New Oceanographer of the Navy  
*By Robert Freeman with Heather Rutherford*
- 50** The Defense Language Institute Foreign Language Center  
*By MC1 (SW/AW) Nathan L. Guimont*
- 55** Interoperability Leads to "Peace"  
*By Heather Rutherford*
- 56** Which Paper Shredder Should I Use?  
*By Steve Muck and Steve Daughety*
- 58** Afghanistan Automated Biometrics Identification System IPT  
First to Earn CMMI-SVC Gold  
*By Sarah Ingram and Tiffany Alexander*
- 59** SSC Pacific First Navy Organization to Achieve  
CMMI-DEV v1.3 Maturity Level 3  
*By Ashley Nekoui and Sandy Van Densen*



### ON THE COVER

The departments of Defense and Navy are focused on efficient resource management with the ultimate goal of ensuring warfighter readiness and national security.

U.S. Navy photo by MC2 Eva-Marie Ramsaran.

## Saving Money, Achieving Good Value

**B**elt-tightening is the order of the day — whether at home or at work — Americans are determined to save money on expenses large and small. But while we are shopping for the things we need, we do not want to scrimp on the quality of the things we buy — we want the same high quality and reliability for our purchases, and we are willing to reuse, repurpose, recycle and buy less to stay within our budgets.

The same objectives are driving policy decisions in the departments of Defense and Navy in meeting the needs of warfighters. The No. 1 priority is to ensure that warfighters have what they need to take to the fight. In this edition, DON and DoD leadership talk about policy decisions resulting in cost-savings, better IT investments and more efficient processes across the departments.

In July, I had the pleasure of interviewing an old friend, Rob Carey, DoD principal deputy chief information officer, about the DoD IT Modernization Strategy. Read about the DoD's security and cyber improvements to come on page 20.

In September, it was exciting to interview two warriors during their participation in the Combined Endeavor exercise, sponsored by U.S. European Command. U.S. Navy Cmdr. James B. "Jamie" Gateau and Canadian Army Lt. Col. TS McLean explained the value of CE, the world's largest C4 interoperability event with 41 participating NATO and Partnership for Peace nations. Read about CE and PFP on pages 32 and 55, respectively.

Personal readiness is also a concern in the Navy, and Lisa Sexauer, fitness program manager for Commander, Navy Installations Command, discusses the Navy's Fit for Life program which emphasizes fun via a comprehensive plan for good nutrition, sports and recreation, and social activities to help military members, family members and DoD civilians maintain a healthy lifestyle. See page 60 for information on this world-class program.

Finally, I'd like to welcome the new CHIPS assistant editor, Heather Rutherford, to the staff. Heather is an experienced technical writer and quality assurance professional with a bachelor's degree in creative writing. It is a pleasure to have her aboard. ●

Welcome new e-subscribers!



SHARON ANDERSON



GRAFENWOEHR, Germany (Sept. 11, 2012) Flags sit in front of each country's representative during Combined Endeavor 2012 at U.S. Army Joint Multinational Training Command. CE is a multinational command, control, communications and computer systems exercise designed to build and enhance communications and network interoperability between 41 nations and international organizations. Photo by U.S. Air Force Tech. Sgt. Araceli Alarcon.

### EDITORIAL CORRESPONDENCE

QUESTIONS? SEND all inquiries and questions to our editor  
[chips@navy.mil](mailto:chips@navy.mil)

# Building a Strong Foundation for Future Success



**“WE CAN’T SOLVE** problems by using the same kind of thinking we used when we created them.” Albert Einstein said these words two generations ago, and yet they ring even more true today. But, we must not stop there. While it is vital that we use current solutions, best practices and technologies to enable our immediate success, we must also maintain a steady eye on the horizon for future requirements, industry trends and threats. Only by balancing the requirements of the present and possibilities of the future, will we become an efficient, effective and forward-looking organization that is positioned for long-term success.

Today’s information technology environment is moving at a pace and complexity where data is driving business. Rapid advancements and increased interconnections enable access to information from both desktop and mobile devices. Effective decision making demands an increased focus on understanding and managing vital data to extract meaningful information that will enable intelligent, fact-based decision-making to guide the DON in meeting future challenges.

In preparing for future challenges,

we realize that the national debt is the United States’ No. 1 security risk. As a result, we face budget reductions that will demand greater levels of efficiencies across our operations. This perfect storm leads us to consider: How do we successfully execute the mission when available resources may not meet the requirements necessary to accomplish that mission? As Sailors and Marines, we are decisive and effective in warfighting. We must become equally decisive and effective as business warfighters who understand how to maximize the efficiency of business operations.

During fiscal year (FY) 2012, we built a strong foundation of cost savings on which we will continue to build in FY13 and beyond, including:

- Data center consolidation (DCC) with the goal to reduce servers into as few modern enterprise data centers as necessary. In conjunction with DCC is the opportunity to reduce the number of supported applications; we have retired several thousand to date.
- Mobile technology optimization through use of mobility management tools to significantly reduce the number of zero-use devices, and enable better management of cellular and data plans to reduce over and under usage.
- Data standardization and categorization to foster consistency of data across the enterprise and increase data visibility and usability.
- Business case analyses that clearly define considerations, such as scope, risks, costs and savings, to justify all DON IT efficiency initiatives.
- Modernization of network infrastructure will enable unified capabilities, including the integration of voice, video and/or data services delivered across an interoperable, secure and highly available IP network infrastructure.

- Update of all IT budget categories in Naval IT Exhibits/Standard Reporting (NITE/STAR) — the DON IT budget database — to better identify IT spending and improve the transparency, consistency and auditability of information.
- Mandatory use of DON enterprise licensing agreements (ELA) to provide better asset and spending visibility. Current expectations are that ELA use will render approximately \$153 million in savings over the Future Years Defense Program (FY13–FY17).
- Efficiency related policies fostering greater oversight and transparency into IT spending, validation and measurement of the progress of IT efficiency efforts through mandatory metrics and data center investment oversight. See the article titled “DON Policies Set Stage for Future IT Efficiencies” for links to IT efficiency related policies.

I thank you all for these efforts. We should be proud of the accomplishments because this work has helped prepare the DON for a successful future; however, there is still much more to do. Our people, processes and technology must be aligned and operating transparently to meet future challenges head-on.

Our people must continue to be flexible, possess the right skills and be prepared for new skills to meet the challenges. We must be prepared to stay ahead of the IT game. Our cyber/IT workforce must be agile, forward-looking and knowledgeable of industry trends, technology advances and new cyber threats.

Our processes must be efficient and not resistant to change simply because they have “always been done that way.” DON IT personnel and business owners must work together to better understand the processes and integration points of IT systems to standardize them across the enterprise and save money.

*Continued on page 7.*

# DON POLICIES SET STAGE FOR FUTURE IT EFFICIENCIES

By DON Enterprise IT Communications Team

**D**URING THE PAST TWO YEARS, the Department of the Navy laid the groundwork for information technology efficiencies that will enable business operations to better support the department's warfighting and humanitarian missions. In support of the IT efficiencies effort, there were several foundational policies issued that were designed to clarify the DON's goals and prepare for a more streamlined and efficient future. The DON is approaching these efforts from an enterprise-wide perspective with many of the policies signed by leadership from across the department's business operations. The following is a list of some key policies released during fiscal years 2011 and 2012.

**UNDER SECRETARY'S DIRECTION TO DON CIO REGARDING AN EFFICIENCY AND EFFECTIVENESS REVIEW OF IT SYSTEMS:** *Department of the Navy (DON) Information Technology (IT)/Cyberspace Efficiency Initiatives and Realignment* (Dec. 3, 2010) ([www.doncio.navy.mil/ContentView.aspx?id=2061](http://www.doncio.navy.mil/ContentView.aspx?id=2061)) directed the DON Chief Information Officer (CIO) to lead the efficiencies efforts surrounding DON IT procurement and business processes and to define a department strategy to shape the way forward in the information manage-

ment (IM), IT and cyberspace (excluding intel, attack and exploit), and Information Resource Management (IRM) domains.

**BUSINESS CASE ANALYSIS REQUIREMENTS:** The *Department of the Navy (DON) Enterprise Information Technology Standard Business Case Analysis (BCA) Template* (April 15, 2011) ([www.doncio.navy.mil/ContentView.aspx?ID=2211](http://www.doncio.navy.mil/ContentView.aspx?ID=2211)) required use of a standard business case analysis to provide all the relevant details to make an informed decision as to whether or not to go forward with a project and to determine a project's place in the DON's overall IT spending priorities. The DON CIO memo, *Required Use of Department of the Navy (DON) Enterprise Information Technology Standard Business Case Analysis (BCA) Template* (June 30, 2011), ([www.doncio.navy.mil/ContentView.aspx?id=2506](http://www.doncio.navy.mil/ContentView.aspx?id=2506)) broadened the requirement to use the BCA template for all DON IT related efforts requiring DON, functional area manager, or Echelon II enterprise-level board consideration.

**DATA CENTER CONSOLIDATION AND APPLICATION RATIONALIZATION:** *Department of the Navy (DON) Data Center Consolidation (DCC) Policy Guidance* (July 20, 2011), ([www.doncio.navy.mil/ContentView.aspx?id=2504](http://www.doncio.navy.mil/ContentView.aspx?id=2504)) placed a moratorium to halt all DON investment in increased data stor-

age capacity without first determining that existing DON data center capacity is insufficient and less cost effective.

*Achieving Measurable Efficiencies through Data Center Consolidation, System, and Application Rationalization Guidance* (Sept. 17, 2012), ([www.doncio.navy.mil/ContentView.aspx?id=4163](http://www.doncio.navy.mil/ContentView.aspx?id=4163)) signed jointly by the DON CIO and Deputy Under Secretary of the Navy and Deputy Chief Management Officer (DUSN/DCMO), announced new processes to improve service delivery, cost transparency, and enable substantive system/application rationalization processes for shore-based applications, networks and systems classified as Mission Assurance Category (MAC) II and III, and DON data centers.

The *Efficiency and Effectiveness Review of Department of the Navy (DON) Information Technology (IT) Systems* (Sept. 19, 2011), ([www.doncio.navy.mil/ContentView.aspx?id=2835](http://www.doncio.navy.mil/ContentView.aspx?id=2835)) charged the DON CIO — as the secretary's senior advisor on IT/national security systems (NSS) performance, and as DON IT/Cyberspace Efficiency Lead — to analyze and assess the DON's IT/NSS investments for efficiency and effectiveness and make recommendations for actions that could reduce the department's IT costs while maintaining operational effectiveness and warfighter support.

**UNDER SECRETARY'S MEMO TO DON CIO REGARDING INFORMATION TECHNOLOGY EXPENDITURE APPROVAL AUTHORITIES (ITEAA):** *Department of the Navy (DON) Secretariat Information Technology Expenditure Approval Authority (ITEAA)* (Sept. 19, 2011) ([www.doncio.navy.mil/ContentView.aspx?id=2834](http://www.doncio.navy.mil/ContentView.aspx?id=2834)) charged that no resource planning, programming or budgeting actions shall be initiated by any organization within the DON Secretariat for an IT expenditure with a projected lifecycle cost totaling \$100,000 or more unless that expenditure has been approved by the DON Chief Information Officer. Likewise, DON CIO must approve any IT software, hardware or service expenditures of \$100,000 or more.

**METRIC REPORTING GUIDANCE:** The *Department of the Navy Information Technology (IT)/Cyberspace Efficiency Initiatives Metric Reporting Guidance* (April 17, 2012), ([www.doncio.navy.mil/ContentView.aspx?id=3948](http://www.doncio.navy.mil/ContentView.aspx?id=3948)) was jointly signed by the Deputy Under Secretary of the Navy and Deputy Chief Management Officer (DUSN/DCMO), Deputy Assistant Secretary of the Navy (DASN) Budget and DON CIO. It mandated standard reporting metrics to measure and validate progress in attaining IT efficiency goals.

**DON ENTERPRISE LICENSING AGREEMENTS:** The *Mandatory Use of Department of the Navy Enterprise Licensing Agreements* (Feb. 22, 2012), ([www.doncio.navy.mil/ContentView.aspx?id=3777](http://www.doncio.navy.mil/ContentView.aspx?id=3777)) signed jointly by Assistant Secretary of the Navy (ASN) (Research, Development and Acquisition (RDA)), Assistant Secretary of the Navy (Financial Management and Comptroller (FMC)) and DON CIO, announced the establishment of DON enterprise licensing agreements (ELA) and mandated that where a DON ELA exists, any software products, hardware and related services offered by that ELA must be procured using that ELA, including those procured by government purchase cards.

#### **REVISED BUDGET LINE ITEMS AND DEFINITIONS**

**FOR PBIS-IT:** *Improving Cost Visibility for the Fiscal Year (FY) 2014 Information Technology and National Security System (IT/NSS) Budget Exhibits* (April 20, 2012), ([www.doncio.navy.mil/ContentView.aspx?id=3962](http://www.doncio.navy.mil/ContentView.aspx?id=3962)) was jointly signed by ASN RDA, Director, Civilian Resources and Business Affairs Division FMB4/Deputy Assistant Secretary of the Navy for Budget and DON CIO. It established a new cost categorization structure in NITE/STAR (PBIS-IT) definitions to provide greater insight into DON IT spending. It also reiterated the requirement to report commercial hardware, software and services in NITE/STAR (PBIS-IT) by contract, vendor, make, model and version. For more information on all DON IT policies, please visit the DON CIO website at [www.doncio.navy.mil](http://www.doncio.navy.mil). ●

---

## **MESSAGE FROM THE DON CIO** *Continued from page 5.*

This will enable informed decision making that breaks down the silos of excellence that have formed within our department.

Our technology must meet the DON's true mission requirements. We look to industry to serve, not only as solution provider, but as educator on the art of the possible. Earlier engagement with industry can help us devise economical and effective solutions that meet the DON's prioritized needs instead of the usual issuance of a prescriptive request for proposal.

As we move into FY13, we will continue

to enhance our business focus and skill by applying the same planning capability, attention to detail and dedication to our business operations that has made the Department of the Navy so effective in combat. We will remain focused on identifying and implementing enterprise-wide efficiency opportunities, such as streamlining printing activities to reduce overall spending, growing the number of DON enterprise licensing agreements to leverage the department's buying power, and increasing accountability and transparency as we move toward audit readiness.

I look to you to help the DON identify further opportunities to increase the effectiveness of its business operations from people, technology and innovation perspectives. In doing so, we will achieve efficiencies and savings that will allow us to significantly enhance the DON's mission. Although still faced with monumental challenges, we have the unique opportunity to address key initiatives that will significantly benefit the department during the next 25 years. ●

**TERRY HALVORSEN**

# Vice Adm. Michael S. Rogers

Commander, U.S. Fleet Cyber Command/U.S. 10th Fleet

Vice Adm. Michael Roger assumed his present duties as Commander, U.S. Fleet Cyber Command, Commander, U.S. 10th Fleet in September 2011. Since becoming a flag officer in 2007, Rogers has also been the director for intelligence for both the Joint Chiefs of Staff and U.S. Pacific Command.

Duties afloat have included service at the unit level as a surface warfare officer (SWO) aboard USS Caron (DD 970), at the strike group level as the senior cryptologist on the staff of Commander, Carrier Group Two/John F. Kennedy Carrier Strike Group, and at the numbered fleet level on the staff of Commander, U.S. 6th Fleet embarked on USS LaSalle (AGF 3) as the fleet information operations (IO) officer and fleet cryptologist. He has also led cryptologic direct support missions aboard U.S. submarines and surface units in the Arabian Gulf and Mediterranean.



Vice Adm. Michael S. Rogers

Rogers' joint service both afloat and ashore is extensive and prior to becoming a flag officer, he served at U.S. Atlantic Command, CJTF 120 Operation Support Democracy (Haiti), Joint Force Maritime Component Commander, Europe, and the Joint Staff.

Rogers responded to CHIPS questions in late September.

**Q:** What is the roadmap for continued success for U.S. Fleet Cyber Command and the Navy?

**A:** The roadmap for continued success requires U.S. Fleet Cyber Command/10th Fleet (FCC/C10F) to address cyber threats, key trends, and challenges across four main areas, which are: (1) integrated operations; (2) an optimized cyber workforce; (3) technology innovation; and (4) reforming development and execution of our requirements, acquisition and budgeting.

Specifically, we will continue to employ Navy and joint cyberspace forces with an effectively recruited, trained and positioned workforce who have clear authorities and are armed with proven

tactics, techniques and procedures (TTPs). We will also continue to leverage industry, academia, interagency, service, joint and allied partners to ensure our team has the most innovative technologies available while concurrently optimizing defense resources.

In summary, the Navy's success across the maritime domain is guaranteed by our ability to defend, project power, and prevail in cyberspace with an exceptionally trained cyber force, continued vigilance, proven tactics, and an unshakable warrior ethos.

**Q:** How do you see the cyber workforce now, and what is the way ahead to develop it to meet the growing needs of Navy and joint forces?

**A:** First and foremost, our FCC/C10F team around the world are warriors who remain motivated and mission focused. The Navy's cyber warriors are doing an incredible job everyday defending the network and achieving information dominance. I could not be prouder.

To preserve the Navy's cyber warfighting advantage, we must continue to de-

velop an elite workforce that is recruited, trained and educated to better understand the maritime environment, employ the latest technological advances, and deliver cyber warfighting capability anywhere around the world.

To do this, in 2009 the Navy acknowledged the centrality of information to maritime warfighting and established the Information Dominance Corps (IDC). This corps consists of information experts, intelligence analysts, meteorologists and oceanographers, space cadre and cryptologists. To optimize employment of our cyber force, a personnel review of the Navy's cyber manpower requirements has been completed and the Navy continues to develop concepts that better inculcate the IDC organization across the fleet to include career path adjustments, cross-field competencies, diversified command opportunities and improved education.

There are challenges that lie ahead, but the strategy is in place and the vision forward is being executed.

**Q:** Could you elaborate on the importance of information and cyberspace to the Navy?



"The U.S. military's critical war winning advantage is the ability to network widely dispersed forces to gain battlespace awareness, extend operational reach, and deliver massed and precision firepower at critical points."

**A:** The U.S. military's critical war winning advantage is the ability to network widely dispersed forces to gain battlespace awareness, extend operational reach, and deliver massed and precision firepower at critical points. For 40 years this has given the Navy an asymmetric advantage. This advantage must be defended, preserved and exploited.

These networked capabilities will be a primary target in future conflicts. The Navy will need to fight through an adversary's attempt to deny access to information and our ability to network this information across the battlespace. The Navy cannot take unencumbered access for granted and the fight to maintain a networked force will be continuous.

While cyberspace has been traditionally thought of as an enabler (supporting combat) in the traditional sea, air and land environs, today, it is a primary warfare domain of equal importance. Because the Navy's combat power is drawn from a highly networked and electromagnetic spectrum dependent force, the Navy will need to lead, engage and win the fight across these critical environments.

FCC/C10F will continue to operationalize cyberspace in order to guarantee resilient command and control of Navy and joint forces to maintain our warfighting advantages.

**Q:** **Do the Department of the Navy policies for data center consolidation, application rationalization, and Navy Information Technology Expenditure Approval Authorities for software**

**and hardware acquisition assist in or have impact on FCC/C10F operations?**

**A:** Consistent with Public Law, Executive Orders, and higher level DoD directives, DON policies are aimed at promoting efficient spending in information technology. We are committed to being good stewards of taxpayer dollars. Therefore, we rigorously review all IT expenditures, and prioritize investments to best meet dynamic mission assignments — across all Lines of Operation.

I need to emphasize that this kind of review is not new, and to ensure these new policies do not inhibit our ability

to maneuver, we have worked very hard to overlay them with our existing practices and to maintain a good balance between focus on the mission and resource management oversight.

Efficiency initiatives force us to make hard decisions based on sound risk management criteria. Done right across the Navy, they also help to reduce vulnerability. ●

**FOR MORE INFORMATION**

Vice Adm. Michael S. Rogers' Biography  
[www.navy.mil](http://www.navy.mil)  
FLT CYBERCOM/10th Fleet  
[www.fcc.navy.mil](http://www.fcc.navy.mil)



MONTEREY, Calif. (Jan. 30, 2012) Vice Adm. Michael S. Rogers, commander of U.S. Fleet Cyber Command and U.S.10th Fleet, speaks to students and staff at the Center for Information Dominance, Unit Monterey, during an all-hands call. U.S. Navy photo by Mass Communication Specialist 1st Class Nathan L. Guimont.

# Kevin C. Cooley

Command Information Officer U.S. Fleet Cyber Command/U.S. 10th Fleet

Mr. Kevin C. Cooley serves as the command information officer (CIO) for the U.S. Fleet Cyber Command. Mr. Cooley assumed these duties in September 2010. In this capacity, Mr. Cooley reports directly to the Fleet Cyber Command/10th Fleet Commander and he serves as the senior civilian information management, information technology and cyber security official for the command. From September 2009 through August 2010, Mr. Cooley served as the assistant deputy chief management officer (ADCMO) for the Department of the Navy. As the ADCMO, Mr. Cooley supported the DON Deputy Chief Management Officer in the execution of his business operations and transformation oversight responsibilities.



Kevin C. Cooley

From December 2006 through August 2009, Mr. Cooley served as the Director, Information Technology Governance & Information Management (OPNAV N61). The Information Technology & Information Resource Management Directorate supported the Deputy Chief of Naval Operations for Communication Networks (N6) and the Deputy DON Chief Information Officer (Navy). Mr. Cooley had overall information technology architecture and governance responsibility for the Navy's IT infrastructure. Additionally, Mr. Cooley exercised oversight of IT programming, budgeting and fiscal execution. Please go to Navy.mil for Mr. Cooley's complete biography. Mr. Cooley responded to CHIPS questions in late September.

**Q: Can you talk about your role as the executive director and command CIO for Fleet Cyber Command?**

**A:** As the FCC executive director and senior civilian official in the command, my role is to assist and advise the commander on matters related to integration of requirements and programs, synchronization of financial execution with requirements, and civilian workforce and performance

management for the FCC organization. I represent the commander in various joint and Navy flag and senior executive panels related to the FCC mission, the planning and budgeting cycle, and financial management. Chief of Naval Operations Adm. Jonathan Greenert has directed that his commanders know their business and that they be judicious in their use of resources. A primary focus of my work as executive director is to help the FCC commander meet the CNO's direction in this area.

I also have a second set of responsibilities, those of the FCC command information officer. My primary responsibility in this role is to be the commander's principal advisor for information technology architecture, IT investment priorities, and to ensure FCC meets requirements for IT portfolio management within the FCC domain.

The architectures, investments and portfolios span all classification enclaves and keeps me engaged in both the Navy enterprise (due to our global mission set for the Navy) and FCC specific domain arenas. Given the nature of FCC's responsibilities in a new warfare domain [cyber], I execute my CIO responsibilities in close coordination with the cyberspace

operations, strategy and planning, and communications directorates at FCC. This means that I season the more traditional technology policy and governance roles of the CIO with a healthy portion of perspective from tactical cyberspace operations executed in a Maritime Operations Center (MOC) context, cyberspace strategy and planning at the operational level of war, and the reality of large scale and global network and security operations.

While these responsibilities can be a bit overwhelming at times, I very much enjoy working with the extremely professional uniformed and civilian personnel at FCC. Hardly a week goes by without me being amazed by the creativity and dedication of our people. It is my high honor to be a part of their leadership team.

**Q: Does Fleet Cyber Command have a role in the Department of the Navy's IT efficiencies effort to improve business IT processes, including: consolidating data centers, developing a data and cloud strategy, and using department-wide enterprise licensing agreements?**

**A:** FCC understands the Navy's need to

have IT systems that are both operationally relevant and affordable. Because of this, FCC also understands the Navy's imperative to gain efficiencies in its IT environments and as such is working in two dimensions.

The first is inside of the FCC domain where we apply significant scrutiny to our own IT environments to ensure that we are as efficient as possible in our own expenditure of resources; including leveraging enterprise solutions wherever feasible.

The second is to support both OPNAV and the DON CIO in their Navy and department-wide initiatives to reduce expenditures on IT systems. Specifically, as one of several Navy second echelon commands and the operational authority for the Navy's networks, FCC has a significant role in the Department of the Navy's efforts to realize greater IT efficiencies.

For example, FCC provides direct support for the Fleet Forces Command sponsored 'Fleet FAM' initiative to eliminate unneeded applications from the afloat environment. Particularly, as the operational authority for networks, we provide the network communications and security perspective for decisions to retain afloat applications. I personally sit on the Business Executive Advisory Board established by the DON Deputy Chief Management Officer (Deputy Under Secretary of the Navy Mr. Eric Fanning) to specifically address opportunities for business process improvement across the DoN.

Additionally FCC, upon the request of OPNAV N2/6, is taking a lead role in the further consolidation of the remaining 'legacy' and 'excepted' networks into the NMCI environment. FCC is also directly supporting the DoD planning and implementation of the Joint Information Environment (JIE) which incorporates at DoD level cloud and implicit data strategy.

**Q:** In his statement to the House Armed Services Committee July 25, which addressed emerging cyber threats and capabilities Commander, U.S.

**Fleet Cyber Command Vice Adm. Michael S. Rogers said to reduce the attack surface exposed to criminals and adversaries, the Navy engaged in a comprehensive campaign to achieve shore network consolidation and modernization by terminating all Navy legacy networks by 2014. I thought all legacy networks had been either retired or modernized with the implementation of the NMCI and the Cyber Asset Reduction and Security effort, or not?**

**A:** With the dynamic nature of the Navy's mission, there will be continued activity to improve and maneuver the Navy's network to meet the mission and counter a dynamic, persistent and sophisticated set of adversaries. Therefore, being better organized and having a smaller exposed attack surface will improve our mission assurance posture.

The Navy has made substantial progress afloat and ashore in fielding our enterprise networks (NMCI, ONE-NET and IT-21). These major network programs have dramatically reduced the variability in [the] security posture of the Navy's networks, and Operations Cyber Condition Zebra (CCZ) and Cyber Asset Reduction and Security (CARS) were the first logical steps to both more thoroughly secure the perimeter and more completely field NMCI and ONE-NET.

It's worth noting that the original task for Operation CARS was to reduce the Navy's networks by 51 percent. In fact, over 1,040 individual Navy networks were terminated during Operation CARS, mostly by migrating key mission applications into a better-protected enterprise perimeter. This included discovery of over 300 previously unregistered networks and equates to roughly 90 percent reduction of the total and far exceeding CNO's tasking. During this period, approximately 300 networks were reviewed and determined to not be a good fit in the near term for immediate migration into the enterprise environment.

These were defined as excepted networks that would be a part of the overall Navy network environment, just not inside of one of the three primary enterprise networks. Some good examples of these include Navy Medicine, our systems commands' RDT&E networks, educational networks for the Navy's degree granting institutions, as well as some tactical networks. What Vice Adm. Rogers was referring to in his comments was the initiative to re-look at these excepted networks to further consolidate wherever feasible.

Our past experience with Operations CCZ and CARS helps us understand that continued consolidation of networks will require corresponding consolidation or elimination of applications. So in this way, there is a linkage between the ongoing network consolidation efforts at FCC, which are focused on March of 2014, and the overall DON Data Center Consolidation effort. Interestingly, we also see the importance of architecture as a part of reducing attack surface. The use of cloud technologies and design approaches that can enable thinner or stateless end use devices can go a long way towards reducing our attack surface and we are working with the technical authority and the acquisition community in this area as well.

**Q:** Can you talk about the "Cyber Wholeness Review" efforts?

**A:** The cyber-warfare wholeness review is being conducted by OPNAV in conjunction with Fleet Cyber Command, Fleet Forces Command, Pacific Fleet, Navy Cyber Forces, Navy Warfare Development Command, the Office of Naval Intelligence, and the Program Executive Office for Command, Control, Communications, Computers and Intelligence (C4I). The review is examining the state of current doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF) that enable Navy's cyberspace operations.

All in our Navy have an interest in

assuring that our investments in cyber warfare are balanced, sustainable and meet the operational needs of the Navy. The wholeness review is simply a part of the process that OPNAV executes to see to this balance.

**Q: Vice Adm. Rogers also said in his testimony that 75 percent of FLTCYBERCOM's workforce operating the networks day-to-day is "out of whack and very dated." Consolidating and centralizing servers and networks into a "cloud" approach will free up personnel from running the networks to actually defending them – and, perhaps, attacking adversaries' systems. Are you beginning to plan how the workforce will operate in this paradigm switch?**

**A:** Absolutely, we are aggressively working both inside of FCC and with our partner type commander, Navy Cyber Forces (NCF) to plan and execute this switch. This speaks directly to a transition from a primary and 'traditional' focus on operating the networks to a more comprehensive and fully relevant focus that explicitly includes a proactive defense, and the capability to support exploitation or attack on an adversary's networks as directed by U.S. Cyber Command. Integrating these functions, along with the other areas of our mission set: information warfare, electronic warfare, signals intelligence and space, will further extend the capabilities of the cyber fleet.

The establishment of the Information Dominance Corps was a first visionary step on this road and FCC is absolutely committed to completing the transformation.

We are specifically working with NCF to evaluate the billet and training requirements to enable our fully integrated operating model. Any new billets will either come from excess lists (via SMRD — Shore Manpower Requirements Determination) based on billets no longer required under the previous model and repurposed, or they will be a part of FCC POM (Pro-

gram Objective Memorandum) inputs to OPNAV.

We expect that the transition to more operationally sustainable cloud technologies enabled by virtualization, the increased use of automation in operating our network and server infrastructures, combined with continuing consolidation of networks, to accelerate. This presents an opportunity for FCC to refocus resources from network operations and traditional information technology end user support to more operationally valuable aspects of operations in and through cyberspace.

**"FCC is a warfighting organization and executes its responsibilities vigorously and with this as a touchstone. FCC has a fully capable MOC..."**

**Q: Vice Adm. Rogers said that the cyber components are warfighting organizations just like every other mission set within the Department of Defense. Can you give examples about some of the taskings that the cyber warriors of Fleet Cyber Command receive from U.S. Cyber Command?**

**A:** FCC is a warfighting organization and executes its responsibilities vigorously and with this as a touchstone. FCC has a fully capable MOC established at its headquarters, as well as an associated set of combined task forces (CTFs), to execute its mission sets. While security classification prohibits the ability to be very detailed, I can speak in more general terms to FCC's mission tasking.

FCC functioned as a U.S. Cyber Command co-lead for a crisis action team and service lead for a follow-on operational planning team in response to recent contingency operations. Planning for options for the delivery of cyber effects encompassed all aspects of cyber operations. Also, FCC is currently tasked with intelligence development and operational planning for the delivery of cyber effects across all aspects of cyber operations in support of various regional COCOM (combatant commander) readiness requirements.

**Q: Could you speak briefly to the functions of command and control, intelligence, fires, movement and maneuver, sustainment, and protection tested in Terminal Fury 2012?**

**A:** FCC functioned as the service component lead for Terminal Fury 2012. Of note, the cyber fires process exercised in Terminal Fury paralleled existing kinetic fires models. Objectives to integrate operational and fires processes between FCC, as the service level component, and U.S. Cyber Command were successfully achieved. These processes included command and control, fires, maneuver and protection.

Terminal Fury is a large and comprehensive exercise that tests our capabilities and generates insights that drive further improvement. One insight we gained highlighted the value of remote support for operations. Importantly, FCC executed successfully using both resources located remotely at its fleet headquarters in [Fort Meade] Maryland and resources forward deployed into the theater of operations. ●

**FOR MORE INFORMATION**  
FLTCYBERCOM/10th Fleet  
[www.fcc.navy.mil](http://www.fcc.navy.mil)

# Medical Insurance Company Faxes Personal Information to Wrong Number for Three Years

**T**HE FOLLOWING IS a recently reported personally identifiable information (PII) data breach involving a private medical insurance company that improperly handled PII. Incidents such as this 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 (DON CIO) Privacy Office.

## The Incident

The spouse of a non-appropriated fund (NAF) employee requested a waiver from a medical insurance company for medicine not carried in the Department of Defense formulary. When the spouse did not receive the waiver as expected, it was discovered that the waiver was sent to an incorrect fax number. The medical insurance company's pharmacy reviewer sent the information to a private business. The individual who received the fax stated that the private business had been mistakenly getting faxes from the medical insurance company for the past three years and had tried unsuccessfully to correct the problem. The individual said the faxed documents sometimes contained personal health information (PHI), as well as Social Security numbers (SSN) and other PII.

## Actions Taken

The Office of the Secretary of Defense (OSD) Privacy Office was notified of the potential breach. The DON Privacy Office was later contacted because at least one of the individuals affected was a Navy NAF employee. Because the breach affected multiple services, the DON and OSD privacy offices worked through the breach process with the medical insurance company. The fax number used by the medical insurance company was



immediately corrected. The individual at the private business stated that he shredded all the information that was received and never used it for any purpose before it was destroyed. Known individuals who were affected were notified of the breach.

## Lessons Learned

- ➔ Faxing is prone to human error and is one of the least secure means of transmitting PHI and PII.
- ➔ Steps that should always be taken include:
  - Double check the fax number to ensure it is correct;
  - Notify the individual that is to receive your fax that you are about to transmit PII or PHI; and
  - After sending the fax, contact the individual to confirm secure receipt of the information.

Effective Oct. 1, 2012, in accordance

with the DON SSN Reduction Phase Three policy message DON CIO DTG 171625Z Feb 12 ([www.doncio.navy.mil/ContentView.aspx?ID=3757](http://www.doncio.navy.mil/ContentView.aspx?ID=3757)) the use of fax machines is prohibited when sending documents containing SSNs and other PII by DON personnel.

External customers such as service veterans, Air Force and Army personnel, family members and retirees may continue to fax documents containing an SSN to DON activities but are strongly encouraged to use an alternative means, including the U.S. Postal Service, encrypted email (WINZIP is an authorized encryption method) and the Safe Access File Exchange (SAFE). For details about SAFE, visit: [www.doncio.navy.mil/ContentView.aspx?id=4098](http://www.doncio.navy.mil/ContentView.aspx?id=4098). ●

**STEVE MUCK** is the Department of the Navy privacy lead.

# SPAWAR Single Technical Authority for IT Systems

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



Rear Adm. Patrick H. Brady

In a letter titled “Navy Information Dominance Way Ahead” dated Sept. 8, 2011, the Chief of Naval Operations directed the Deputy Chief of Naval Operations for Information Dominance (OPNAV N2/N6) to seek of Assistant Secretary of the Navy for Research, Development & Acquisition (ASN RDA) support for a plan to unify technical authority for IT/information systems, communications and networks under SPAWAR.

Since then, OPNAV, ASN RDA, Naval Sea Systems Command (NAVSEA), Naval Air Systems Command (NAVAIR) and SPAWAR have been working together to develop guidance to implement this task, and I believe it is one of our most important efforts to fundamentally improve the way the Navy develops, procures, installs and sustains IT systems and networks.

Establishing a single Technical Authority (TA) will provide the architectures, requirements, interfaces, technical standards, tools, and systems engineering and integration processes that are in conformance with applicable policies and will drive effectiveness and efficiency into our IT development and acquisition, across the Navy.

Building the single TA for information technology, communications and networks is a prime enabler to achieve the Navy’s information dominance vision. Lack of consolidated authority, responsibility and accountability for information and communication systems, ashore and afloat, creates economic inefficiencies, interoperability issues, and hinders our progress toward information dominance.

The power of a single TA leverages sound system engineering principles to impact acquisition decisions at the Navywide level through individual programs. Developing the single TA aligns with the previous work SPAWAR has been doing in this area while better preparing the Navy to meet fiscal pressures.

From our perspective, TA encompasses a few key elements. First, it assures adherence by programs and projects to prescribed technical standards and policy. IT systems and networks are pervasive throughout our operations and are central to the information dominance warfare area. Standards and policy keep these systems interoperable, capable and secure. Second, it ensures that support continues throughout the life cycle of the program or project.

One-off or non-program of record system buys may fulfill an immediate fleet requirement at a favorable short-term cost. However, the preponderance of system acquisition costs occurs during the in-service sustainment phase. Adding a new system without a resourcing plan in place for sustainment is asking for problems in the out-years.

The final and broader advantage of a single TA is that it ensures practical and complete solutions to programmatic technical needs and solutions that fit into the bigger picture. This drives solutions that complement or leverage existing systems, avoids redundancy and fields systems that enhance the operational excellence of our IT systems and networks. The bottom line is better capability for the fleet with less overhead and cost.

System of systems (SoS) engineering is SPAWAR’s central approach that addresses the required elements of a single TA. A government study showed that when a project spent 10–15 percent of its budget on systems engineering, the project came in on time and on cost. The analysis and insight provided by a sound SoS approach from top-level requirements down to the project level is essential in the technical, fiscal and security environment for IT systems and networks.

There are challenges in establishing a single TA. The large number of IT systems and because IT is elemental to so many other weapons systems and platforms make codifying the scope of governance complex work. SPAWAR is working with the OPNAV staff and partner commands to establish the governing instruction and supporting documentation for a single TA with incremental establishment of the authority through fiscal years 2012 and 2013.

The bottom line is that when the single TA is in place, the Navy will be able to better provide cost-effective information dominance capabilities to the fleet. It’s a very important effort with tremendous potential for our Navy. ●

#### FOR MORE INFORMATION

SPAWAR  
[HTTP://TWITTER.COM/SPAWARHQ](http://twitter.com/SPAWARHQ)  
[WWW.FACEBOOK.COM/  
SPACEANDNAVALWARFARESYSTEMSCOMMAND](http://www.facebook.com/SPACEANDNAVALWARFARESYSTEMSCOMMAND)

# Information Technology Acquisition Approval Process

By Capt. Scott J. Hoffman  
SPAWAR Deputy Director for Contracts



Capt. Scott J. Hoffman

The Navy buys several billion dollars of non-weapon system and non-C4ISR system IT and IT support services each year. "Several" is the key word because we did not have service-wide visibility of Navy IT purchases. This lack of visibility hindered our ability to make capability-based, cost-effective procurement decisions. To address this issue, CNO and ASN RDA signed a joint letter in October of 2011 that designated SPAWAR as the Navy's single IT procurement approval and oversight authority for command and control, information and IT.

This new single collection point, and the review process developed around it, gives the Navy visibility to make informed decisions on IT procurement to optimize technical approach, alignment, savings and overall performance.

The technical perspective is a crucial element of the review. A technical review of procurement determines if the request meets Navy standards to minimize the danger of one-off, non-standard purchases that may not be compatible with other Navy systems in terms of capability, operation or security. An incompatible system adds risk to our networks and additional long-term sustainment costs.

Additionally, the volume of Navy IT purchases gives us tremendous buying power. However, this advantage can be negated if we make stand-alone, uncoordinated purchases. Strategic sourcing and maximizing the use of competitive contract vehicles brings the best long-term value to all Navy users.

These reviews also identify redundancy

or unused capacity issues. A special case, but a good illustration, is data storage. Procuring additional data storage locally while the Navy-enterprise already has significant unused capacity on servers at existing data centers is not an effective use of limited funding. Uncoordinated IT procurements are likewise not an effective or efficient use of resources. ITAAP, the Information Technology Acquisition Approval Process, is designed to give the Navy the visibility necessary to optimize our IT resources.

ITAAP uses the Web-based Navy Information Dominance Approval System (NAV-IDAS) to funnel IT Procurement Requests (ITPRs) from the Echelon II CIO to OPNAV N2/N6. OPNAV N2/N6 is the IT Expenditure Approval Authority (ITEAA). As the ITEAA, OPNAV N2/N6 determines if the proposed procurement is something the Navy should invest in given limited resources and the overall information dominance strategy. If the answer is "yes," the ITPR flows to the SPAWAR Chief Engineer for a review of the technical approach. Next is an acquisition review by SPAWAR Contracts to review the acquisition approach to drive toward economies of scale while not suboptimizing other goal performances.

For those commands not yet on NAV-IDAS, requests for technical and acquisition review should be submitted via email to SPAWAR.IT.REVIEW.FCM@NAVY.MIL in those cases where

procurements are equal to or greater than \$500,000. On purchases less than \$500,000, an information copy spreadsheet of monthly consolidated ITPRs are sent to SPAWAR. We expect email submissions will not be necessary once NAV-IDAS is implemented across the Navy.

SPAWAR has tech reviewed 9,355 line items from 14,800 ITPRs valued at \$3.3 billion. This includes all manual ITPRs, NAV-IDAS submissions and consolidated spreadsheets. To date, 70 ITPRs valued at \$5.7 million have been disapproved. All numbers are cumulative for FY12 to date.

Ultimately, the visibility and insight we continue to gain into Navy IT expenditures will support strategic sourcing on IT procurements — ensuring service-wide alignment, technical approach and efficiency.

To view Commander SPAWAR message R 01023Z DEC 11 ZYB, "Information Technology Acquisition Approval Process (ITAAP)" go to: [www.public.navy.mil/spawar/Press/Pages/IT\\_PROCUREMENT\\_APPROVAL\\_AND\\_OVERSIGHT.aspx](http://www.public.navy.mil/spawar/Press/Pages/IT_PROCUREMENT_APPROVAL_AND_OVERSIGHT.aspx). ●

#### FOR MORE INFORMATION

SPAWAR  
[HTTP://TWITTER.COM/SPAWARHQ](http://twitter.com/spawarhq)  
[WWW.FACEBOOK.COM/SPAWAR](http://www.facebook.com/spawar)  
[WWW.DONCIO.NAVY.MIL/CHIPS](http://www.doncio.navy.mil/chips)

# Fleet Cyber Command Establishes Enterprise Information Technology Service Management Governance

## *Naval Enterprise Networks and Fleet Cyber Command charters Navy's Enterprise ITSM Office*

*By Eric Markland*

On April 17, Fleet Cyber Command (FLTCYBERCOM) and Naval Enterprise Networks (NEN) Program Office (PMW 205) launched the Navy Enterprise ITSM Office (ITSMO), charged with establishing enterprise-level ITSM governance to drive improved IT service quality, interoperability and efficiency across the Navy.

While the ITSMO's efforts are currently focused on coordinating and governing the NEN Program Office's ITSM efforts for the Next Generation Enterprise Network (NGEN), the partnership formalizes a critical relationship between network operations and an IT acquisition program and represents a significant milestone and shift in culture for management of Navy IT networks.

The Navy's IT networks are vital to enabling traditional business and administrative functions, and more importantly, executing the warfighting and national security mission. As such, greater visibility and control of the Navy's IT networks and resources are required to make informed decisions concerning the employment of those resources and, ultimately, to optimize the value to fleet operational missions.

Increased visibility and control requires enhanced IT governance and increased government roles and responsibilities. Historically, management and governance of Navy IT networks and services have been shared among multiple, often independent, government organizations, acquisition programs and vendors. This impedes enterprise visibility and control of networks and resources, creates gaps or conflicts in accountability for critical IT functions, limits enterprise-level interoperability across programs and systems, and contributes to operational inefficiencies and increased management costs.

To address these challenges, provide a structured approach to enterprise governance and ITSM, and ensure alignment

between IT services and fleet operational missions, FLTCYBERCOM partnered with Naval Enterprise Networks to stand up the Navy Enterprise ITSMO.

"Establishing an enterprise-wide IT governance framework will enable the government to achieve our goals of gaining situational awareness and command and control over our networks," said Mr. Eric Markland, FLTCYBERCOM deputy CIO for enterprise architecture.

*"Establishing an enterprise-wide IT governance framework will enable the government to achieve our goals of gaining situational awareness and command and control over our networks."*

Eric Markland  
FLTCYBERCOM Deputy CIO

### **Enterprise ITSMO Vision, Mission and Goals**

The ITSMO's vision for Navy IT is to establish a mission-focused, integrated set of IT functions and supporting competencies that deliver optimal value to the Navy missions they support. To accomplish this, the ITSMO is championing the adoption of a comprehensive ITSM framework based on industry and government best practices and international standards, including COBIT (Control Objectives for Information and Related Technologies), ISO 20000 and 38500, and the Information Technology Infrastructure Library known as ITILv3.

This framework will clearly define the enterprise-level IT management policies, standards, processes, roles and responsibilities required to inform and guide IT acquisition programs and service management initiatives.

When asked about the impact of the

ITSMO's efforts, ITSMO's chairman Lt. Cmdr. Todd Glidden said, "In order to foster standardization of ITSM architecture, we needed to adopt controls and develop an ITSM reference architectural model and tool kit, which can be used by process design teams across the enterprise."

This framework is consistent with the DoD Enterprise Service Management Framework (DESMF) and serves as a key enabler to Navy's Naval Networking

Environment (NNE) and Joint Information Environment (JIE) strategies.

As chartered by Mr. Markland and NEN Program Manager Capt. Shawn P. Hendricks, the ITSMO's mission is "to coordinate and govern the development and execution of a customer-focused, enterprise-wide approach to IT service management that drives improved service quality and interoperability across Navy enterprise networks to support the Department of the Navy (DON) information management (IM)/IT strategic goals and efficiency initiatives."

The ITSMO's key goal "is to ensure that IT services delivered to IT customers are fit for purpose, stable, reliable and fully support the Navy's mission and business needs."

Today, in addition to chairman Lt. Cmdr. Todd Glidden of FLTCYBERCOM, the ITSMO consists of principal membership



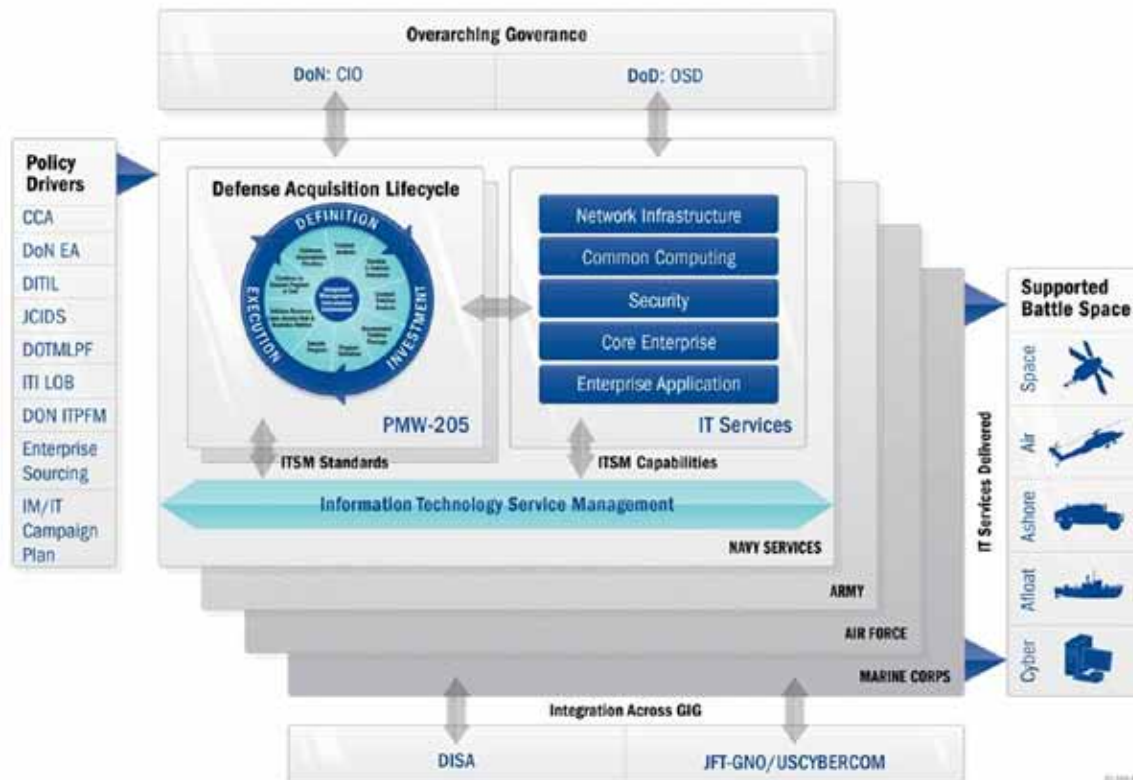


FIGURE 1. THE NAVY ENTERPRISE ITSM OFFICE (ITSMO) IS CHARGED WITH ESTABLISHING ENTERPRISE-LEVEL ITSM GOVERNANCE TO DRIVE IMPROVED IT SERVICE QUALITY, INTEROPERABILITY AND EFFICIENCY ACROSS THE NAVY. POLICY DRIVERS INCLUDE THE CLINGER-COHEN ACT (CCA); DEPARTMENT OF THE NAVY ENTERPRISE ARCHITECTURE (DON EA); DEFENSE ITIL (DITIL); JOINT CAPABILITIES INTEGRATION AND DEVELOPMENT SYSTEM (JCIDS); DOCTRINE, ORGANIZATION, TRAINING, MATERIEL, LEADERSHIP AND EDUCATION, PERSONNEL AND FACILITIES (DOTMLPF) FUNCTIONAL NEEDS ANALYSIS; IT INFRASTRUCTURE LINE OF BUSINESS (ITILOB); DON IT PORTFOLIO MANAGEMENT (DON ITPFM); ENTERPRISE SOURCING; AND THE DON IM/IT/CYBERSPACE CAMPAIGN PLAN.

from the FLTCYBERCOM office of the CIO, NEN Program Office and Naval Network Warfare Command (NETWARCOM). Adjunct membership also includes representation from U.S. Marine Corps Enterprise IT Service Management (E-ITSM); Navy Cyber Defense Operations Command (NCDOC), Space and Naval Warfare Systems Command (SPAWAR); SPAWAR Systems Centers Atlantic and Pacific; ONE-NET; Echelon II Contract Technical Representatives (CTRs); the Navy's Consolidated Afloat Networks and Enterprise Services (CANES) program office; U.S. Fleet Forces Command; and U.S. Pacific Fleet.

Core office functions include: Governance, Architecture and Integration, Quality Management, and Strategic Communications. Governance is foundational to the office, and in its role as the ITSMO Governance Board, the board is charged with overseeing and aligning command- and program-level ITSM initiatives and resources.

The board meets monthly to provide direction, facilitate decision making, and charter subordinate ITSM governance

The ITSMO's key goal "is to ensure that IT services delivered to IT customers are fit for purpose, stable, reliable and fully support the Navy's mission and business needs."

boards, including the Process and Service Owner Councils.

Architecture and Integration (A&I) is focused on the development and management of an enterprise ITSM reference architecture and supporting standards. The A&I team conducts architecture reviews with ITSM design and implementation teams and facilitates integration and prioritization of ITSM initiatives to ensure interoperability.

The Quality Management function is working to establish a quality manage-

ment system that defines the approach and methodology for achieving quality in all provisions of services and processes across Navy ITSM initiatives.

Strategic Communications manages communications with members, stakeholders and governance bodies. This function is focused on development of training and awareness programs and facilitation of ITSM team mentoring and training.

### NEN ITSM Efforts Underway

In May 2012, the NEN Program Office released the NGEN Transport and Enterprise Services request for proposal (RFP) that establishes the Navy's acquisition approach for NGEN. In preparation for the development and release of the RFP, NETWARCOM developed the NGEN NetOps Concept of Operations (CONOPS) and Strategy for Network Command and Control (C2) over the the Navy's portion of the Global Information Grid (NAVIGIG). These documents formalize the Navy's strategy and framework for the government to achieve increased operational

control of NGEN. With added control, the government increases its responsibilities for service management and delivery. FLTCYBERCOM and the NEN Program Office have acknowledged that this shift in responsibility requires the Navy to develop and establish an effective, skilled ITSM workforce.

The ITSMO has made significant progress supporting NGEN government operational readiness (GOR) efforts focused on the development and implementation of critical ITSM competencies and capabilities. Notable progress includes the development and establishment of ITSM governance, reference architecture, standards, and supporting resources, including subject matter expert support, training and design guidance, as well as tools and templates.

The ITSMO successfully launched the ITSMO Governance Board, designated NGEN ITSM "Process Owners" and chartered the ITSM Process Owners Council. The ITSM PO Council serves as the central coordination forum for Process Owners to correct cross-process issues and risks affecting delivery and quality of IT services, as well as issues caused by internal or external service providers. The Process Owner is a critical role that is accountable for the proper design, execution and continual improvement of an ITSM process and holds the responsibility and executive authority for the overall process results across the enterprise.

The ITSMO is actively drafting and evaluating charters for the ITSM Service Owner Council and Tools Advisory Group. The ITSM Service Owner Council is responsible for coordinating and governing IT service ownership. The "Service Owner" is accountable for the proper design, execution, and improvement of one or more IT services and holds the responsibility and executive authority for all aspects of the end-to-end strategic management of the service throughout its entire lifecycle. The Tools Advisory Group is responsible for guiding decisions concerning the identification and fulfillment of ITSM tools and technology requirements.

The ITSMO also developed, signed and promulgated an architecture policy directing consistency and alignment with the NGEN ITSM reference architecture — the Navy NGEN Process Definition Model



CORONADO, Calif. (April 30, 2012) Vice Adm. Michael Rogers, commander of U.S. Fleet Cyber Command and U.S. 10th Fleet, addresses Information Dominance Corps officers and Sailors of the Naval Special Warfare community at Naval Amphibious Base Coronado during an all-hands call. Fleet Cyber Command is the Navy's central operating authority for networks, cryptologic and signals intelligence, information operations, cyber, electronic warfare, and space capabilities. U.S. Navy photo by Mass Communication Specialist 2nd Class Shauntae Hinkle-Lymas.

(NNPDM). The ITSMO has conducted numerous architecture reviews with NGEN government operational readiness ITSM design teams and provided meaningful feedback and guidance to ensure compliance with standards, consistency across design efforts and products, and alignment with the NNPDM.

### ITSMO Way Ahead

As described in its charter, the ITSMO is charged with developing and executing an enterprise-wide approach to ITSM that enables standardization and operational efficiency across Navy IT organizations and programs. To do that, additional levels of governance above the ITSMO are required to empower the ITSMO to extend its reach beyond NGEN and across Navy organizational and program boundaries.

Vice Chief of Naval Operations (VCNO) Adm. Mark Ferguson said, "We no longer have the resources to let each command optimize their organization at the expense of the enterprise. We need to develop and implement a governance model that controls the number of decentralized decisions at lower levels in our organizations

that are producing sub-optimal outcomes and higher transactional costs."

In addition to continuing to provide support and guidance to NGEN transition efforts in the near-term, the ITSMO is developing a comprehensive Enterprise ITSM Governance Model to help drive consistency and alignment beyond NGEN to other IT networks, acquisition programs, and efficiency initiatives, including, but not limited to, ONE-NET, CANES, E-ITSM, and the Department of the Navy's Data Center Consolidation effort.

The ITSMO is also exploring the development of a Naval Networking Environment Process Reference Model to serve as the single, authoritative reference model for all Navy ITSM efforts across the enterprise. ●

**ERIC MARKLAND** is the Fleet Cyber Command deputy CIO for enterprise architecture.

ITSMO CONTACT INFORMATION & INQUIRIES  
LT. CMDR. TODD GLIDDEN:  
TODD.GLIDDEN@NAVY.MIL  
[HTTPS://WWW.PORTAL.NAVY.MIL/FCC-C10F/  
CIO/1/ITSMO/DEFAULT.ASPX](https://www.portal.navy.mil/fcc-c10f/cio/1/ITSMO/DEFAULT.ASPX)

# The Joint Information Environment

## ***DoD is transitioning to a single, joint, secure, reliable and agile command, control, communications and computing (C4) enterprise information environment***

*By the Office of the Deputy Chief of Naval Operations for Information Dominance (N2/N6)*

The Joint Information Environment is a construct that facilitates the convergence of the Department of Defense's multiple networks into one common and shared global network. It will provide enterprise services such as email, Internet/Web access, common software applications and cloud computing. Primary objectives behind this transition are increased operational efficiency, enhanced network security and cost savings through reduced infrastructure and manpower.

### **Key Attributes**

- The shared JIE technology infrastructure includes: a network that is defendable and virtually accessible from any location globally, strategic to tactical locations; DoD level consolidation of data centers and network operations centers; a single security architecture; and the use of enterprise services.
- The JIE infrastructure will look, feel and operate by common standards regardless of service provider and/or use (i.e., mission specific utilization) and will apply common tactics, techniques and procedures developed at the enterprise level.
- Capabilities required across DoD to enable information sharing, collaboration and interoperability will be provisioned as enterprise services. Email, Web access, mass data storage and data analytics for decision support will be provided to any access point.
- The JIE effort does not preclude the Navy from becoming a service provider for one or more designated enterprise services or infrastructure capabilities. As such, the Navy may be called upon to support the provisioning of enterprise service(s) for the entire DoD.
- The Navy will adopt JIE standards for existing programs of record and adapt to JIE standards and requirements in future IT modernization. For example, the Consolidated Afloat Networks and Enterprise Service (CANES) shipboard network will adapt to JIE standards to ensure interoperability.
- Navy components that operate and maintain portions of the shared IT infrastructure (i.e., switches, servers, routers, etc.) will do so in accordance with Space and



KEY WEST, Fla. (Sept. 16, 2012) The guided-missile destroyer USS Gravelly (DDG-107) arrives at Naval Air Station Key West to participate in UNITAS Atlantic Phase 2012. UNITAS is an annual multinational exercise hosted by U.S. 4th Fleet in the western Caribbean Sea from Sept. 17 through Sept. 28. Thirteen ships from seven partner nations are participating. U.S. Navy photo by Lt. Cmdr. Corey Barke.

Naval Warfare Systems Command (SPAWAR) IT Technical Authority through the Joint Information Environment Technical Synchronization Office (led by the Defense Information Systems Agency), and with operational direction provided by U.S. Cyber Command.

### **The JIE will:**

- Encompass all DoD networks.
- Enhance network security by employing a single security architecture.
- Save DoD IT resourcing dollars by minimizing network hardware, software and manpower.
- Provide DoD users with access to the network from anywhere in the world, to include afloat units.
- Be a network focused on protecting data as opposed to one that simply delivers hardware.

### **Moving to the JIE**

The initial focus of JIE Increment One (Fiscal Years 2013–2014) is on achieving five

core IT efficiencies in Europe:

- Network Normalization (virtualizing network applications by reducing legacy applications);
- Data Center Consolidation (from hundreds to tens);
- Identity and Access Management (single solution for all the components, services and agencies);
- Enterprise Services (email, Web and data storage); and
- Governance (single DoD-wide IT policy).

OPNAV N2/N6 is designated as the lead office for bringing the Navy's intelligence, cyber warfare, command and control, electronic warfare, battle management and knowledge of the maritime environment areas together to align oversight, governance and synchronization mechanisms to deliver end-to-end insight and accountability for Navy information requirements, investments, capability development, and force development. ●

# Robert J. Carey

Department of Defense Principal Deputy Chief Information Officer

Mr. Robert J. Carey serves as the Department of Defense Principal Deputy Chief Information Officer. Selected to this position after a brief tour as Director of Strategy and Policy for the U.S. Fleet Cyber Command/U.S. 10th Fleet his principal roles are to help lead the consolidation of the DoD information technology enterprise, as well as align, strengthen and manage the office of the DoD CIO to better serve the department's mission. From November 2006 to September 2010 he served as the fifth Department of the Navy (DON) Chief Information Officer where he championed transformation, enterprise services, the use of the Internet and information security. In his new role, he will also help strengthen the enterprise architecture, network and information security and help lead the IT workforce into the 21st century.



Robert J. Carey

Mr. Carey entered the Senior Executive Service in June 2003 as the DON Deputy Chief Information Officer (Policy and Integration) and was responsible for leading the DON CIO staff in developing strategies for achieving IM/IT enterprise integration across the department.

Mr. Carey is an active member of the U.S. Navy Reserve and currently holds the rank of captain in the Civil Engineer Corps. He was recalled to active duty for Operation Desert Shield/Storm and Operation Iraqi Freedom, where, in 2006-2007, he served in the Al Anbar province with I Marine Expeditionary Force. For more information about Mr. Carey, visit: <https://cio.gov/author/robert-j-carey/>.

CHIPS caught up with Mr. Carey at an AFCEA Hampton Roads event July 10, 2012, where he talked about the steps or "big rocks" of implementing the Joint Information Environment or JIE. The initial focus efforts that are underway across the DoD include: network normalization, data center consolidation, identity and access management and enterprise services.

**Q:** **The primary goals of the DoD's IT Modernization Strategy (<http://dodcio.defense.gov/>) are: to consolidate infrastructure, stream-**

**line processes and strengthen the workforce. Do you see these changes occurring simultaneously?**

**A:** The consolidation, standardization, homogenization [of the network environment], raising the security, changing the processes to be more efficient and effective, and then having the workforce able to do that [work] are not happening completely at the same time. The actual design of the network has to occur first to enable the security protocols to be designed in. We'll then have the basis for what the workforce needs to know to operate in the new state. So we are lagging the design just a little bit.

But it [the design] needs to come first so that the heavy lifting of the thinking through this new network architecture can be done. It will drive other governance and procedural changes on how we care and feed and optimize the network and provision it. Then what do the people that operate and run the network today have to do differently? And more importantly, what will the users do differently? Enabling the user experience is one of the things that I was pushing in the Navy [as DON CIO]. It will not be the same as it is now in 2015, 2016 [or] 2017. One will ask: How will I train to operate the network differently?

**Q:** **You said the network, are you talking about the JIE, the Joint Information Environment, or the GIG, Global Information Grid?**

**A:** From my perspective, you will see the JIE term taking a greater hold, and the GIG term used less and less. The GIG was meant to describe the overarching continuity of DoD network topologies. JIE is the network environment that includes all IT infrastructure assets to include space assets, undersea assets, and the terrestrial components ... the entire network environment.

**Q:** **Beyond just a reduction in data centers and facilities, what is the end state that you are looking for under the department-wide Data Center Consolidation effort?**

**A:** The term I use is that it is more of an optimization. Today, we have excess computing capacity, and we need to eliminate that because it costs money and we get no benefit for it. We need to standardize and homogenize the network environment so that secure network information access can be achieved.

Additionally, we are working to

optimize applications and further push for enterprise services as a method to achieve efficiencies and desired service delivery levels. Now that is not to say that we will go to a single network right away — once a threat is in, it's in [and could take down the network]. We will go to a methodology by which defense in-depth and defense in-breadth are used to protect data that is accessed by identity.

So now I can't do a search on the entire dot-mil for information I might require to do my job ... but we need to be able to afford information access to authorized users wherever they may be. I believe in the future we will be able to do that, and the most important feature of that function will be can a warfighter deployed downrange in Djibouti or Kabul — can they look for information in the entire JIE, find it, access it, conduct a transaction or render a decision and feed it into the boss in real time with whatever devices they have — that's the goal that we have. So this standardization and this common JIE environment is the only way we know to get that done.

**Q: You talked about (Commander, U.S. Cyber Command, Director, National Security Agency/Chief, Central Security Service) Gen. Keith Alexander's inability to see inside the network which makes defending it more difficult. Will transparency inside the network be part of the end state you are looking for in the JIE concept?**

**A:** Absolutely. United States Cyber Command (USCC) has the challenging and unenviable job of defending [DoD's] hundreds of network environments and enclaves that are built ever so slightly differently. Until we stratify that [complexity of networks] a good deal, affording USCC the ability to defend it and protect it and close off something that is being attacked or shut it down, we're going to be at risk. We are running and defending our networks; we are supporting the warfighter but we're running it at risk to mission. This really affords us

**"Today we have excess computing capacity, and we need to eliminate that because it costs money and we get no benefit for it."**

the ability to lower the risk and improve the protection of our information.

Because when we look at a computer today, whether you are downrange or you're here [stateside], you trust whatever is on that screen, you just do. Information shows up; it's good. But do you really, really trust it? The answer is yes, we do. But if you know about the threat you could see how that might be erroneous to do that in the future.

So we need to be able to better protect, we need to better afford Gen. Alexander and the component cyber commanders [Fleet Cyber Command, Marine Forces Cyber Command, Army Cyber Command and 24th Air Force] the ability to more simply protect and more effectively protect the networks.

**Q: Will the enterprise architecture you talked about get us there?**

**A:** Yes. The JIE enterprise architecture

will drive structural changes in the network. The reduced number of data centers and nodes that are on what is today the DISN (Defense Information System Network), the backbone, will start creating a standardized environment so that I can, in fact, protect it better, access it better and operate it more efficiently.

**Q: You talked about enabling agile IT; do you think DoD will need better acquisition models to get to the end state of standardized networks? Will it include tactical IT as well as business IT systems?**

**A:** I think it has to. We all recognize that as we change the network architecture to a more standardized design and start to build the JIE, I see us as having to become more agile, and agile is a term within acquisition to do things in smaller more orderly, bite-sized chunks. Similarly, the budget process has to change because today we are 'POM-ing' or budgeting, (Program Objective Memorandum) for things starting the end of July 2012 to figure out what we are going to do in FY15.

In IT years, FY15 is eons from now. Only a few companies are even looking that far, but we're now attempting to plan with certainty and estimate the cost of the things we want to do two

### The JIE delivers the future DoD IT environment

#### Our Approach

#### Build the Joint Information Environment Architecture

- Ruthlessly enforce during budget process
- Produce milestones to drive implementation

#### Optimize information, networks and hardware

- Application normalization, standardization and rationalization
- Data Center Consolidation
- Security architecture standardization and optimization

#### Separate server computing from end-user computing

#### Optimize support software

#### Provide common applications

- Migrate to standardized environment

and a half years from now. So both the budget process and the acquisition process have to be reconciled to this more homogenous network architecture to allow us to solve real-time problems in cyberspace.

When we deployed HBSS (Host Based Security System), for example, HBSS was an unfunded requirement and there was a lot of money that we pulled out of things that we programmed for to fund HBSS. That being said, acquiring HBSS went slower than we thought because we tend to tell our program managers to drive out risk — not necessarily to manage risk.

Similarly, we train contracting officers and IT attorneys to avoid risk, so those functions need to be reconciled and brought into the future state, whether it is IT systems, purchases of infrastructure or enterprise licensing agreements. We have to approach it differently than we do today; all of those are underway, but they are not done. Some of the process changes can occur independently of the end state, but some will be linked to the end state as well.

**Q:** In your presentation you talked about the budget crisis being a catalyst for change because people are willing to consider ideas that they would not entertain when they had money. Do you foresee that budget problems could require DoD approval for IT purchases, maybe the Under Secretary of Defense for Acquisition, Technology and Logistics or the CIO would say, “You can’t buy that — it doesn’t fit within the DoD network.”

**A:** Yes. Let me say this: I see the architecture and standards being produced for the transport layer and flagship data centers for the DoD, the ones that will become the core data centers for the Department of Defense, the backbone of computing, those standards will be promulgated.

So if you have a data center that you want to retain connected to the JIE, and you start buying something that isn’t consistent with that architecture, it will not be connected. So yes, I imagine at some point in time somebody has the ability to

say, ‘You cannot buy that, but you can buy this.’

**Q:** The Navy is doing that right now with its Information Technology Expenditure Approval Authority, but tactical systems are exempt for now. Do you think that in the future IT approval for the DoD will include warfighting systems?

**A:** It has to because the C2 systems and the sensor systems that utilize the JIE, or in today’s terms, the GiG, have to run within the GiG — not run around it, including the business systems. So for all these systems, we do not want a system to invent or build its own infrastructure; it has to be built to ride within the confines of this architecture [JIE].

**Q:** You mentioned that probably not every mobile device will be approved for use within the DoD security domain due to the risks associated with some of the devices, but what do you think will be the outcome of the DoD’s Mobile Device Strategy (<http://www.defense.gov/news/dodmobilitystrategy.pdf>)?

**A:** [Former DON CIOs] Dave Wennergen and I, and even back to Dan Porter’s days, we imagined the term ‘nomadic workforce.’ We never worried about where a member of the workforce was located but that they are ‘connected.’ In the grand scheme of operating inside the Beltway, the last thing we want is to waste an hour of somebody’s time coming to a facility just to have his warm body there when, in fact, he could do everything he needs to do from somewhere else. I think mobility changes that communications paradigm that exists in DoD today. It’s beyond telework; people tend to associate mobility with telework. It’s really about: Can I access information to render either a transaction or decision in support of a higher objective, and can I do that securely and at will?

These devices, the tablets and some of the smart phones today present a very close approximation of a laptop and its functionality. So how do we take advantage of these different form factors to

perform functions? Another thing that is maybe even more important is the app store construct which presents a way [for DoD] to invent a process to solve a problem engaging data from a handheld device and a lite app.

Many of the lite apps that you download to your smart phone have a full-blown application or website somewhere else. [Use of lite] apps has enabled us to solve problems faster, cheaper and more efficiently than before, for example, than perhaps paying a vendor to build some heavy application. I can harness the workforce’s ability and industry’s ability to innovate and build tools that I didn’t have before. I like to refer to mobility as a ‘platform of innovation.’ It is really critical that I unleash this intellectual prowess of the Department of Defense in support of problems I don’t know I have yet. That’s the cool thing.

**Q:** Can you point to any of the successes of the modernization plan?

**A:** The data centers are being identified and consolidated. Part of that is due to the fact that OMB (Office of Management and Budget) is pushing it hard, and we are pushing it hard. We are making significant progress. Applications are being, you can pick your word: normalized, rationalized, reduced. Identity management was a far off goal, like a planet, 10 years ago. People now realize the connection to identity, to data, to security, and then using identity credentials to reduce anonymity from the network.

We’ve started the standardization of the network; we’ve identified duplicative applications and eliminated many. We’ve developed a way ahead for mobility and initiated the roll out of PKI for the SIPRNET. We have begun the development of data standards, reduced the overcapacity that we have, and lastly, we’ve reduced the application stack. Now we are able to operate more efficiently than in the past. As I said in the talk today, the budget is going to be the catalyst of change for us. We are living within our means and providing information to the warfighter when he or she needs it with whatever device and location.

Structural changes are taking root in all four services and the fourth estate (DoD agencies) in such a way that we will build off it and continue the new activities into 2015, '16 and '17 and continue on the journey to deliver the JIE. We are making tangible successes. Now that we briefed our way ahead, we believe we have a tremendous amount of support from the Secretary [of Defense] and Deputy Secretary as well as the Chairman and Vice Chairman [of the Joint Chiefs].

We will be held accountable. Every service and agency will have to report what they have done, [for example], how many SIPR PKI tokens rolled out, and data centers and networks eliminated. There is a point in time where will be at our destination ... but that is a few years away. Now the question is: Is that sufficient or do we keep going? Every military department has taken money out of the budget so they have no choice but to get to this new efficient operating state.

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

**A:** We live in very exciting times. It has been very enlightening for me, while the Department of the Navy is a department of two services, now to help make a difference for all four services and the DoD. There are both challenges and opportunities that exist. The catalyst of change has become the budget, as resources become scarcer, we'll be challenged to make this transition. We will never really be done because we are always maturing the network infrastructure but this is exciting because if we had the money that we did even a few years ago, we wouldn't be working on this [IT Modernization Strategy]. So now we are working on some great things because we can't afford to fund the status quo.

**Q: Under Secretary of the Navy Robert Work said this is a time when good ideas matter.**

**A:** Absolutely. Secretary Work knows that bringing ideas to the fore is vital to the department's success. There is no dearth of ideas, ones that are thought through in the context of the problem, the budget,

"There is no dearth of ideas, ones that are thought through in the context of the problem, the budget, and the payoff in terms of a business case, those are the ones we need to wrestle to the ground. When money is tight, people are willing to do things that they weren't willing to do when they had money."

and the payoff in terms of a business case, those are the ones we need to wrestle to the ground. When money is tight, people are willing to do things that they weren't willing to do when they had money.

We are excited because this is the first time we have a solid partnership with each of the services to help build this future state. This is not a top-down dictate; this is a complete team effort with the Joint Staff. Frankly, if the Chairman and Vice Chairman were not in support of this or their IT advisers, the J6, Maj. Gen. Mark Bowman, and Marty Westphal, (assistant deputy director and chair for C4/cyberspace functional capabilities board, J8), it would be hard to push this thing. The ideas are coming and questions I get asked turn into ideas. I just had one today. We want the hard questions.

**Q: I've been reading about the Army's progress with enterprise email.**

**A:** Yes, it is coming. We are testing the validity of our model for delivery of an enterprise service, but our team at DISA (Defense Information Systems Agency) is well on their way to success. We have the Army, Air Force and Joint Staff, and the COCOMs (combatant commands) are on board, and [we] will bring aboard the Navy and Marine Corps last. ●

**FOR MORE INFORMATION**

**DOD CIO**  
<http://dodcio.defense.gov/>

**DoD's Cyber Footprint - Total Budget for FY13: \$37 billion**

**DoD IT User Base**

- ~1.4 million active duty
- ~750,000 civilian personnel
- ~1.1 million National Guard and Reserve
- 5.5+ million family members and military retirees
- 146+ countries
- 6,000+ locations

**IT Systems**

- >10,000 operational systems (20% mission critical)
- ~800 data centers
- ~65,000 servers
- ~7+ million computers and IT devices
- Thousands of networks/enclaves, email servers, firewalls, proxy servers, etc.

**Mobile devices**

- ~ 250,000 Blackberries
- ~ 5000 iOS Systems (Pilots)
- ~ 3000 Android Systems (Pilots)

# Mailbox Storage and Security Improvements Coming Soon for NMCI Users

*By Michelle Ku, Naval Enterprise Networks Public Affairs Support*



## NMCI Standard Mailbox Doubling to 100 MB of Storage Space

Navy users of the Navy Marine Corps Intranet will soon get one of their most common service requests: a larger mailbox.

By Thanksgiving, the mailbox size for every classified and unclassified Navy user will double from the standard 50 megabytes (MB) to 100 MB at no additional cost to commands. The schedule for upgrading communities of interest (COI) mailboxes has not been determined yet. A detailed deployment schedule is available on Homeport (<https://homeport.navy.mil>).

Although a 100 MB mailbox may still be considered too small to meet NMCI users' mailbox capacity requirements, this is the first step in improving mail services over the next two years through the end of the NMCI Continuity of Services Contract. An additional mailbox upgrade is expected in calendar year 2013 when NMCI upgrades mail servers to Microsoft Exchange 2010. The size of that mailbox capacity increase is

still to be determined, but will improve NMCI mail services and more closely align them with user expectations and requirements.

The additional mailbox capacity is a result of recent storage efficiency initiatives implemented by the Naval Enterprise Networks (NEN) Program Office and Hewlett-Packard Enterprise Services (HPES), the NMCI service provider, which freed approximately 700 terabytes (TB) of storage capacity space in the storage infrastructure used to support NMCI mail and file share services.

One of the major efficiencies was implemented in March 2012 when NMCI initiated a concept called "thin provisioning." In a thin provisioned storage infrastructure, storage capacity is dynamically allocated as it is used rather than statically allocated in a "thick provisioning" model. With thin provisioning, any allocated but unused storage space is made available for someone else to use.

For example, under the previous static thick provisioning model, each user was given 50 MB of mailbox space regardless of how many folders and emails users actually kept in their mailbox. If a user

used 10 MB of this space, the remaining 40 MB was still reserved for that user and could not be used to satisfy email requirements of other users. With the dynamic allocation of the thin provisioning model and the increased 100 MB mailbox capacity, if a user used 60 MB of the allocated space, only 60 MB is actually provisioned for that user. If a user needs more than the 60 MB, additional space is provisioned dynamically as required up to the allocation of 100 MB.

Since mailbox space is an issue for most NMCI users, the NEN Program Office and HPES decided to increase the size of the standard Navy mailbox. After conducting an analysis of the amount of storage available at each server farm site, the program decided on providing an additional 50 MB of space for each user.

With the larger mailboxes, the mailbox notification policies have changed. Users will receive a mailbox capacity warning when the total size of their mailbox is 90 MB. Users will not be able to send emails if their mailbox is at 100 MB capacity. At the 200 MB mark, users will no longer be able to receive messages.

The NEN Program Office and HPES



plan to increase mailbox capacity to 100 MB is currently in progress. The second increase in mailbox size will take place in calendar year 2013 following the enterprise-wide upgrade of the mail servers to Microsoft Exchange 2010. ●

## SIPRNET Token Will Eliminate Username and Password Authentication Requirement

Navy Marine Corps Intranet users with Secure Internet Protocol Router Network accounts have until Dec. 31, 2012, to obtain new SIPRNET tokens for their account.

The SIPRNET token is a smartcard issued by the Navy Public Key Infrastructure (PKI) team that enables users to securely log onto their SIPRNET account the same way that they log onto their unclassified accounts by using two-factor authentication with both the token and a unique personal identification number (PIN). The SIPRNET token will also contain PKI certificates used to digitally sign and encrypt email messages.

The implementation and support of the SIPRNET token allow the Naval Enterprise Networks Program Office and NMCI to:

- Improve the user experience by eliminating mandatory SIPRNET account password resets every 60 days.
- Increase security by replacing the current user name and password authentication with a more secure two-factor authentication system.
- Meet a Department of Defense (DoD) and United States Cyber Command mandate to enforce cryptographic logon (CLO) for all user accounts on the SIPRNET by March 31, 2013.

By implementing two-factor authentication using a SIPRNET token, network security is increased since users must present something they have (the SIPRNET token) and something they know (the SIPRNET token's PIN)



prior to being granted access to their network account. From a network user perspective, this capability allows users to eliminate the need to remember and frequently reset their SIPRNET account password.

Users are required to obtain SIPRNET tokens from the Navy PKI team, via their command's trusted agent and/or information assurance manager, by Dec. 31, 2012. Users are required to enable and enforce their NMCI SIPRNET account by March 31, 2013. Beginning April 1, 2013, SIPR users may not be able to log onto their NMCI SIPRNET accounts without using a token and PIN.

Once users have obtained a SIPRNET

token, the following steps must be completed to enable their SIPRNET network account to use their token for logon, digital signature and encryption:

- Associate the token to the user's SIPRNET account by following the procedure detailed at <https://cloenablesite.nmci.navy.smil.mil>.
- Once the token is associated with the account, call the NMCI Service Desk (866-843-6624) and request that the service desk enforce the account for CLO.

Users will not be required to complete mandatory password resets every 60 days once the token is CLO enforced. ●

### Naval Enterprise Networks

Naval Enterprise Networks (NEN) is part of the Department of the Navy's Program Executive Office for Enterprise Information Systems (PEO-EIS), which oversees a portfolio of enterprise-wide information technology programs designed to enable common business processes and provide standard IT capabilities to Sailors at sea, Marines in the field and their support systems.

PEO-EIS: [www.public.navy.mil/spawar/peoeis/Pages/default.aspx](http://www.public.navy.mil/spawar/peoeis/Pages/default.aspx)

NEN Program Office: [www.public.navy.mil/spawar/peoeis/NEN/Pages/default.aspx](http://www.public.navy.mil/spawar/peoeis/NEN/Pages/default.aspx)

# It's Time to Change the Way We Refer to SHF Satellite Communications

## *What's the flavor of your SHF SATCOM?*

By Lt. Jason J. Hughes

**FROM** a shipboard perspective, we can no longer strictly refer to super high frequency satellite communications as simply Defense Satellite Communications System (DSCS) and Commercial Broadband Satellite Program (CBSP) operations. The lines between the bands for which DSCS and CBSP have traditionally operated have blurred due to employment of new military and commercial satellites and the installation of new multi-spectrum capable shipboard terminals with high data rates. Therefore, we must change the way in which we refer to these services in Communications Spot Reports (COMSPOT) to ensure there is no ambiguity or confusion between providers and customers when working to establish and activate these links or when working to restore lost services.

In this case, the providers are the Naval Computer and Telecommunications Area Master Station Atlantic and its subordinate and partner organizations. NCTAMS LANT provides secure and reliable classified and unclassified, voice, messaging, video and data telecommunications to its customers: surface, subsurface, air and ground forces in support of command, control, communications, computers and intelligence (C4I) for real-world operations and exercises and to U.S. naval, joint and coalition operating forces worldwide.

### **UHF Versus SHF**

The narrowband ultra high frequency portion of the radio frequency spectrum has been referred to over the years as the "workhorse" of joint and naval communications; however, the demands and services we leverage on our SHF communications today brings into question which is truly the current workhorse of our Navy. Through this vital wideband link, afloat units gain access to email, Web browsing, chat rooms, message traffic, business systems database replication, file transfers and Voice over IP (VoIP) telephone service, and all through connection to the NIPRNET, SIPRNET, Joint Worldwide Intelligence Communications System (JWICS),

secure telephones, video conferencing, video teletraining, telemedicine/medical imagery, national primary image dissemination, intelligence database/tactical imagery, and more. So which part of the spectrum, UHF or SHF, could you live without for an extended period of time while deployed on a ship? Most communicators would probably put more emphasis on restoration of wideband links rather than narrowband links today.

In the past, the fleet received its SHF SATCOM from three distinct services. Force level for carriers and multipurpose amphibious assault ships and group level for cruisers and guided missile destroyers accessed the Defense Satellite Communications System with the AN/WSC-6 SATCOM terminal to a DSCS III Service Life Extension Program (SLEP) satellite that operated strictly in the X-band portion of the RF spectrum, for at most a T1 (1.544 megabytes per second (Mbps) to E1 (2.048 Mbps) data rate.

Most unit level access for frigates, mine countermeasures and coastal patrol ships accessed commercial Inmarsat satellite service with an Inmarsat terminal that operates strictly in the L-band portion of the RF spectrum, for nothing more than a 64 to 128 kilobyte per second (Kbps) data rate. Force level ships also had the ability to make use of commercial satellites for greater bandwidth up to 4 Mbps through the Commercial Wideband Satellite Program (CWSP) accessing service through an AN/WSC-8 SATCOM terminal to a commercial satellite that operated strictly in the C-band portion of the RF spectrum. During these times it was fairly clear to all stakeholders what exactly was meant when a unit was "down" on DSCS or CWSP.

The initial launch of the Wideband Global Satellite system in 2007, the replacement for the Defense Satellite Communications System III SLEP satellites, brought significant additional capacity to DSCS. In fact, one WGS satellite has about the same capacity as 10 DSCS III SLEP satellites.

The WGS satellites will complement the DSCS III SLEP and Global Broadcast Server (GBS) payloads and offset the eventual decline in DSCS III capability. The WGS system is a constellation of highly capable military communications satellites. WGS space vehicles (SVs) are the Department of Defense's highest capacity satellites. Each WGS satellite provides service in both the X and Ka frequency bands, with the unprecedented ability to cross-band between the two frequencies onboard the satellite.

WGS supplements X-band communications, provided by the Defense Satellite Communications System and augments the one-way GBS service through new two-way Ka-band service. These SATCOM improvements have enabled the ability to assign a force level ship upwards of a single 8-megabyte SHF link or two 6-megabyte SHF links; however, the Ka-band is more susceptible to weather interference much as links operating in the extremely high frequency (EHF) spectrum.

### **Terminal Advances**

The Navy has long used the AN/WSC-6 SATCOM terminal for SHF services. The AN/WSC-6(V)9 terminal installed on many guided missile destroyers enables the ability to also operate in the commercial C-band with a feed horn change out. A feed horn, horn or microwave horn is an antenna that consists of a flaring metal waveguide shaped like a horn to direct radio waves in a beam. The latest versions of the AN/WSC-6, F(V)9 and G(V)9 terminals allow simultaneous X and Ka-band operation. Therefore, it is possible for a unit to be up on the X-band and down on the Ka-band; hence, the statement of a unit being down on DSCS leaves too much ambiguity as to whether a ship is up or down on SHF services.

In 2008, the U.S. Navy Communications Program Office, under the Program Executive Office for C4I, initiated the Commercial Broadband Satellite Program to acquire commercial SATCOM operating in the C-band, commercial X, Ku, and pos-

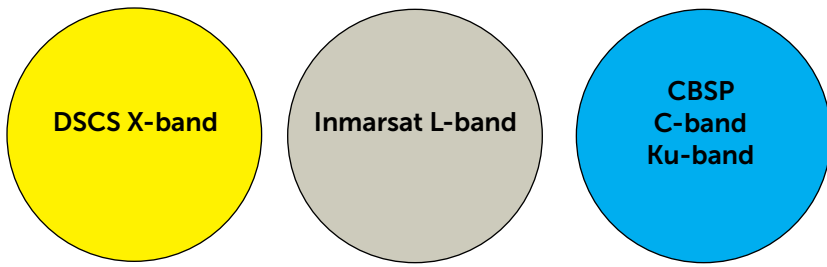


Figure 1. Graphic depicting past SHF configurations. The Defense Satellite Communications System (DSCS) operated only within the X-band of the RF spectrum. Inmarsat (a commercial service) operated within the L-band of the RF spectrum. The Commercial Wideband Satellite Program (CWSP) operated only within the C-band of the RF spectrum.

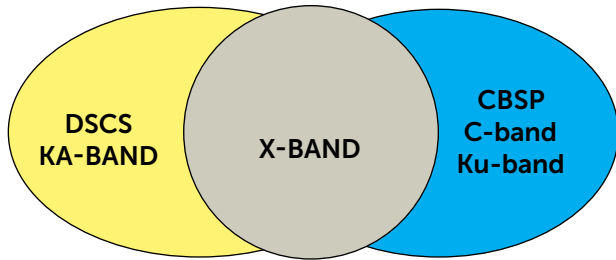


Figure 2. Graphic depicting current SHF configurations. The Defense Satellite Communications System, with the inclusion of the Wideband Global Satellite (WGS), brings the capability of Ka-band along with X-band military SHF SATCOM. The Commercial Broadband Satellite Program brings, in addition to traditional C-band, the ability to receive commercial SHF SATCOM via Ku-band and now X-band.

sibly other bands, as well as terrestrial and supporting requirements for three variants of CBSP terminals. The terminal in use is the AN/USC-69 that comes in a Force Level Variant (FLV), Unit Level Variant (ULV) and the Small Ship Variant (SSV).

The FLV is capable of operating in the Ku and C-bands and is intended to eventually replace the AN/WSC-8 terminals installed on force level units. The ULV is capable of operating in the Ku and X-bands and is mostly installed on frigates; the SSV is capable of operating only in the Ku-band, and is installed on mine countermeasures ships and coastal patrol craft and several Military Sealift Command units. Interestingly, the AN/USC-69 terminal also can allow operation in the Ka-band; however, it is not currently an option with the fleet variants in use today.

Mine countermeasures ships and patrol craft that are down on CBSP could only be down on commercial SHF SATCOM because there is no military satellite communications option that operates in the Ku-band. However, saying a frigate is down on CBSP can be confusing. From a frigate's perspective, it is down because its AN/USC-69 terminal was acquired under the CBSP program which replaced the Inmarsat terminal previously installed. From initial install to completion of a system operational verification test, it has always been referred to as CBSP; however, this is a misnomer because CBSP is a program and not a service or circuit. SHF access could be provided from a commercial Ku-band or an X-band satellite operated by a commercial provider or a military-owned DSCS satellite.

To add even more confusion, the new

Navy Multiband Terminal (NMT), AN/WSC-9, is capable of operating in the Q, Ka, X and GBS bands. The AN/WSC-9 is intended to eventually replace the AN/WSC-6 terminals beginning in fiscal year 2013, according to the Command, Control, Communications, Computers, and Intelligence Systems Program Roadmap issued under OPNAVNOTE 3090 March 26, 2010. SATCOM changes are illustrated in Figures 1 and 2.

### Communications Spot Reporting

The fleet's primary method of reporting a communications outage or degradation of service is via a COMSPOT in accordance with Navy Telecommunications Procedures (NTP) 4, Appendix B, paragraph 2 of a COMSPOT is intended to list the system, service or circuit affected. In the past, we have been able to list the system and service as DSCS or CWSP with little ambiguity or confusion to all parties involved regarding the outage or degradation encountered. Now, we can clearly see that continuing to state DSCS and CBSP in paragraph 2 of a COMSPOT fails to clearly articulate the exact system or service outage. It is now important to state whether the system, service or circuit is military or commercial SATCOM and the operating band, the satellite the unit is receiving the services from and the SHF mission number for easy reference, in accordance with a naval message issued by Naval Network Warfare Command, COMNAVNET-WARCOM DTG 01917ZAPR11.

To reduce ambiguity and ensure your outage is resolved as quickly as possible, see the text box at right for recommendations on COMSPOT completion. ●

### COMSPOT Examples

[MILSATCOM X-BAND, ELNT, CS1234-12](#)  
(Military Satellite Communications X-band of RF spectrum, East LANT DSCS satellite, mission number CS1234-12)

[MILSATCOM KA-BAND, ELNT, CS1234-12](#)  
(Military Satellite Communications Ka-band of RF spectrum, East LANT DSCS satellite, mission number CS1234-12)

[C-SATCOM C-BAND, IS-1002, CWS-123-12](#)  
(Commercial Satellite Communications C-band of RF spectrum, Intelsat Satellite 1002, mission number CWS-123-12)

[C-SATCOM KU-BAND, IS-15, CWS-123-12](#)  
(Commercial Satellite Communications Ku-band of RF spectrum, Intelsat Satellite 15, Mission number CWS-123-12)

[C-SATCOM X-BAND, SKY-5A, CWS-123-12](#)  
(Commercial Satellite Communications X-band of RF spectrum, Skynet satellite 5A, mission number CWS-123-12)

LT. JASON J. HUGHES recently served as NCTAMS LANT Joint Fleet Telecommunications Operations Center (JFTOC) director.

FOR MORE INFORMATION  
NCTAMS LANT  
[WWW.NCTAMSLANT.NAVY.MIL](http://WWW.NCTAMSLANT.NAVY.MIL)

# Matthew H. Swartz

Director, Communications and Network Division

Deputy Chief of Naval Operations for Information Dominance (N2/N6)

Mr. Matthew Swartz is a member of the Senior Executive Service and serves as Director, Communications and Networks (N2/N6F1) for the Deputy Chief of Naval Operations for Information Dominance. The N2/N6F1 Division provides oversight and resource sponsorship for Navy afloat and ashore networks and communication systems, terminals and infrastructure, and management of the electromagnetic spectrum. Additionally, N2/N6F1 is the principal Navy advisor for enterprise-wide communications and networking, enterprise initiatives that drive efficiencies in hardware, software and system procurement, and planning, programming, resourcing, and implementing the Navy's vision for an integrated afloat and ashore network, information technology, and communication systems.



Matthew H. Swartz

The establishment of N2/N6 represents a landmark transition in the evolution of naval warfare, designed to institute information dominance as a prominent Navy warfighting discipline on par with air, surface and submarine warfare, and firmly establishes the U.S. Navy's prominence in intelligence, electronic warfare, cyber warfare and information management.

Mr. Swartz responded to CHIPS questions about the U.S. Navy's Information Dominance Roadmap for Electromagnetic Spectrum Usage and how spectrum will be operationalized in the Navy in September.

**Q:** There has been recent publicity about the U.S. Navy's Information Dominance Roadmap for Electromagnetic Spectrum Usage. Can you amplify the scope of this roadmap?

**A:** In April 2011, N2/N6 approved the U.S. Navy's Information Dominance Roadmap for Electromagnetic Spectrum Usage. This roadmap is a comprehensive plan (FY2010-FY2022) to understand the Navy's EMS requirements and develop new operational capabilities. The roadmap contains four top level goals and specific actions

and tasks to achieve those goals. I've provided a graphic (Figure 1) of the roadmap goals for your readers' use and understanding and to help show how comprehensive this plan is.

Goal 1 – Assured Spectrum Access (ASA): Assured electromagnetic spectrum access is vital to maintaining our national security, military superiority, and our responsiveness to events at home and abroad.

Goal 2 – Real-Time Spectrum Operations (RTSO): The U.S. Navy has the capability to adapt spectrum usage in real-time in response to changes in the electromagnetic environment and operational requirements.

Goal 3 – Strategic E3/Spectrum Acquisition Engineering (SAE): The alignment and enforcement of Spectrum/Electromagnetic Environmental Effects (E3) policy and requirements, and emphasis on spectrum design considerations throughout the systems engineering process.

Goal 4 – E3/Spectrum Outreach and Training (O&T): Ensure that operational, acquisition and administrative workforces of Navy and DoD (military, civilian and contractor) understand and manage all aspects of E3 and the electromagnetic spectrum.

We developed the graphic to show

that there are required capabilities in Assured Access, Real-Time Spectrum Operations and the need to enforce policies and procedures through our strategic electromagnetic environmental effects (E3) and acquisition efforts, but all require a foundational capability for E3 and Spectrum Training.

**Q:** Can you talk about the National Broadband Plan and if it is related to your EM spectrum roadmap efforts?

**A:** First, let me say that the National Broadband Plan (NBP) is an important part of the N2/N6 Electromagnetic Spectrum Usage (EMSU) Roadmap; it falls under Goal No. 1, Assured Spectrum Access (ASA) and provides strategic guidance in how we balance this critical capability for economic prosperity and national security. Under this goal our first objective is to ensure the Navy must be prepared to validate and justify its EMS requirements. The pressures to reallocate portions of the EMS to support commercial interests will continue, and we must ensure we fully understand the Navy's current and future requirements.

Secondly, in June 2010, the White House released a memorandum,

'Unleashing the Wireless Broadband Revolution,' directing the identification of 500 megahertz (MHz) of new spectrum for this expansion, without impacting existing and planned federal capabilities. The portion of the EMS targeted for the commercial wireless industry, below 3 gigahertz (GHz), is heavily encumbered with existing users, including many military subscribers.

To date, the Navy has completed three assessments: (a) Fast Track Report (1675-1710 MHz, 1755-1780 MHz, 3500-3650 MHz, and 4200-4220 MHz, 4380-4400 MHz) Nov. 15, 2010; (b) an Assessment of the Viability of Accommodating Wireless Broadband in the 1755-1850 MHz Band, dated March 27, 2012; and (c) U.S. Navy Initial Response on the 5 GHz National Broadband Plan Assessment, dated 16 May 2012.

These studies indicate that there could be significant operational impacts to Navy systems. One of our studies shows that it will take in excess of \$18 billion and more than 10 years to vacate most (not all) federal operations.

**Q:** As a follow-up, can you talk about how the NBP could impact our operations worldwide?

**A:** Access and use of the EMS continues to be a critical enabler of our war-fighting capabilities. Navy leadership is cognizant and sensitive to the unprecedented spectrum demands resulting from the department's increasing reliance on spectrum-dependent technologies and the rapid modernization of commercial mobile devices.

Fully recognizing the linkages between national security and economic prosperity, the department is investing in technologies and capabilities aimed at more efficient uses and management of spectrum, and for increased interoperability with our coalition partners and with federal, state and commercial entities. Further erosion of access may reduce our operational capability. Spectrum requirements to support national defense missions are, in fact, increasing due to growing information

transfer requirements, while spectrum resources are decreasing due to commercial competition.

**Q:** You mentioned spectrum efficiency technologies; I assume you are also addressing spectrum sharing. I've read that the Defense Advanced Research Projects Agency is continuing work with flexible and dynamic spectrum access, and there is other work in sharing spectrum, for example, based on geographic separation.

**A:** Yes, we are definitely looking at all the technology organizations: DARPA, NRL (Naval Research Laboratory), CNA (Center for Naval Analyses) and ONR (Office of Naval Research), as well as industry partners to help us share spectrum. Advanced technologies that can 'sense' the presence of a radio frequency signal and wait to transmit until other equipment or systems cease use. This type of technology is called

both 'white space' and 'gray space' technologies, which are also addressed in the roadmap.

N2/N6 has held several 'industry days' venues to bring the technology organizations and industry together to discuss our views on information dominance and how they could help. Three such high level meetings have been held: Information Dominance Symposium (June 23-24, 2010), Navy Information Dominance Industry Day (March 2, 2011) and Navy Information Dominance Industry Day (March 7, 2012).

At the end of each meeting we have solicited white papers and received several informative comments from industry leads. We continue to engage industry and technology organizations to leverage work being accomplished in support of Navy efforts.

**Q:** Besides spectrum sharing, what new concepts or capabilities is the Navy investigating?

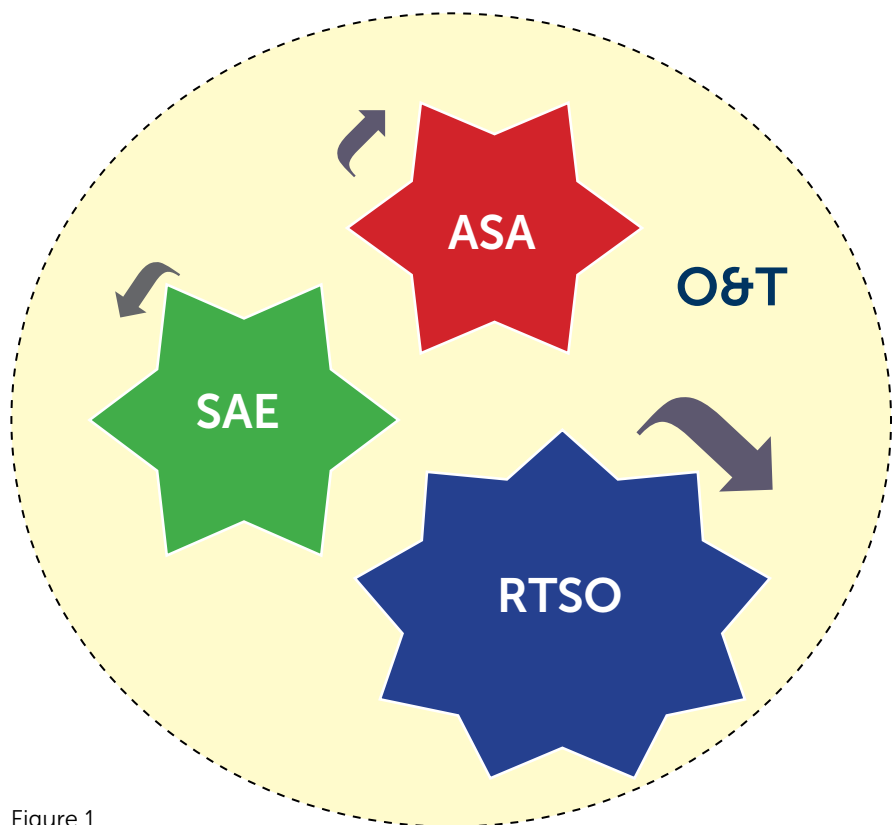


Figure 1.

**A:** I am glad you asked. In May 2010, N2/N6 published the U.S. Navy Information Dominance Vision. Early in the vision discussion, you will read a quote: 'To achieve information dominance... we must transition from a Navy that relies on individual units managing their own electromagnetic spectrum, to fleets and battle forces collectively achieving command and control over the electromagnetic spectrum in an automated fashion.' This is the heart of the Real-Time Spectrum Operations concept and a major goal of the roadmap.

In day-to-day operations, the fleet can experience electromagnetic interference (EMI) which can result in performance degradation of mission critical systems. You realize that today's shipboard systems overlap specific spectrum bands and therefore cause EMI.

But if we could effectively manage all the emissions on a given ship, we could control which systems are on and which systems are off, and determine where this free space is and then use it. This would ultimately eliminate a major portion of the blue-on-blue EMI.

**Q:** **What technologies are being utilized to support your RTSO concepts?**

**A:** We are currently investigating technologies to allow systems to sense their EMS environment and change to another frequency, but we would not want systems to be hopping all over the place without a centralized controller. This is where the RTSO capability comes into play.

RTSO is the orchestra conductor to direct which systems operate and for how long — all in order to comply with the commander's intent.

In the order of battle, we will need systems to engage at certain times and we need systems to listen during other engagements, but it is all based on the current war effort, information dominance or sharing priorities, and commander's intent. As you can quickly see the effort becomes very compli-

cated. The EMS Usage Roadmap lays out a plan starting in FY 2012 through FY 2022 to provide incremental capabilities to control the spectrum of all systems on all platforms and strike groups.

**"Our Sailors need to sense, understand and employ the EMS environment in a similar way that submariners (officers and enlisted) eventually mastered acoustics and the undersea domain."**

**Q:** **On the second of November 2011, the CNO, in his remarks to the House Armed Services Committee, discussed "operationalizing the electromagnetic spectrum." Can you elaborate?**

**A:** This electromagnetic spectrum presents us with challenges and opportunities in the 21st century similar to the undersea domain in the 20th century. Like the undersea domain, the EMS environment is an area we can use to gain an advantage over our adversaries. To command this new environment, we need the ability to monitor and be aware of the electromagnetic environment, manage our emissions, inconspicuously communicate, find, track and defeat threats, and conduct attacks as needed.

Our Sailors need to sense, understand and employ the EMS environment in a similar way that submariners (officers and enlisted) eventually mastered acoustics and the undersea domain. Today, we understand how specific adversary radars and communications systems work, emissions that indicate a threat or attack, which signals and techniques can defeat

those EM systems, and the effects of the atmosphere on EM activity. But this knowledge and capability is exclusively inherent in different — but specific — systems and people, and is not managed in real time. Going forward, we will develop the sensors and ability to pull all this information together coherently and continuously.

I should mention that electronic warfare (EW) is inextricably connected to the EM spectrum. Command and control (C2) of spectrum depends heavily on traditional EW components (electronic attack and electronic protect). We are working very closely with the EW community to leverage new operational concepts for electronic warfare and electromagnetic battle management (EWBM/EMBM).

Since the CNO's testimony we have moved forward with the idea that EM signals in all frequency bands (transmit and receive), must be part of this discussion. For example, large-scale communications, radars, tactical data links and SIGINT (signals intelligence) collection transit the same EM spectrum as our EW systems. There are good explanations for how we have traditionally sustained and employed these assets, but technology has advanced to a point that makes those distinctions less and less important.

We are at the very beginning of an effort to synchronize the planning and operation of our emitters across the entire EM spectrum. This synchronization will be mostly manual at first, but must eventually transition to significant automation if we hope to avoid EM fratricide and operate faster than the threat in this complex environment.

**Q:** **Can you talk about the Information Dominance Corps?**

**A:** The Navy created the IDC as a means of leveraging the specialized skills of the information workforce and synthesizing the value of each IDC sub-community into an even more effective warfighting capability.

Our goal is pretty simple. In essence,

our goal is to recruit, hire, educate and then retain the world-renowned, world-class workforce in the information arena — anything less than that is underachieving.

To do that, we need to change some of the processes we have for how we recruit, how we hire, and certainly we need to alter our training and education structures. Right now, we train by stovepipes.

Our intent is to broaden, as well as deepen the skill sets of the members of the IDC. Whether military or civilian, each member will not only understand his or her role within their respective IDC sub-community or discipline (i.e., oceanography, meteorology, information warfare, communications, networks, intelligence, spectrum, etc.), but how their sub-community and their individual work relates to the other ID disciplines and how it adds value to Navy missions.

We will still develop the experts and expertise that the IDC has historically provided; indeed, what the IDC's component communities are traditionally known for. Our more senior members will emerge from their parent discipline and assume leadership positions within other IDC sub-communities.

Navy leaders both inside and outside the IDC can expect the same specialized, unique expertise from the IDC. Under this reformed construct, however, they can also expect senior professionals with the broadened knowledge, expertise and experience necessary to draw on all aspects of the information realm in support of the commander.

**Q: Do you have any other comments?**

**A:** We have made great strides in executing our EM Spectrum Usage Roadmap. The roadmap was published last year, and is already in need of review and update. My team is currently reviewing the roadmap and developing updates for the future; they will push the envelope to forecast spectrum capabilities through FY 2027. I have asked my team to perform yearly reviews and up-

**"Our challenge is to establish, maintain and ensure continued access to critical information and employ essential C2 over the EMS, especially in high threat, anti-access and area-denial scenarios at sea."**

dates; this challenge has been accepted.

Also, you may be aware OPNAV is currently revising and updating the Information Dominance Roadmap, focused on assured C2, battlespace awareness and integrated fires. Access to and maneuver within the EMS is a fundamental requirement of all these areas. The EMSU Roadmap can be thought of as providing an increased level of fidelity on the spectrum strategy that supports the overall ID Roadmap that is being updated.

In closing, these are extremely exciting times; not just for the Navy, but across the Department of Defense. The continuing information revolution presents both opportunities and challenges for the U.S. Navy. The Navy has long enjoyed operating from the information 'high ground,' employing superior information-based intelligence and network technologies better and faster than our adversaries.

There is an opportunity to extend our existing advantages and to further improve how we collect, process and exploit the electromagnetic spectrum well into the future. Our challenge is to establish, maintain and ensure continued access to critical information and employ essential C2 over the EMS, especially in high threat, anti-access and area-denial scenarios at sea. ●

**FOR MORE INFORMATION**  
MR. MATTHEW H. SWARTZ BIOGRAPHY  
[WWW.NAVY.MIL](http://WWW.NAVY.MIL)



## Information Dominance Corps Reserve Command

NAVMIN 215/12 designated the Commander, Information Dominance Corps Reserve Command (CIDCRC) as the IDC reserve type commander with responsibility to man, train and professionally develop IDC Reserve Sailors in the following designators and ratings:

- ◆ Information Warfare officers (181X, 644X, 744X designators).
- ◆ Information Professional officers (182X, 642X, 742X designators).
- ◆ Intelligence officers (183X, 645X, 745X designators).
- ◆ Space Cadre officers (5500x or 6206x subspecialty codes or VSx AQD).
- ◆ Cryptologic Technicians (CTI, CTN, CTR, CTT ratings).
- ◆ Intelligence Specialists.
- ◆ Information Systems Technicians.

IDCRC units are aligned to a broad spectrum of active component commands, with units and/or billets assigned in support of every numbered fleet, every combatant command, combat support agencies, OPNAV, and the full spectrum of warfare and support enterprises. IDCRC personnel provide operational support to active component commands through mobilization as well as other types of operational orders. ●

*Office of the Deputy Chief of Naval Operations for Information Dominance (N2/N6)*

U.S. Navy Cmdr. James B. "Jamie" Gateau, Combined Endeavor 12 Strategic Plans  
 Canadian Army Lt. Col. TS McLean, CE12 Officer-in-Command, Combined Joint  
 Communication Control Center

Combined Endeavor is a U.S. European Command-sponsored multinational exercise intended to enhance communication network interoperability and information exchange among nations with common stability, security and sustainment goals and objectives.

CE is the largest command, control, communications and computers (C4) interoperability event in the world. Each year, more than 1,000 communications professionals from about 40 NATO and Partnership for Peace countries, and other strategic security partners, gather at a main operating base and a virtual forward site to conduct a series of operationally-focused interoperability tests.

Multiple remote national sites supporting live troop movements and training are integrated into the overall scenario via high frequency radio or satellite links. This year Combined Endeavor ran from Sept. 6 to 20. CHIPS caught up with U.S. Navy Cmdr. Gateau and Canadian Army Lt. Col. McLean in the middle of CE to talk about the unique advantages of working in a large coalition of communications professionals.



U.S. Navy Cmdr. James B. "Jamie" Gateau and Lt. Col. TS McLean during Combined Endeavor in Grafenwoehr, Germany.

**Q:** It has been said that the Interoperability Guide (IOG) is the single most important product produced after each CE. Does the IOG include specific equipment for the coalition to use or just standards for interoperability?

**GATEAU:** The IOG is a database that specifies the type of equipment, firmware and software and the interoperability test system data collection of each Combined Endeavor for the last 17 years. It also provides the test criteria and results to recreate an understanding of what we meant when we judged a test to be successful. Over the years, many nations have successfully used the IOG to plan and execute coalition networks.

Joint Interoperability Test Command provides the IOG to EUCOM and

participating nations. They [JITC] also provide support for planning and execution of the interoperability tests and provide third-party verification, ensuring the reliability, validity and repeatability of the information obtained as part of the tests. The IOG can provide multinational communications planners with a high degree of certainty that the C4 equipment of each nation will interoperate, potentially streamlining C4 planning for multinational operations. Countries can access IOG interoperability information on the Web, or contact JITC for help if they don't have access to the IOG.

**Q:** Is the alleged problem with using the IOG that it is just too big with too much information to find what you need to plan a mission?

**MCLEAN:** The IOG contains everything you could want to know about every test ever conducted at Combined Endeavor; unfortunately, it is not very well organized for use as an interactive C4 planning tool. On the other hand, JITC has not had sufficient input or feedback from coalition C4 planners to fix that because, unless you are involved in Combined Endeavor, the IOG is not something you use on a regular basis. In Canada, for example, we don't use the IOG in our military C4 planning because we have never done the work with JITC to make it more useful for that purpose.

**Q:** So CE doesn't usually include new technologies?

**GATEAU:** It happens not to this year, but we've seen many introduced over the 18 years of the exercise. Every year, though,



you could say we see an increase in technology sophistication. For instance, over the 18-year history of CE, countries have gone from very simple radio communications to full-fledged battle command networks. This year, Ukraine is testing WiMAX, which you couldn't say is a new technology; but it is new to Ukraine since they haven't tested it at a previous Combined Endeavor.

Moreover, we no longer simply look at the technical interoperability of two pieces of equipment, one to the other; rather, we now look at information put into the network by a commander or sensor at one level of command and have the assessors follow that information through several different countries and echelons of command to see if the information makes its way in a timely, accurate and secure manner to the various commanders and staffs throughout the simulated combined joint task force (CJTF) who need it.

**MCLEAN:** What we often see is the next version of a piece of software or firmware. Most changes in technology at Combined Endeavor are evolutionary; things which aren't completely new, but aren't completely familiar either. Additionally, we rarely see technologies that have never been fielded operationally—but that's to be expected. CE isn't the venue for experimental equipment; there are other events better suited to that purpose. Combined Endeavor is where we test fielded (or near-to-be-fielded) equipment with real signal operators.

### **Q: What new skills can participants learn in CE12?**

**GATEAU:** New skills include the tactics, techniques and procedures (TTPs) required to build, operate, maintain and defend a coalition network. Countries do indeed use CE as a training opportunity; they bring new [versions of] kit, but also junior operators who need to learn that kit. Additionally, there are a number of positions within CE that have to be filled that model a CJTF Network Control Center. It supports an order of battle interconnected with a large computer

network that has to be operated, defended, maintained and troubleshot.

We need technical experts, the best guys on the field, to isolate, identify and fix the weird things that happen to a network like this in order to gain collective experience with such networks, and the junior operators can certainly learn from them.

### **Q: I noticed that you have a cyber component to Combined Endeavor.**

**GATEAU:** There are two other events hosted at Combined Endeavor: Cyber Endeavor and Phoenix Endeavor. Cyber Endeavor is a series of seminars, covering technical and management tracks in cyber security and computer network defense. The management track includes the overarching concepts of auditing a network. The technical track includes such topics as incident response, intrusion detection and building firewalls.

The second event hosted at CE is Phoenix Endeavor. It teaches spectrum management: the tools, methods and processes. We found that while many nations in Europe were producing spectrum managers with good skills, those skills didn't always translate to a multinational or coalition environment. Europe is a very contested spectrum environment with different rules and laws. Electromagnetic waves do not obey borders and lines on a map; it is a very tricky problem and Phoenix Endeavor allows people to learn European rules with the specific goal of becoming a spectrum manager for a JTF.

Beyond those two specialized events, there are specific 'cyber injects' included in the operational scenario at CE itself. After building the coalition network and conducting functional tests between the various systems, we run a humanitarian assistance/disaster relief scenario for the CJTF. That scenario includes a number of physical security and combat events to test battle management system interoperability, but also a number of cyber events to test network defenses within the CJTF.

### **Q: So the roles to be filled for Combined Endeavor are designated in the planning stages before CE begins?**

**GATEAU:** The planning for Combined Endeavor is actually part of the exercise and part of the training; it is an interconnected, integrated process of planning, building, operating and defending a coalition network by a multinational team. As we design the network, we designate the nations which will serve at various echelons in the CJTF as well as the test regime. This allows us to collect data on both how to plan and how to run a federated coalition network.

Interestingly, everyone in Combined Endeavor is volunteered by their nations for the seven weeks of the exercise. We all have full-time jobs, so we do this in addition to our day jobs. Everyone in Combined Endeavor is highly dedicated—there are 42 nations and organizations, about 1,200 people, and 42 high frequency stations located all over Europe. Combined Endeavor is planned in less than 20 days over four conferences, including the network infrastructure, services and applications, and the real life planning considerations of radio frequency clearances and satellite access that have to be coordinated with the German government since we are hosted in Grafenwoehr. There are more than 1,000 interoperability tests and multiple remote sites. It's pretty impressive.

In addition to evaluating the systems and networks and the planning process, Combined Endeavor has a director of evaluation cell that is responsible for evaluating how well CE meets its own goals and objectives. We have Navy Reserve [information systems technology] Sailors from an Atlanta, Ga., unit, led by Cmdr. Joey Dodgen [commanding officer of the Navy Reserve J6 unit and director of evaluations for CE12] who volunteered to aid in this assessment. Joey, who is the director of evaluation collection analysis, also has troops augmenting several other functions at CE.

### **Q: In addition to the Navy's role in evaluation collection**

**and analysis, what is the unique testing that the Navy is doing with Finland's Global Command Control System (GCCS)?**

**GATEAU:** This year, Commander, U.S. Naval Forces Europe is deploying its Maritime Ashore Support Team (CNE-MAST) from Sigonella, Sicily, to Grafenwoehr, Germany, to simulate a noncombatant evacuation operation scenario. Due to the long timelines involved, both in planning CE and re-tasking an operational capability, CNE-MAST wasn't quite ready to be fully integrated into CE12. It is exactly the kind of operational unit we want to bring to CE, but CE is hard to integrate into real-world operations. Instead, we hosted them at CE to test interoperability between GCCS-M and the organic Finnish Navy Sea Surveillance System (MEVAT) — its own GCCS-M — and, point-to-point [network topology], we proved it does, in fact, work.

This test included the sort of cryptographic devices you would see in complicated, real-world operations using Type 1 encryption over a link. We can't generally require crypto at CE, as it is not available to all participants. In this case, the test was very successful. We expect they [Finland] will come again next year and demonstrate [MEVAT] on the coalition network.

**Q: So in the planning conferences, one network is built — or each nation brings its own network?**

**MCLEAN:** A bit of both, actually. Each nation has its own network of computers, phones, radios and so on that they use in national operations. For CE, the nations are formed into coherent multinational military units and formations within a simulated CJTF to respond to the humanitarian and security crisis described in the scenario. This results in a number of multinational brigade headquarters with subordinate battalions, companies and platoons that connect with each other and with air and maritime components within the CJTF to create the coalition network (CNet).

That's where the complexity lies: interconnecting the various national networks to form the international network over which coalition command and control is exercised. A simple telephone call, for example, might pass through five different national networks; computers routinely exchange operational data across four or more networks within the federation.

**GATEAU:** We are also encouraging more countries to participate from home stations and to link CE exercise play and testing into real-world operations centers. This reduces costs and has the added benefits of increasing participation and linking in real-world systems that nations would ultimately use in response to a crisis.

**Q: Do nations come to Combined Endeavor with their own objectives or do they focus on the overall objective of interoperability?**

**GATEAU:** CE has overall goals and objectives, but each nation comes with their own that determine which systems they will bring, which echelon of the CJTF they will play [in] and which tests they will conduct.

**MCLEAN:** I can speak to how it works for Canada. We come to Combined Endeavor to test our equipment and procedures to ensure they are interoperable with coalition partners such as those with whom we are currently operating in the International Security Assistance Force (ISAF) in Afghanistan.

We do not want to spend money and time on equipment that is not going to be able to operate effectively within a coalition force. We not only need to be able to work within a coalition — we need to be capable of responding with our allies and coalition partners on short notice. Combined endeavor lets us work out interoperability issues before we need to really employ them, so that our C4 systems stand ready for short notice coalition operations.

This year in Combined Endeavor, the

coalition is simulating the provision of humanitarian aid and disaster relief to a troubled nation in an unstable part of the world that just experienced a serious earthquake. International aid convoys are ambushed by local gangs and the instability of the country's internal security situation is affecting neighboring countries. The coalition must conduct an operation to evacuate international civilians from the region (i.e., a noncombatant evacuation operation). Finally, on top of all that, the country located immediately to the north attempts to take advantage of the chaos by invading under the guise of providing relief and assistance. These are evocative of the types of real-world events in which we all now routinely operate. It is within the framework of this overall scenario and the C4 systems that each nation would bring to such an operation that the individual nations express their national goals and objectives for interoperability testing at CE.

At this point, we should probably talk a bit about the Future Mission Network (FMN). It is the attempt to codify the lessons learned from ISAF and the Afghan Mission Network (AMN). COMISAF (Commander ISAF) needed all of his subordinate units within ISAF to communicate on a single coalition network. Instead of doing what we usually do in such situations — that is, simply putting everyone on the Combined Enterprise Regional Information Exchange System-International Security Assistance Force (CENTRIXS ISAF) network or, perhaps, a single Mission Secret Network for Afghanistan provided by NATO — the nations agreed to federate their own systems into a single security domain on a common network. That federated network is the AMN.

**GATEAU:** In the CENTRIXS model that TS mentioned, the United States would effectively provide the entire network and pay for all the equipment. It was to our advantage to do that because we wanted to work with the coalition. But now we simply can't afford it, and as multiple nations have developed their own command and control systems and processes, it doesn't make sense to

move them onto 'our' network and make them use our systems. There is a better way with the FMN.

Late last year, the Joint Staff J6 was tasked by the Chairman to 'evolve the Future Mission Network' so that the United States would be ready to operate in future coalitions. As the sponsoring COCOM (combatant commander), EUCOM has championed a model where, as in AMN, countries could work on the equipment they know and understand, instead of having them have to learn something new.

The Joint Staff has tasked EUCOM and CE to evaluate and improve FMN JMEI (Joining Membership and Exiting Instructions). This is a different paradigm from the past. Previously, CE simply produced an exercise plan useful only for that exercise and TTPs that — although applicable to all coalition operations — were rarely made available to other units. FMN gives us an outlet for our tested interoperable configurations: joining instructions that explain how to configure to work together in coalition exercises and operations.

FMN is a framework that provides, as a minimum, the enterprise services of video teleconferencing, Voice over IP, chat, email with attachments, Web browsing and global address list sharing for mission partner operations on a single security level. The goal of FMN is to take the fight off of SIPRNET (DoD's U.S.-only classified network) and onto the coalition mission network where all the coalition partners can operate together with their own battle command systems and processes. To be successful, FMN needs to be incorporated into operational plans, exercises and training; this is what CE planners really do, but before FMN and JMEI it has been hard to export that knowledge, getting it into instructions and making it available to everyone.

FMN eliminates the limiting factors when conducting mission partner operations solely on the SIPRNET for strategic and operational commanders. It provides governance, policy and standards. FMN looks at the entire DOTMLPF (doctrine, organization, train-

GRAFENWOEHR, Germany (Sept. 11, 2012) Key leaders listen to morning briefings during Combined Endeavor 2012 at U.S. Army Joint Multinational Training Command. Photo by U.S. Air Force Tech. Sgt. Araceli Alarcon.



ing, materiel, leadership and education, personnel and facilities) solution. In order to work through interoperability problems, it leverages exercises like CE and CWIX (Coalition Warrior Interoperability Exploration), and capabilities like CIAV (Coalition Interoperability Assurance and Validation).

**Q: Working with so many organizations is a great opportunity — what is the most exciting part of the exercise or most beneficial?**

**GATEAU:** The simple fact of getting to work with so many multinational IT professionals is, for me, the most beneficial part. We get to see how other nations solve their C4 problems, how they meet interoperability hurdles, and we get to learn from each other. The human connections we make are at least as important as the 'green' — successful — interoperability tests. I've had to work with a number of CE participants in my day job. Since we already have a relationship and shared experiences, it is much easier to work together.

On a more general level, we all benefit from increased human interoperability, learning about other cultures and establishing the relationships in the exercise that we will need in operations.

**MCLEAN:** I would have to agree with Jamie. The most beneficial part of participating in CE is the opportunity to

share experiences with and learn from military IT professionals from 41 other nations and organizations, most of whom are facing the same technical and procedural challenges we are, and many of whom routinely participate in coalition operations of which Canada and the Canadian Forces are a part.

I also believe that it is an opportunity for Canada, and other nations, to share the benefits of our own, sometimes unique, perspectives and experiences regarding the operational and technical interoperability of C4 systems with a community of like-minded allies and potential coalition partners in order to improve our collective C4 interoperability and readiness.

**Q: Is there anything else you would like to add?**

**GATEAU:** I just want to add that I would be remiss if I didn't mention the U.S. Army Joint Multinational Training Command (<http://www.eur.army.mil/jmtc/>) in Grafenwoehr, Germany, that is hosting Combined Endeavor. JMTC has fantastic simulation centers and facilities to connect everyone up and provide realistic training. The best part is that lessons learned can be immediately transferred to the battlefield in Afghanistan. ●

**FOR MORE INFORMATION**  
[www.eucom.mil/combined-endeavor](http://www.eucom.mil/combined-endeavor)

# A New Century for Unmanned Maritime Systems

**T**ODAY'S UNMANNED VEHICLES can trace their roots back to the inventor of alternating current (AC), Nikola Tesla (1856-1943).

Renowned for his work with AC motors, dynamos, hydroelectric power and X-ray technology, Tesla found time to invent the world's first practical remote-controlled unmanned vessel. In 1898, Tesla was granted a U.S. patent for a "Method of and Apparatus for Controlling Mechanism of Moving Vessels or Vehicles." The patent covered "any type of vessel or vehicle which is capable of being propelled and directed, such as a boat, a balloon or a carriage." During an electrical industry trade show at Madison Square Garden in New York, Tesla publicly demonstrated his unmanned ship in a large tank of water. The historic event created some sensation about his method of using radio for command and control.

While adoption of unmanned aircraft is reaching epic proportions, unmanned maritime systems (UMS) have had slower progress. But during the next decade, a significant increase in the application of UMS is anticipated. Unmanned maritime systems, which include surface and underwater vessels, will provide enhanced capabilities to maritime administrators and operators with a significant reduction in costs. Studies predict an investment of billions of dollars will create a new generation of unmanned vehicles for various land, sea and air functions.

Applications for UMS can be classified into two main groups: commercial and governmental. Commercial applications will provide services to be sold by contractors in the course of carrying out normal business operations. Governmental applications, on the other hand, will ensure public safety and security by addressing different emergencies, issues of public interest and scientific matters.



RELIABLE RADIO FREQUENCIES TO SUPPORT RELAYED COMMAND AND CONTROL ARE VITAL ... ALONG WITH THE "SENSE AND AVOID" SUPPORT REQUIREMENT.

Unmanned maritime systems are especially practical for hostile maritime environments in which deploying a crewed vessel is ill-advised. Hostile waters include high threat environments or areas contaminated by nuclear, biological or chemical agents. A key challenge for the global introduction of unmanned maritime systems is reassuring all maritime administrations and organizations that operations will integrate seamlessly into current manned maritime procedures and that UMS operations are safe.

Another critical priority for operating unmanned maritime systems is the seamless integration into the global

maritime communication environment. Unmanned maritime systems will use the same equipment as manned vessels to communicate with vessel traffic control. However, due to the remote nature of human interaction, command and control are vital to operating unmanned maritime systems and will influence the eventual development of composite electromagnetic spectrum requirements.

Like many current unmanned aircraft systems, UMS command and control will be transmitted via radio frequency links between the control station and the unmanned systems. For safe operations of an unmanned maritime system,

highly reliable radio communications between the UMS and the maritime control station are required to support sense and avoid functions. In the end, unrestricted and autonomous unmanned maritime systems operations will rely on critical communications.

Current traffic management relies heavily on the internationally used Automatic Identification System. AIS is a tracking system used on ships and by vessel traffic services for identifying and locating vessels by electronically exchanging data with other nearby ships and AIS base stations. The AIS provides information such as vessel unique identification, position, course and speed. New operational requirements for a future maritime data link environment will need to be developed. In some environments, additional radio frequency links called vessel traffic control relay will be required to relay communications received and transmitted by unmanned maritime

systems. Reliable radio frequencies to support relayed command and control are vital and must be considered along with the "sense and avoid" support requirement. These communications are especially critical for safe navigation in high-traffic maritime areas. In the near future, international standards may be necessary to develop these types of communications.

Sense and avoid corresponds to the piloting principle "see and avoid," which is used in all situations where a vessel's operator is responsible for ensuring adequate separation from nearby vessels, terrain and obstacles, including weather. To determine appropriate spectrum characteristics related to sense and avoid, two aspects must be considered.

First, all radio frequency equipment designed to collect raw data related to the "sense" function will have identified requirements specified by the planned radio services. For example, UMS radar equipment will operate in internationally allocated radio-determined frequency bands. The data derived by the sensors could either be directly processed inside a UMS or transmitted to the maritime control station for processing.

Second, sense and avoid system functions will be continually or regularly checked at the maritime control station for proper operation. Sense and avoid equipment parameters may also be modified by a maritime control station and transmitted back to an unmanned maritime system depending on the area, weather conditions or level of autonomy.

Bidirectional sense and avoid communications between a maritime control station and an unmanned maritime system will require two distinct sense and avoid information streams. A data downlink will allow the maritime control station to control sense and avoid operations according to local conditions, while a data uplink from a UMS to a maritime control station will provide feedback that the sense and avoid functions are operating properly.

As with current unmanned aircraft systems, the need to send sense and avoid video streams must also be considered. Similar to command and control, sense and avoid data spectrum requirements must be compliant with future standards for the safe operation of an unmanned maritime system in areas under the responsibility of maritime authorities.

Safe operations of unmanned maritime systems may also require alternative back-up communications to ensure high reliability of critical communications links. An unmanned maritime system must be able to operate in both high and low density sea environments. The vessel traffic control system may not be able to restrict an unmanned maritime system to low-density space. Larger systems are likely to be equipped with terrestrial communication capabilities such as geostationary satellite links. However, the impact of latency on unmanned maritime systems' command-and-control systems will be critical when considering the safety of operations.

While today's 21st century UMS technology has developed from Nikola Tesla's 19th century vision, it remains an emerging technology. Many challenges, including the operational complexities of managing radio frequency electromagnetic spectrum, must be overcome for unmanned maritime systems to become commonplace in commercial and governmental applications. The DON Chief Information Officer maintains continual national and international engagement in electromagnetic spectrum and maritime regulatory bodies to ensure the success of naval UMS for our Sailors and Marines. ●

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

**STEVE WARD** provides international spectrum strategy support to the Department of the Navy.



*By Jim Knox*

# STOP REINVENTING THE WHEEL

## KNOWLEDGE MANAGEMENT IN THE DEPARTMENT OF THE NAVY

In today's complex operating environment, a knowledge advantage is a key to effective performance. However, due to information overload and an inability to tap into knowledge generated by others, we often "re-invent the wheel" instead of building on knowledge that already exists within the departments of the Navy and Defense. How can we capture the richness of that knowledge and reduce the cycle time needed to make decisions and complete actions — by employing the principles of knowledge management.

### **What is Knowledge? What is KM?**

There are many definitions of knowledge; one idea holds that knowledge is the understanding of a discipline, topic or task. Also, knowledge can be thought of as the specific information relevant to a user's task or decision.

Knowledge can be defined as being either explicit or tacit. Explicit knowledge is recorded in some media. Tacit knowledge is not recorded; it resides in our minds. In the case of tacit knowledge, people are not always aware of the knowledge they possess or how it can be valuable to others.

Knowledge management means different things to different people and organizations. Examples of KM include: maintaining knowledge repositories, battle rhythm management, knowledge capture interviews with subject matter experts (SMEs), threaded discussions, expertise locators or "yellow

books," lessons learned and collaboration methods. Some refer to KM as a "hot wash" or "turnover." Any way you slice and dice it — building and refining KM is an effective way to preserve and reuse the knowledge and experience of our people.

The application of KM practices can capture both tacit and explicit knowledge and make it available to those who need it. To be effective, KM efforts must be relevant and meaningful to the stakeholders of a command or organization. Merely standing up a portal is not practicing KM and will not produce results that can be sustained over time.

A Department of the Navy definition of knowledge management is: "KM systematically brings together people and processes, enabled by technology, to affect the exchange of operationally relevant information and expertise to increase organizational performance."



Knowledge Management captures and quickly and easily provides (push and/or pull) knowledge (actionable information) to users (people, processes, and systems) when they need it to make a decision or complete an action.

### Putting KM to Use

Chances are your command is already taking advantage of some aspects of KM even though it might not be thought of as KM. On the other hand, many DON and DoD organizations have robust KM programs. A number of these commands have shared their KM experience at the DON Information Technology Conferences hosted by the DON Chief Information Officer in KM sessions over the last several years. Commands sharing lessons learned include: Commander, Pacific Fleet, Marine Corps Combat Development Command, Joint Enabling Capabilities Command, U.S. Army Combined Arms Center, Space and Naval Warfare Systems Command, Tactical Training Group Pacific, NASA and Naval Special Warfare Command. These commands have been practicing KM for several years with notable results.

### Top Cover

The DON CIO released the DON Knowledge Management Strategy on Oct. 20, 2005 (<http://www.doncio.navy.mil/uploads/1230NIM61275.pdf>). Since that time, KM efforts continued to mature within the department.

On July 16, 2012, the Chief of Naval Operations issued OPNAV Instruction 3120.32D, *Standard Organization and Regulations of the U.S. Navy*, which contains the new Standard Organization and Regulations Manual (SORM). The manual specifies the establishment of a knowledge management officer in Navy commands. KM is not a program of record in the DON, so the SORM update is significant because it is the first directive implementing knowledge management in the Navy. The SORM (<http://doni.daps.dla.mil/Directives/03000%20Naval%20Operations%20and%20Readiness/03-100%20Naval%20Operations%20Support/3120.32D.pdf>) states:

#### 3.4.22 KNOWLEDGE MANAGEMENT OFFICER (KMO)

a. BASIC FUNCTION. The KMO is designated in writing by the commanding officer as the focal point of the integration of people and processes, enabled by technology, to facilitate the exchange of operationally relevant information and expertise to increase organizational performance.

b. DUTIES, RESPONSIBILITIES, AND AUTHORITY. The KMO develops and executes a KM strategy for the unit, leveraging technology, to improve communications, collaboration and information exchange within the command and outside organizations.

c. ORGANIZATIONAL RELATIONSHIPS. The KMO reports directly to the commanding officer, regarding the effective management of the unit knowledge management program. The KMO coordinates with the FDO (foreign disclosure officer), security manager, IAM (information assurance officer) OPSEC (operations security) officer and the PAO (public affairs officer), regarding information exchanges with internal and external audiences, as well to ensure both proper use of official information and coordination of Internet-based capabilities.

d. REFERENCE. DON Knowledge Management Strategy (DON CIO MEMO 20OCT2005).

### DON CIO Command KM Course

The Department of the Navy's KM champion is the DON Chief Information Officer (CIO). The DON CIO Director of Information and Knowledge Management, Jim Knox, leads a two-day Command KM Course several times a year in the Norfolk, Va., and San Diego, Calif., fleet concentration areas. He and his team are also available to provide special assistance to commands that are interested in standing up or improving their KM programs.

Classes are designed to be interactive with plenty of group discussion and participation. Participants receive tips and techniques for building and sustaining successful KM programs within their commands as well as instructions and templates for several no-cost KM processes that can be implemented immediately.

Mr. Knox and two of his colleagues led a Command KM Course in Norfolk in August for more than 90 Navy, Marine Corps, Army and Air Force military and civilian personnel. This article presents just a few of the concepts that you will learn by taking the DON CIO's Command KM Course.

### Tapping into Available Knowledge

The complexities of work and decision making, as well as the amount of available information, have increased substantially. "Doing more with less" is a driving force in many organizations. Also, in many naval commands, team members are not collocated; reach-back from the field and between work groups is vital to performance. Most likely, a lot of your com-



Figure 1

# THE DON CIO KM FRAMEWORK

Mission Priorities	1	People	Building a sharing culture, gaining leadership commitment, building relationships and communicating
	2	Process	<b>KM PROCESSES:</b> <b>Tacit:</b> making people-to-people connections <b>Explicit:</b> capturing, mapping, analyzing, disseminating <b>COMMAND PROCESSES:</b> Knowledge flows to the right processes at the right time to make decisions or accomplish tasks
	3	Content	<b>Tacit:</b> people knowledge, expertise <b>Explicit:</b> content, records, value, relevant, current, accurate
	4	Learning	<b>LEARNING:</b> <b>Knowledge transfer:</b> learning what we need to know and “gaining” knowledge we don’t have Not reinventing the wheel, storytelling, listening, creating, growing, experimenting, building context, establishing feedback loops, training
	5	Technology	<b>Tacit:</b> enabling, facilitating, empowering, promotes innovation

mand’s information remains untapped. The result is that your people often start from scratch and rebuild knowledge that already exists. Implementing KM practices can go a long way to remedying these situations.

Using the DON CIO KM Framework (Figure 1), start your efforts by aligning KM strategies to your command’s mission priorities and articulate how KM can solve a problem or remove barriers to success. Start with a small project that matters and build on its success.

Next, move to the people part of the process by building a culture of sharing. Leadership commitment is critical, but so is building strong relationships throughout the command and mechanisms for communicating the value of KM. A good tip here is to get the early adopters, stakeholders and “influencers” in your organization on board with your efforts. Be sure to sell the benefits of using KM but don’t overstate what it can do. Another good tip is to use simple, understandable terms to communicate. Use Navy language, or the language of your organization. For example, Tactical Training Group Pacific suggests that Navy strike group knowledge managers might use:

- ➔ Warfighting command and control (C2) instead of knowledge management;
- ➔ Warfare commanders and “bubbass” instead of communities of practice;
- ➔ Warfighting experience instead of tacit knowledge;

- ➔ SOPs, Naval Air Training Operating Procedures Standardization (NATOPS), and the like, instead of explicit knowledge; and
- ➔ Commander’s intent instead of strategic vision.

Many have said, “It’s all about the processes.” That’s certainly true when it comes to implementing KM. There are processes that focus on KM procedures such as maintaining a list of command SMEs to facilitate connecting to people to share tacit knowledge. KM is also important to other command processes by ensuring knowledge flows to the right processes at the right time.

Implementing KM projects without proper attention to relevant content will fail or at best be ignored. That seems obvious, but numerous KM projects floundered because content was not sufficiently planned. In each case, it was assumed that users would automatically start providing content — they didn’t. Even with content properly planned from the outset, continued management is critical; content must be kept current, relevant and accurate. The first time it is not, is the last time a user will look for it. This isn’t just true of explicit content in a repository. For instance, it also applies to yellow pages used to link people to a SME for tacit knowledge sharing.

Learning is about acquiring the knowledge and information needed to make a decision or complete a task. Just as there are

many aspects to KM, there are many ways to learn and many ways to convey learning. This concept also applies to those working on KM projects. Project leaders should continuously learn about their command's KM environment by establishing feedback loops and listening to what people are saying about their efforts.

Notice that technology is the final spoke in the framework. Though technology allows us to do remarkable things, for most KM projects, it should be an enabler rather than a focus. Also, when considering technology, first consider using what is readily at hand — and already paid for — even if it doesn't have every "bell and whistle."

Simply put, KM's goal is to capture and quickly and easily provide (through push and/or pull) actionable information to users (people, processes and systems) when they need it to make a decision or complete an action. KM can create time because personnel aren't spending valuable time searching for and managing information — instead they can be empowered by knowledge, inspired to excel, exceeding expectations and innovating ways to do the business of your organization better.

### **KM Resources:**

**DON CIO Command KM Course** – conducted several times a year in San Diego and Norfolk. For more information, contact Jim Knox, DON CIO director of information and knowledge management, at jim.knox@navy.mil. Special assists may be available upon request. Mr. Knox also conducts KM sessions at the semiannual DON IT Conferences held in San Diego and Norfolk.

**Afloat Knowledge Management Course (AKMC)** – conducted by Tactical Training Group Pacific in San Diego each fall and in Norfolk each spring. The objective of AKMC is to provide an understanding of KM fundamental theory and to give context to KM in the military environment. The course provides an operational KM focus on people, processes, organizations, and technology's supporting role within the constraints of afloat operations. For more information, contact TTGP at ttgp\_ncwsyndicate@navy.mil.

**APQC** – a research organization that specializes in metrics, process improvement, knowledge management, measurement, best practices and benchmarking. The DON CIO has funded membership for DON personnel. Register by using your navy.mil or usmc.mil email address at www.apqc.org.

**DON KM Quarterdeck** – contains the DON CIO KM course material. Users are able to share KM success stories by going to <https://www.intelink.gov/sites/donkmquarterdeck>. Permission is required for access; register by going to: <https://www.intelink.gov/passport/register.flow?execution=e1s1>. Access via the Navy Marine Corps Intranet is required unless you have Department of National Intelligence-Unclassified (DNI-U) Remote Access: <http://ra.intelink.gov>.

**JIM KNOX** is the DON CIO director of information and knowledge management.

**SHARON ANDERSON**, CHIPS senior editor, contributed to this article.

## KM PROGRAM CHECKLIST

- Before starting a KM effort, identify the "So What" or "Why" your organization needs to implement KM. A good place to look is your command's priorities (strategic plan, vision, commander's intent, fiscal year goals, etc.) then align your KM efforts to those priorities.
- Identify what the command is attempting to accomplish and the barriers to success.
- Listen for challenges – attend meetings and listen for the pressure points. Brainstorm how the KM team can help solve those challenges.
  - Actively listen, observe and ask questions of whomever you can.
- Words matter – define KM in a meaningful way for your command:
  - Avoid using KM terms when normal or operational terms will do.
  - Describe KM in terms that will resonate with the workforce.
- The KM plan should have specific outcomes that:
  - Improve organizational performance; and
  - Are accepted/embraced by your organization's leadership.
- Avoid overstating what KM can do.
- Engage the influencers – the boss and leaders below the boss.
  - Who are people of influence in your organization? How do you bring them along in your project?
- Might start with a "quick-win" – if it is about something that matters!
- Demonstrate the "What's in it for me" (WIIFM) of KM for all levels of the command.
- Monitor, assess and improve KM efforts regularly:
  - Take a look at what you're doing. What's worked? What hasn't worked?



# Cloud Computing

COMING SOON

By Heather Rutherford

**T**HE DEPARTMENT OF THE NAVY will soon be embracing cloud computing technology, which offers more efficient and accessible methods to obtain information.

The National Institute of Standards and Technology (NIST) 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."

On July 10, 2012, the Department of Defense (DoD) announced a new cloud computing strategy that is designed to "create a more agile, secure, and cost effective service environment that can rapidly respond to changing mission needs," according to a Defense Information Systems Agency (DISA) press release.

DoD named DISA the enterprise cloud service broker. In a memo from June 26, 2012, the DoD Chief Information Officer (CIO) said the agency is in charge of "making it easier, safer, and more productive to navigate, integrate, consume, extend and maintain cloud services, within the Department, from other Federal and commercial cloud service providers."

The DoD CIO Cloud Computing Strategy, included as an attachment to the memo, stated that the "adoption of and use of cloud computing will include reduced costs and

## FOR MORE INFORMATION

- [www.disa.mil/News/PressResources/2012/DISA-DOD-Enterprise-Cloud-Service-Broker](http://www.disa.mil/News/PressResources/2012/DISA-DOD-Enterprise-Cloud-Service-Broker)
- <http://dodcio.defense.gov/>
- [www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=3936](http://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=3936)

increased IT service delivery efficiencies, increased mission effectiveness, and enhanced cybersecurity."

The Department of the Navy is approaching cloud use in its current cost-saving data center consolidation and business IT transformation efforts. The DON is looking at all options when considering where data can be hosted and envisions a hybrid solution of commercial, private and community clouds to yield benefits, such as reduced manpower and improved security. This will ultimately lead to more efficient ways to process and access information. ●

**HEATHER RUTHERFORD** is the assistant editor of CHIPS magazine. She can be reached at [chips@navy.mil](mailto:chips@navy.mil).



**WE WANT  
YOU**  
TO SUBMIT YOUR GOOD IDEAS!

By Don Reiter and Sharon Anderson

The Department of the Navy seeks to save money by improving IT management, inserting IT or changing existing processes.

“ Everything is on the table” when it comes to ways to reduce the department’s IT costs and improve the efficiencies of its business systems and processes.

– DON CIO TERRY HALVORSEN

pated costs, benefits, effects on operations and risks. The BCA template also helps to ensure the best course of action is taken.

The DON CIO established the A-BCA template for stakeholders to submit ideas. However, it is not meant to replace the DON Enterprise IT Standard BCA template. The abbreviated version is meant to be a faster, more efficient start to a structured cost-savings conversation.

The purpose of using the A-BCA is to foster efficient and effective communications of cost-savings ideas to the DON CIO and other leadership, from all sources, including DON personnel, industry and academia, by providing a shorter and more condensed cost-savings focused format. The A-BCA focuses on the critical elements of a BCA, including a brief discussion of the problem statement; proposed scope; key assumptions, constraints and risks; costs, savings and other benefits; and operational impacts. Although it requires analysis, the A-BCA does not require the same level of analysis that the full BCA demands, but should still be based on facts, evidence and reasonable assumptions.

Examples of cost cutting ideas include proposals for reducing the costs and improving the efficiencies of the department’s cellular phone services; the IT acquisition process; commodity purchases for enterprise software licensing, hardware and IT services; and cyber/IT workforce training. To quote DON CIO Terry Halvorsen: “Everything is on the table” when it comes to ways to reduce the department’s IT costs and improve the efficiencies of its business systems and processes.

Sharing your cost-cutting suggestions presents an exciting opportunity to transform and modernize the department’s business IT assets and improve processes. Since the DON CIO published its request for ideas in July, interest has sparked across the department with three ideas already submitted.

Recommendations may be submitted using the abbreviated BCA template located at [www.doncio.navy.mil/Content/View.aspx?id=4056](http://www.doncio.navy.mil/Content/View.aspx?id=4056). Please send completed BCAs to Don Reiter, lead for cost metrics/savings, Office of the Department of the Navy Chief Information Officer, at [donald.reiter@navy.mil](mailto:donald.reiter@navy.mil). ●

**FOR MORE INFORMATION** about Department of the Navy IT efficiencies and cost-savings policies, visit the DON CIO website: [www.doncio.navy.mil/efficiencies](http://www.doncio.navy.mil/efficiencies).

**DON REITER** is the deputy director, Department of the Navy Enterprise Commercial IT Strategy and lead for Cost Metrics/Savings, in the office of the DON Chief Information Officer.

**SHARON ANDERSON** is the senior editor for CHIPS magazine.



Good people and good ideas have a way of rising to the top; so the Department of the Navy Chief Information Officer is asking stakeholders to come up with ways to improve the efficiency of the department’s information technology

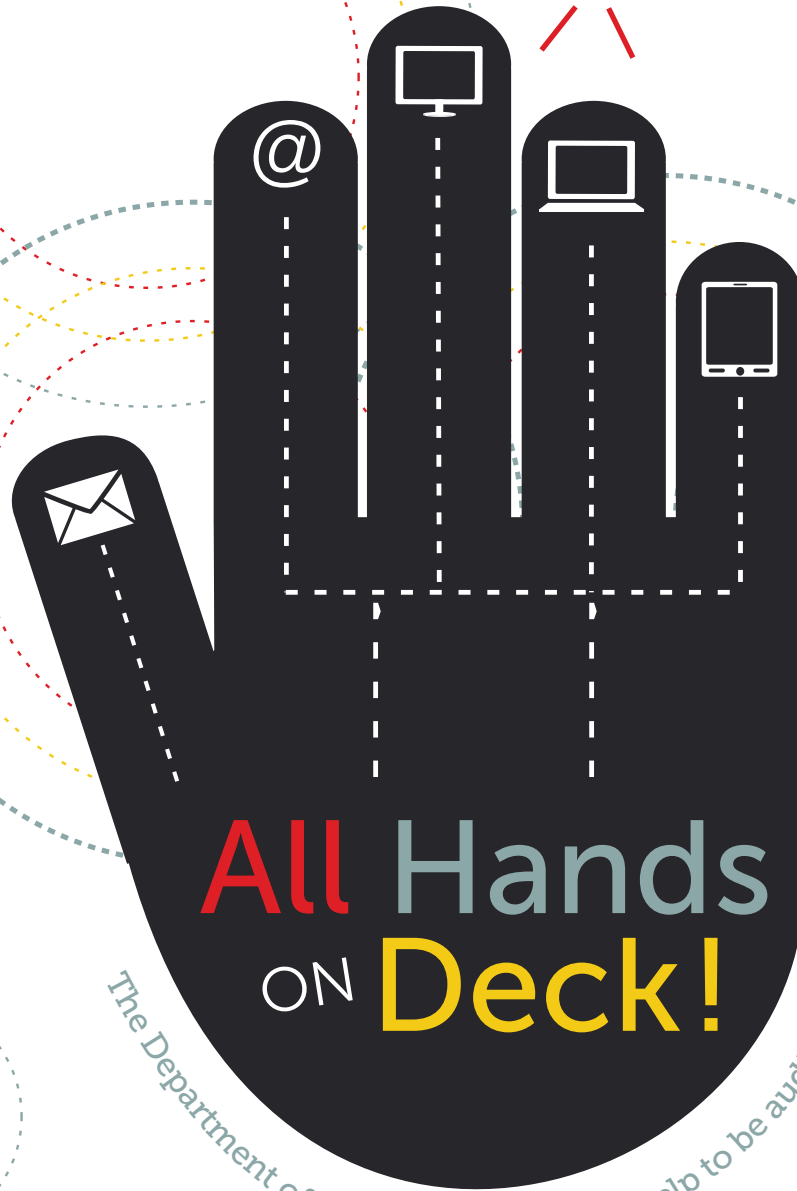
and cyberspace-related procurement and business processes using business case analyses (BCAs). To make this easier for all, the DON CIO has recently released a newer and simplified version of its business case analysis template — the abbreviated BCA (A-BCA).

The need to transform IT business processes is urgent. In 2010, Under Secretary of the Navy Robert O. Work directed the DON CIO to reduce the department’s IT bill by 25 percent over a five-year period. Business information technology is a logical area to achieve savings. As technology is always improving, the department can leverage these improvements in a strategic way that meets the needs of the DON. We need to ensure that our technology, policy and processes support efficient behavior and inform the DON’s decision making. Additionally, purchasers often did not take advantage of the volume discounting available through enterprise-wide contracts for software, hardware, IT services and telecommunications. As a result, the DON was not positioned to achieve its potential in savings.

Since 2010, the DON CIO has been aggressively leading efforts to achieve the \$2 billion-reduction target and improve efficiencies through several initiatives, including: data center consolidation, application rationalization, and the use of BCAs for all DON IT investments of \$1 million or more. Use of the BCA template is mandatory to ensure consistency. It facilitates comparisons of proposed alternatives and clearly defines anti-

By Sharon Anderson

ATTENTION!



# All Hands ON Deck!

The Department of the Navy needs your help to be audit-ready.

## What does it mean to be audit-ready?

Audit readiness is a state of being prepared at all times to demonstrate proper manual and automated processes and documentation of financial transactions through process controls, financial controls and information technology controls that are executed in accordance with policy and appropriate accounting standards.

The Department of the Navy (DON) is working to achieve full financial auditability by 2017 and be prepared for an

audit of the Statement of Budgetary Resources (SBR) by 2014. Everyone — every Sailor, every Marine, every civilian — across the department is responsible for meeting this goal. You may say that you are not in a position that executes a financial transaction, but you may be surprised to learn that entering your time and attendance, requesting leave or simply certifying an invoice for payment are all examples of financial transactions that an auditor would review to ensure proper controls are met.

A financial audit is an independent evaluation of whether an organization's financial statements are fairly presented and in accordance with appropriate accounting standards. The DON's annual budget of \$150 billion would place it near the top of the Fortune 500 list. All U.S. companies are required by law to regularly undergo a financial audit. The DON has not successfully completed a financial audit on several attempts.

One of the key challenges in the audit readiness effort is the difficulty in tracing the flow of transactions and individual data elements from initiation through reporting. Many DoD and DON systems, particularly older legacy feeder systems, were not designed to capture transactions at a level of detail that readily supports a financial statement audit. Additionally, newer enterprise resource planning (ERP) systems do not guarantee auditability. ERP systems may not fully support audit readiness or may not yet be fully operational at the time of audit.

Another common challenge is insufficient system process and data flow documentation. Documentation is often incomplete or does not reflect system updates, resulting in an inability to determine whether controls exist and/or are suitably designed. When system documentation is incomplete, inaccurate or unavailable, an auditor is unable to design or execute procedures to assess the operational effectiveness of system controls.

The Defense Department is the only major federal agency that cannot pass a financial audit. Now, more than ever, the DON must manage its money as tightly as it manages its operational mission. The Secretary of Defense has challenged the DON to achieve audit readiness with its SBR by the end of calendar year 2014.

Senior leadership across the departments of Defense and the Navy have made it clear that audit readiness is a top priority for all commands and personnel. As these leaders have repeatedly emphasized, improving the DON's financial processes and systems is a critical goal that is important to every member of every community within the DON — not just the department's comptrollers and budget offices. Everyone is expected to contribute to this goal.

Not only is it important to improve the DON's financial management to meet the Congressional mandate for audit readiness, but it is also crucial to make the DON a responsible steward of taxpayer dollars, to improve the efficiency and reliability of the DON's business, to provide accurate data for decision-makers, and to allow the DON to effectively execute its missions in an era of fiscal limitations.

The Office of the Assistant Secretary of the Navy (Financial Management and Comptroller) Office of Financial Operations (FMO) is leading the DON's efforts to comply with DoD's mandate for audit-readiness. FMO, with the support of several other Navy organizations, has created the first DON audit readiness video. The video serves as an excellent standalone product or as a stage setter for follow-on audit readiness discussions and presentations. To access the video, go to the FMO website at [www.fmo.navy.mil/auditready](http://www.fmo.navy.mil/auditready).

## RESOURCES

- FMO Audit Readiness Information Center  
[www.fmo.navy.mil](http://www.fmo.navy.mil)

## ADDITIONAL READING

- Audit Ready – The Challenge  
[www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=4033](http://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=4033)
- Interview with Charles E. Cook III  
Principal Deputy Assistant Secretary Navy  
(Financial Management and Comptroller)  
[www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=4026](http://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=4026)

FMO's Audit Readiness Information Center located at [www.fmo.navy.mil](http://www.fmo.navy.mil) provides resources detailing how the DON is systematically working toward its audit-ready goal and how you and your command can contribute to these efforts.

### How can YOU support audit readiness in your day-to-day actions?

- Ensure your processes are standardized, well-documented, sustainable and support accountability;
- Verify your work steps and ensure transactions are fully documented, correct and available on demand;
- Identify issues that arise in transaction processing that may cause auditability related issues;
- Educate yourself with resources provided on the Audit Readiness Information Center website at [www.fmo.navy.mil](http://www.fmo.navy.mil); and
- Ensure the DON can maintain a constant state of audit readiness by having business processes that are sustainable, traceable and repeatable.

### Everyone Must Be Onboard

In a video message ([www.fmo.navy.mil/AuditReadiness/senior\\_leadership\\_memos.html](http://www.fmo.navy.mil/AuditReadiness/senior_leadership_memos.html)) regarding audit-readiness, Secretary of Defense Leon Panetta stressed the need to maintain military strength as the department is tightening its belt to reduce the defense budget by \$487 billion during a 10-year period. This means the DoD must become more efficient and effective in managing its resources, he said. In this regard, the secretary asked personnel to follow several precepts, including:

- Maintain complete and accurate records of financial transactions;
- Maintain complete and accurate inventories of assets and equipment; and
- Spend every dollar as if it were your own. Before you order supplies or equipment make sure it is truly necessary. ●

**SHARON ANDERSON** is the CHIPS senior editor. She may be reached at [chips@navy.mil](mailto:chips@navy.mil).

# Rear Adm. Jonathan White New Oceanographer of the Navy

By Robert Freeman with Heather Rutherford



Rear Adm. Jonathan White

**O**n Aug. 20, 2012, Rear Adm. Jonathan White assumed the title of "oceanographer of the U.S. Navy," replacing Rear Adm. David Titley who retired in July. Assigned to the Chief of Naval Operations staff, White is now head of the Oceanography, Space and Maritime Domain Awareness directorate (OPNAV N2N6E) under the Deputy Chief of Naval Operations for Information Dominance.

White also serves as head of the Navy's Positioning, Navigation and Timing directorate and he holds the title "navigator of the Navy." In addition, White is director of the Navy's Task Force on Climate Change, the naval deputy to the National Oceanic and Space Administration, and director of the Office of the Department of Defense Executive Agent for Maritime Domain Awareness.

"It's a great honor for me to lead this group of dedicated professionals," White said. "The various branches of N2N6E collectively work to ensure enhanced knowledge of the physical environment through a wide array of sensing capabilities and data fusion.

"This knowledge helps support safe and effective operations forward and provides warfighting advantage through decision superiority. I like to say that it gives us home field advantage ... at the away games."

White is the 20th person to hold the oceanographer of the Navy title since its inception in 1960. The U.S. Navy has a vital operational oceanography program, providing naval, joint and coalition warfighters understanding of the maritime environment to ensure safety and readiness for unencumbered

global operations, as well as timing and reference information to support precision navigation, maneuvering and targeting.

As the senior oceanographer in the Navy, White advises naval leadership on all issues related to oceanography, meteorology, hydrography, climatology, precise time, and geospatial and celestial referencing. His staff provides policy guidance and resourcing for the operational oceanography program, and he serves as the senior policy adviser for issues relating to national ocean policy and governance.

As navigator of the Navy, White provides policy and requirements guidance to ensure naval forces have state-of-the-practice positioning, navigation and timing capabilities for accurate operational maneuver and optimum weapons employment, enabling a competitive advantage across the full spectrum of naval and joint warfare.

White serves as the director of Task Force Climate Change, which addresses the implications of climate change for naval operations and informs policy, strategy and investment plans.

According to the DON Environment and Climate Change website, factors affecting naval force structure and operations include:

- ➔ The changing Arctic;
- ➔ The potential impact of sea level rise on installations and plans;
- ➔ Changing storm patterns and severity;
- ➔ Water and resource challenges;

- ➔ Stress on vulnerable nation states; and
- ➔ Increased humanitarian assistance and disaster response.

The ultimate goal of TFCC is to ensure the Navy is ready and capable to meet all mission requirements in the 21st century.

As director of the N2N6E Space branch, White oversees the Navy's space-related policies, programs, requirements, investments, and resourcing. The Navy's interests in space include satellite systems that enable global, networked communications; intelligence, surveillance and reconnaissance; positioning, navigation and timing; early missile warning; and environmental sensing capabilities.

White also assumed the oversight responsibility for the Department of Defense and Navy's maritime domain awareness initiatives as director. Under the delegated authority of the Secretary of the Navy, White leads a dual-hatted organization focused on the effective understanding of anything associated with the global maritime domain that could impact the security, safety, economy or environment of the United States. ●

**BOB FREEMAN**, Office of the Oceanographer of the Navy. Freeman can be reached at [robert.freeman@navy.mil](mailto:robert.freeman@navy.mil).  
**HEATHER RUTHERFORD** is the assistant editor of CHIPS magazine.



PACIFIC OCEAN (June 30, 2012) 55 feet remain visible after the crew of the Floating Instrument Platform, or FLIP, partially flood the ballast tanks causing the vessel to turn stern first into the ocean. The 355-foot research vessel, owned by the Office of Naval Research and operated by the Marine Physical Laboratory at Scripps Institution of Oceanography at University of California, conducts investigations in a number of fields, including acoustics, oceanography, meteorology and marine mammal observation. U.S. Navy photo by John F. Williams.



NUUK, Greenland (Oct. 9, 2010) Secretary of the Navy the Honorable Ray Mabus and Prime Minister of Greenland Jakob Edvard Kuupik Kleist, foreground, speak aboard a search and rescue patrol boat off the coast of Nuuk, Greenland. Mabus concluded a day-two day trip to Greenland, meeting with leaders and scientists to discuss the importance of regional security and the environmental impacts of climate change. U.S. Navy photo by Mass Communication Specialist 2nd Class Kevin S. O'Brien.

ARABIAN SEA (Feb. 9, 2012) Meteorology and oceanography officers Lt. Cmdr. Shane Stoughton, left, Lt. Cmdr. Ana Tempone, along with Cmdr. Dan Van Meter, a strike operations officer, assemble a drifting buoy used to measure ocean currents before deploying it from the fantail of the Nimitz-class aircraft carrier USS Carl Vinson (CVN 70). Carl Vinson and Carrier Air Wing (CVW) 17 are deployed to the U.S. 5th Fleet area of responsibility. U.S. Navy photo by Mass Communication Specialist 2nd Class James R. Evans.



**FOR MORE INFORMATION**  
 Rear Adm. White's Biography  
[www.navy.mil/](http://www.navy.mil/)  
 U.S. Navy  
 Energy, Environment and Climate Change  
<http://greenfleet.dodlive.mil/climate-change>

# The Defense Language Institute Foreign Language Center

*Courses in 23 languages and two dialects offered to service members and more*

*By Mass Communication Specialist 1st Class (SW/AW) Nathan L. Guimont*

The Defense Language Institute Foreign Language Center (<http://www.dliflc.edu/index.html>) has awarded 7,762 Associate of Arts (AA) degrees since the inception of the program in 2002, to active duty, reserve service members, foreign military students and civilian personnel working in the federal government and various law enforcement agencies who complete the basic foreign language program at the Institute.

The DLIFLC is regarded as one of the finest schools for foreign language instruction in the nation. As part of the Army Training and Doctrine Command, the Institute provides resident instruction at the Presidio of Monterey in 23 languages and two dialects, five days a week, seven hours per day, with two to three hours of homework each night. Courses last between 26 and 64 weeks, depending on the difficulty of the language.

In December 2001, Congress chartered and authorized DLIFLC to award foreign language AA degrees. According to the state of California, an institution that grants degrees must be regionally accredited. In January 2002, the Accrediting Commission for Community and Junior Colleges (ACCJC) of the Western Association of Schools and Colleges gave DLIFLC degree granting status. DLIFLC awarded its first DLIFLC foreign language AA degree in May 2002. In July 2012, the ACCJC reaccredited the institute for another six years.

As the Department of Defense's premier foreign language educator, DLIFLC is vital to the nation's defense. DLIFLC's dedicated faculty and staff carry out a critical mission providing outstanding culturally based language education to military language professionals while simultaneously supporting the general purpose force with predeployment materials in more

than 40 languages. The degree program is specific to a student's language of study and is designed to allow students to complete general education credits after completing the basic foreign language program at the Institute.

Dr. Robert Savukinas, associate dean of Academic Affairs and Accreditation for DLIFLC, said completion of the basic DLIFLC language course is defined as 45 credits followed by a successful Defense Language Proficiency Test (DLPT) score, as set forth by the government Interagency Language Roundtable (ILR), with proficiency level scores of 2 in listening, 2 in reading, and a 1+ in speaking.

A level 2 proficiency in listening is defined as limited working proficiency with sufficient comprehension to understand conversations of routine social demands and limited job requirements.

A level 2 proficiency in reading is defined as a limited working proficiency with sufficient comprehension to read simple, authentic written material in a form equivalent to usual printing or typescript on subjects within a familiar context.

A level 1+ proficiency in speaking is an elementary proficiency to initiate and maintain predictable face-to-face conversations and satisfy limited social demands.

"In addition to these [DLIFLC] requirements, a student must be able to transfer 18 credits from courses taken at an accredited college, producing a total of 63 credits for a DLIFLC [foreign] language AA degree," Savukinas said. "These courses include math, English, natural/physical science, social science, technology and physical education. Along with the DLIFLC program, DLPT scores, and 18 credits, students will be awarded a DLIFLC language AA degree."

Students can meet the DLIFLC foreign language AA degree requirement transfer

credit by successfully completing a College-Level Examination Program (CLEP – <http://clep.collegeboard.org>) test, or Defense Activity for Non-Traditional Education Support (DANTES – [www.dantes.doded.mil/DANTES\\_Homepage.html](http://www.dantes.doded.mil/DANTES_Homepage.html)) test, or by attending a local college class while they are at DLIFLC, or attending a regionally accredited college after graduating from a basic foreign language program.

Typically, one out of every three service members that graduate from DLIFLC, whether they are from the Army, Air Force, Navy or Marines, meets the DLIFLC foreign language AA degree requirements — either with prior college, a CLEP or DANTES test, or an extra college class while attending the institute.

The remaining two service members will receive the DLIFLC foreign language AA degree at their next duty assignment, after completing a distance learning class, or by going to their local education office and enrolling in a foreign language course at a regionally accredited college that offers the program.

"The AA degree office realizes that the student's first priority is to learn a foreign language while at DLIFLC," Savukinas said. "The AA degree is a voluntary program, and we don't want to interfere with the teaching and learning in the classroom."

"It wouldn't be surprising to me to see some of these students take their DLIFLC language AA degree and go on to earn their BA. The credits that are earned at DLIFLC are transferrable, because we are regionally accredited and that's the first standard for transferring credits from one college to another," Savukinas said.

Savukinas explained the benefits of the DLIFLC language AA degree.

"The DLIFLC language AA degree is an added benefit to a military student's education, and possibly their career," he said. "Some military services give

promotion points to service members who earn a degree. When a student starts using their GI Bill, it saves the government money. By having a DLIFLC language AA degree, this also makes the student more competitive when they apply to a four-year institution.”

When comparing the foreign language course at DLIFLC to a typical four-year college degree model, one should consider that a Bachelor of Arts degree at many colleges mathematically credits classroom time and nothing else. A typical BA degree encompasses 120 credits earned by passing various classes. At DLIFLC, a student learning Arabic receives 1,890 hours of classroom instruction, which equates to 118 credits earned of just foreign language training in 63 weeks.

“The rigor of what occurs in the classroom here [DLIFLC] is intense, six hours a day, five days a week of instruction, plus homework daily,” Savukinas said.

“It’s an immersion environment where target language is encouraged with smaller teacher-student ratios. With regard to proficiency, our students generally spend a lot more time in the classroom in the foreign language discipline than I would argue most, if not all, AA and possibly BA degree granting institutions.”

The AA degree office at DLIFLC is staffed with two full-time advisers who focus on the program requirements and how DLIFLC graduates can meet degree requirements. The staff advisers are experts at interpreting course descriptions and transcripts, conferring the degree, and counseling students about which courses are, and which ones are not, creditable to the degree program.

Current and past DLIFLC students can get more information by going to the DLIFLC website: [www.dliflc.edu](http://www.dliflc.edu); under the Services tab, click on the AA degree link.

Approximately 10 percent of graduating students earn the DLIFLC language AA degree; Arabic, Chinese-Mandarin and Spanish are the top three languages in which students earn



MONTEREY, Calif. (Nov. 3, 2011) Cryptologic Technician (Interpretive) 1st Class Rachel Cleaver prepares Spanish students for a multimedia-based, interactive grammar lesson at the Defense Language Institute Foreign Language Center. U.S. Navy photo by MCS1 Nathan L. Guimont.

MONTEREY, Calif. (March 12, 2012) Seamen Cortese, right, Cottingham and Beeson, students at the Middle Eastern School II studying the Basic Arabic Course, perform a ‘peer correcting’ of fellow students homework assignments. U.S. Navy photo by MCS1 Nathan L. Guimont.



## Center for Information Dominance

The Center for Information Dominance is the Navy’s learning center that leads, manages and delivers Navy and joint force training in information operations, information warfare, information technology, cryptology and intelligence. The CID domain comprises nearly 1,300 military, civilian and contracted personnel. Additionally, CID oversees the development and administration of more than 223 courses at four commands, two detachments and 16 learning sites throughout the United States and in Japan. CID also provides training for approximately 24,000 members of the U.S. Armed Services and Allied Forces each year.

degrees. Since 2002, the average number of DLIFLC language AA degrees awarded annually to Sailors is 144. The total DLIFLC language AA degrees awarded to DLIFLC graduated Sailors since 2002 is 1,581. ●

**MCS1 (SW/AW) NATHAN L. GUIMONT** is with the Center for Information Dominance Unit Monterey public affairs office.

**FOR MORE INFORMATION**  
DEFENSE LANGUAGE INSTITUTE FOREIGN  
LANGUAGE CENTER: [WWW.DLIFLC.EDU](http://WWW.DLIFLC.EDU)

CENTER FOR INFORMATION DOMINANCE:  
[WWW.NAVY.MIL/LOCAL/CORRY/](http://WWW.NAVY.MIL/LOCAL/CORRY/)

**Now hear this:**

**NAVY**

**311**  **is at  
your service!**

**NAVY 311 is your gateway to service desks for everything Navy.**

**Got a question? Get an answer.** NAVY 311 is your single point of entry to access help desk support across the Navy—and no topic is off limits. Ask NAVY 311 about systems, equipment, training, facilities, career, IT, medical, logistics, and more. Whether you're at sea, in port, on duty or liberty, NAVY 311 is available 24/7. So toss away that wheel book. NAVY 311 is all you and your family need to reach authorized Navy service providers worldwide.

**1-855-NAVY-311**

(1-855-628-9311)

**Web:** [www.Navy311.navy.mil](http://www.Navy311.navy.mil)

**Email:** [Navy311@navy.mil](mailto:Navy311@navy.mil)

**Text:** Type 'Navy311@navy.mil' into the TO line of text message



**NAVY 311.**  
**Your Navy. Your Needs.**

NAVY 311 is delivered by the Sea Warrior Program (PMW 240) within the Program Executive Office for Enterprise Information Systems (PEO EIS).

# NAVY 311: YOUR SINGLE ENTRY POINT FOR SERVICE AND SUPPORT

ASK ANY QUESTION, ABOUT ANY TOPIC, ANYTIME, FROM ANYWHERE

*By Sea Warrior Program Public Affairs*

**I**t was almost midnight in the Indian Ocean, and a storm was bearing down on the USS Enterprise (CVN 65); poor timing for the carrier to lose access to the classified Intelink website. An information systems technician (IT) 3rd class petty officer (IT3) called NAVY 311 to find an expert who could quickly troubleshoot the problem. The NAVY 311 call center representative immediately documented the issue and referred the IT3's request to the Regional Maintenance Center (RMC) and Intelink Services Management Center (ISMC) service desk. In less than an hour, the ISMC responded directly to the IT3 via SIPRNET and resolved the Intelink website access issue.

On the other side of the world, the son of a deceased Navy veteran urgently needed official U.S. Navy documentation to prevent a major financial crisis for his mother. Her home was pending foreclosure and sale within a week — unless official U.S. Navy documentation could verify that she was eligible for benefits. The son contacted NAVY 311 and his request was expedited to the Navy's Survivor Benefits and Entitlements Branch, which, in turn, produced the proper documentation. Foreclosure averted.

Thousands of stories like these characterize the power of NAVY 311. Simply stated, when in need of assistance, turn to NAVY 311. The NAVY 311 call center operation is a single entry point into hundreds of help desks, call centers, and support organizations across the Navy. Ask any question, about any topic, anytime, from anywhere.

The NAVY 311 capability is not a new service or program start, but rather a new name for the customer relationship management (CRM) component of the Navy's Distance Support (DS) capability, which was established in March 2007 by

the Chief of Naval Operations (CNO).

"Basically, NAVY 311 rebrands and simplifies the various service request methods under the Distance Support umbrella whereby Sailors can get help. Those methods were 1-877-41-TOUCH, the AnchorDesk website and the Global Distance Support Center (GDSC), which formed the core DS CRM effort," explained Cmdr. Cord Luby, assistant program manager for Distance Support. "With NAVY 311, Sailors need only remember one point of entry — via phone, email, Web, text, chat — to get on-demand non-tactical information assistance 24/7, classified or unclassified. And, the NAVY 311 call center is available to all U.S. Armed Forces members and their families, DoD civilians, contractors and the occasional inquisitive citizen."

Adopted by more than 300 major cities, "3-1-1" is becoming a universal moniker for citizens to get non-emergency help. Baltimore, Chicago, San Francisco, New York, and other large municipalities, are using their centralized 3-1-1 call center operations to make city government services more accessible and transparent. Likewise, under the Sea Warrior Program (PMW 240), the Distance Support team is applying the principles of customer advocacy and knowledge management to provide the first-of-its-kind 3-1-1 solution focused on Navy needs.

## **FROM DISTANCE SUPPORT TO NAVY 311**

The customer relationship management component of Distance Support originated in 1999 through a collaborative agreement between Naval Sea Systems Command (NAVSEA), Naval Supply Systems Command (NAVSUP), Space and Naval Warfare Systems Command (SPAWAR) and the fleet commanders to provide a better interface for the

fleet into the shore support infrastructure. This effort produced the Global Distance Support Center, a hub for the shore-based sources of support (SoS) network for fleet logistics and technical assistance.

The requests for assistance quickly grew beyond the bounds of the hardware that systems commands provided to include other Echelon II command services such as personnel, Chaplain Care, medical, facilities, training and other needs.

"Early on, we quickly found ourselves at the tip of the spear when it came to helping Sailors figure out who to call for what," said Craig Brandenburg, NAVY 311 director. "By removing the burden from the Sailor trying to navigate the shore infrastructure, we connect their problem to the appropriate service provider. What Distance Support, and now NAVY 311, has become over time is a coordinated and collaborative network of responsive support to the fleet that spans the entire shore infrastructure and the provider enterprise."

Significant about NAVY 311 is the federated approach for providing service through the network of support providers. A helpful analogy is to compare NAVY 311 to a health maintenance organization (HMO). Although the type of organizational structure, independent specialty and membership vary across an HMO network, all share the collective goal of providing comprehensive care. The kinds of expertise and delivery systems vary across an HMO, but the providers agree to standardize provisions making available the care, facilities and services the customer base requires.

NAVY 311 and the support provider network operate in a similar fashion. A Sailor may submit a service request to the NAVY 311 call center via any NAVY 311 channel. Or, a Sailor may directly

contact one of the Navy's independent help desks or contact centers (e.g., 1-800-U-ASK-NPC in Millington, Tenn.) for support. Either way, the Sailor's request is processed following mandated SoS business rules; each support request is documented, processed within a prescribed response time, and accessible via the shared CRM data environment. The end result is the same: Sailor problem resolution with the transactional information captured for business intelligence. All participants of the SoS network are focused on serving Sailors and customers while maximizing business efficiency.

## THE EMERGING BUSINESS VALUE OF NAVY 311

As the NAVY 311 CRM solution continues to evolve, opportunities are evident to use the vast amount of collected service request data for better management decisions.

Currently, NAVY 311 technologies and processes integrate data from various transactional support systems across the Navy to give fleet customers and program offices a broader view of recurring system issues. There are three NAVY 311 call center hubs focused on various areas of support: Norfolk, New Orleans and San Diego. The shared data environment houses more than 6 million support request records.

"Today, NAVY 311 metrics reveal that we [support providers] are very good at being reactive and responsive. We are focused on decreasing both the find time and fix time when it comes to getting Sailors what they need. It's very exciting; the next step is to help the Navy business managers and stakeholders with the use of robust data analytics. Ultimately, NAVY 311 should help forestall issue occurrences, save money and improve readiness. The good news is the CRM data and volume of tickets amassed over the past decade has evolved in size and scope. We are poised to start using more sophisticated business analytics on the CRM data," said Laura Knight, program manager for the Sea Warrior Program (PMW 240).

The Surface Warfare Enterprise



An electronics technician 3rd class (ET3) from the USS Mahan (DDG 72) identifies two separate circuit card assembly (CCA) faults. The ship's force replaces the CCAs with onboard maintenance assistance modules (MAMs), yet both CCAs continue to fail, and the ship's force is unable to identify the cause. Via email, the ET3 requests support from NAVY 311, who documents the issue, records customer and problem data and assigns a service request to Norfolk Ship Support Activity (NSSA) Detachment Naples, Italy. With NSSA Det Naples' assistance, the ship's force of the USS Mahan determines that the SA-2112 secure voice switch has a faulty power supply and orders a replacement unit.

(SWE) has used data analysis to evaluate all tech assists for recurring maintenance problems to provide type commanders with insight into who repeatedly requires support.

In the training and education area, course curriculum managers revised training curricula to address fleet trends and highlight ongoing areas that need attention.

NAVY 311 is an invaluable tool. It quickly brings a Sailor and other customer issues to the experts who can help solve them. And by mining NAVY 311 data, engineers, acquisition managers and resource sponsors can more proactively anticipate problems and cost effectively respond to them.

*Isn't it time you used NAVY 311?* ●

### Contacting Navy 311

PHONE 1-855-NAVY311 (1-855-628-9311) Toll free

DSN 510-NAVY311 (510-628-9311)

EMAIL Navy311@navy.mil (unclassified); Navy311@navy.smil.mil (classified)

WEB www.Navy311.navy.mil (unclassified); www.Navy311.navy.smil.mil (classified)

TEXT type Navy311@navy.mil into the TO line of text message

CHAT via Navy311 website

PLAD NAVY THREE ONE ONE NORFOLK VA

### About the Sea Warrior Program

The Sea Warrior Program (PMW 240) manages a complex portfolio of information technology (IT) systems to recruit, train, pay, promote, move, retire, and support Navy personnel and deliver Distance Support IT to the fleet. The PMW 240 Program is part of the Navy Program Executive Office for Enterprise Information Systems (PEO-EIS), which develops, acquires and deploys seamless enterprise-wide IT systems with full lifecycle support for the warfighter and business enterprise. For more information, please contact the PMW 240 Public Affairs Office at 703-604-5400 or PMW240\_PAO@navy.mil.

# Interoperability Leads to "Peace"

## Partnership for Peace nations work together to build cooperation

By Heather Rutherford

Once a year, Combined Endeavor, the largest security co-operation and military exercise in the world, brings together 1,400 communications professionals from about 40 NATO and Partnership for Peace (PfP) countries and international organizations with the intent to explore and resolve multinational tactics, techniques and procedures and improve interoperability between nations. This year, the event took place at the U.S. Army's Joint Multinational Training Command in Grafenwoehr, Germany, and remote sites across Europe in September.

The PfP is a program of practical bilateral cooperation between individual Euro-Atlantic partner countries and NATO. It allows partners to build an individual relationship with NATO, choosing their own priorities for cooperation. Based on a commitment to the democratic principles that underpin the NATO alliance, the purpose of Partnership for Peace is to increase stability, diminish threats to peace and build strengthened security relationships between individual Euro-Atlantic partners and NATO, as well as among partner countries.

PfP participation in Combined Endeavor began in 1995 with 10 nations and about 150 participants. Back then, the technological focus was on high frequency or single-channel radios and hard-wired voice telephone circuit switching. In a 2007 interview with CHIPS, Army Lt. Col. James Pugh, then the director of Combined Endeavor, said: "It was like taking a square plug and putting it in a round hole simply trying to make the systems interoperate. It was 'Can you hear me now?' type testing."

Until last year's Combined Endeavor exercise, the focus was on an individual nation's ability to link to and communicate with another nation's system. While this type of testing proved the technology was operational, it did not address the "flow" of information. During Combined Endeavor 2011, assessments of critical information exchanges were made.

"Now, we can look at an order given by a commander at the operational level of command, and have the assessors follow that information through several different countries and different echelons of command to see if the information made its way to the foot soldier — timely and securely," said Army Capt. Kelvin Scott, U.S. European Command public affairs action officer for CE12.

A new feature of this year's Combined Endeavor is the ability for nations to link to an operations center from a home station, allowing those taking part in CE from their home countries to leave a "larger footprint" in the exercise, while reducing cost and increasing overall participation.

Interoperability is the key theme for the Combined Endeavor exercise. Since its inception, more than 16,500 interoperability test results have been recorded. Additionally, an Interoperability



GRAFENWOEHR, Germany (Sept. 11, 2012) Flags sit in front of each country's representative during Combined Endeavor 2012 at U.S. Army Joint Multinational Training Command. CE is a multinational command, control, communications and computer systems exercise designed to build and enhance communications and network interoperability between 41 nations and international organizations. Photo by U.S. Air Force Tech. Sgt. Araceli Alarcon.

Guide is developed at the end of each exercise. According to the CE website, the Interoperability Guide "takes the guesswork out of deploying multinational C4 networks and has been used extensively in current operations and crises, including Operations Enduring Freedom and Iraqi Freedom, International Security Assistance Forces (ISAF), NATO Kosovo Force (KFOR), and U.N. peacekeeping and humanitarian missions."

On a personal level, Combined Endeavor creates an environment in which the participants can achieve an understanding of other cultures thanks to the multinational representation. As Pugh pointed out, "When you get so many participants from so many nations together talking about a common issue, it lowers the barriers between them." ●

**HEATHER RUTHERFORD** is the assistant editor of CHIPS magazine. She can be reached at [chips@navy.mil](mailto:chips@navy.mil).

#### U.S. European Command

[www.eucom.mil/combined-endeavor](http://www.eucom.mil/combined-endeavor)

[www.eucom.mil/key-activities/partnership-programs/partnership-for-peace](http://www.eucom.mil/key-activities/partnership-programs/partnership-for-peace)

<https://www.facebook.com/EUCOM>

#### CHIPS

[www.doncio.navy.mil/chips/ArticleDetails.aspx?id=2907](http://www.doncio.navy.mil/chips/ArticleDetails.aspx?id=2907)

#### Partnership for Peace

[www.nato.int/cps/en/natolive/topics\\_50349.htm](http://www.nato.int/cps/en/natolive/topics_50349.htm)



WHICH

# PAPER SHREDDER



SHOULD I USE?

BY STEVE MUCK AND STEVE DAUGHETY



"DISPOSAL METHODS ARE CONSIDERED ADEQUATE IF THE RECORDS ARE RENDERED UNRECOGNIZABLE OR BEYOND RECONSTRUCTION."

The Department of the Navy Chief Information Officer (DON CIO) Privacy Office receives frequent inquiries regarding paper shredding as a means of destroying unclassified documents containing personally identifiable information (PII). Some commonly asked questions include:

- Which shredder should I purchase?
- Should I use a straight cut or cross cut shredder?
- What are the DON policy requirements?
- How small is small enough with regard to shredder residue?
- Where can I find a list of approved shredders?
- Can I use a shredder service?

Paragraph 8.b. (1) of Secretary of the Navy Instruction (SECNAVINST) 5211.5E, Department of the Navy Privacy Program, states:

"Disposal methods are considered adequate if the records are rendered unrecognizable or beyond reconstruction (e.g., tearing, burning, melting, chemical decomposition, burying, pulping, pulverizing, shredding, or mutilation)."

The key words are: "rendered unrecognizable or beyond reconstruction."

While there is no DON policy specifying the type of shredder to use, it is highly recommended and considered a best practice to always use a cross cut shredder. There have been cases involving straight cut shredders where the resulting paper strips could be pieced together to reconstruct privacy sensitive information. In one case, the straight cut shredder residue corresponded to the actual rows of a spreadsheet. As a result, none of the PII had been destroyed.

DON policy does not address shredder residue size. As a best practice, refer to the National Institute of Standards and Technology (NIST) Special Publication 800-88, "Guidelines for Media Sanitization: Recommendations of the National Institute of Standards and Technology," issued September 2006, which states:

"Destroy paper using cross cut shredders which produce particles that are 1 x 5 millimeters in size (reference devices on the NSA paper Shredder EPL), or to pulverize/disintegrate

paper materials using disintegrator devices equipped with 3/32-inch security screen (reference NSA Disintegrator EPL)."

The National Security Agency (NSA) Evaluated Products Lists (EPL) for shredders can be found at [www.nsa.gov/ia/\\_files/government/MDG/NSA\\_CSS-EPL-02-01-Z.pdf](http://www.nsa.gov/ia/_files/government/MDG/NSA_CSS-EPL-02-01-Z.pdf).

An alternative to purchasing a shredder is to contract with a General Services Administration (GSA) approved shredder service. With increased public awareness regarding the threat of identity fraud, availability and use of shredder services continue to increase. Benefits of using a shredder service include:

- Shredder services decrease labor hours and physical space disposal requirements;
- Mobile services allow documents to be shredded on-site or to be taken away to be destroyed;
- Certificates of destruction are issued to verify disposal;
- Bulk disposal is extremely efficient; and
- GSA approved shredder services are considered secure and in compliance with DON policy, and NIST and NSA guidelines.

While shredding is arguably the safest means of disposal, the use of burn bags remains a viable option. Regardless of the method of destruction, the creation of documents containing sensitive personal information should be avoided or minimized to the greatest extent possible.

Remember, the choice of a shredder must make paper documents containing PII unrecognizable or beyond reconstruction. DON policy does not specify specific particle size requirements, but a best practice states that particles should be 1 X 5 mm or smaller. Other disposal options are available and should be evaluated to determine what is best for the specific needs of your office.

Visit the DON CIO website at [www.doncio.navy.mil](http://www.doncio.navy.mil) and search "shredder" for information, tips and best practices. ●

**STEVE MUCK** is the Department of the Navy privacy lead.

**STEVE DAUGHETY** provides privacy policy support to the Department of the Navy.

# Afghanistan Automated Biometrics Identification System IPT First to Earn CMMI-SVC Gold

By Sarah Ingram and Tiffany Alexander

In January 2012, the Afghanistan Automated Biometrics Identification System (AABIS) integrated process team accomplished a milestone that no other IPT within Space and Naval Warfare Systems Center Atlantic had yet achieved. The AABIS IPT was the first to be awarded a Gold Level Capability Maturity Model Integration (CMMI) Process Excellence award for successfully implementing the CMMI for Services (CMMI-SVC) model.

The AABIS team decided to use CMMI-SVC as a framework for streamlining processes in support of biometrics identity management and training services. Biometrics identity management is a key enabler to achieving enhanced security through improved vetting processes. The ability to achieve identity superiority and implement biometric technologies to identify potential adversaries ultimately depends on the way biometric and identity information is collected, identified, analyzed, shared and stored.

Equally important is the capability to protect, manage and dominate identity information using biometric technologies to facilitate positive identification, and enhance security and support criminal prosecution.

The purpose of the AABIS program is to develop a biometrics capability for the Afghan government that can be self-sustained by the Afghanistan National Security Forces (ANSF) as a long-term solution. The biometrics capability is a commercial off-the-shelf biometrics system, which was procured and built to meet the specific needs of the ANSF. The integrated architecture for the AABIS program encompasses planning, budgeting, managing, surveying, designing, procuring, installing, researching, developing, testing, training and maintaining.

Upon program initiation, the team immediately implemented SSC Atlantic project management, monitoring and control processes to provide a sound foundation for follow-on efforts. Industry partners from Booz Allen Hamilton spearheaded process improvement initiatives resulting in unprecedented, back-to-back internal CMMI-SVC Silver and Gold Level appraisals, achieving SSC Atlantic's first CMMI-SVC Process Excellence Awards in May



Afghanistan Automated Biometrics Identification System IPT: Apryl Akery, Tiffany Alexander, Adolphus "JR" Burrow, Sarah Ingram, Andrew Osti and Sarah Sorenson.

2011 and January 2012.

The AABIS IPT began the internal CMMI assessment process by focusing on nine Silver Level process areas, including project planning, project monitoring and control, configuration management, requirements management, service delivery, risk management, process and product quality assurance, measurement and analysis, and supplier agreement management. In May 2011, the IPT successfully completed an internal Silver Level appraisal and received a Silver Level Process Excellence Award for CMMI-SVC.

IPT lead Adolphus "JR" Burrow supported the IPT moving forward with Gold Level implementation building upon sound Silver Level process areas. The team began to develop and implement processes to support the eight additional process areas including capacity and availability, incident resolution and prevention, service continuity, service system development, service system transition, strategic service management, integrated project management, and decision analysis and resolution. An internal data collection form was compiled, and throughout the data collection and mapping efforts, approximately 500 artifacts were collected and reviewed. The internal appraiser pointed to several AABIS activities that were highlighted as strengths and best practices. by the internal appraiser.

The AABIS Service Management Plan (SMP) Template is the first to be submitted to the SSC Atlantic process asset library, supporting CMMI-SVC artifacts. Additional template submissions include a service delivery log, document review matrix, requirements traceability matrix, threat analysis and response plan, and a call history log for tracking service incidents and reusable solutions. The IPT contributed these artifacts for use by others who are considering implementing the CMMI-SVC model. The internal appraiser noted that the response time for receiving updated artifacts was the fastest she had ever encountered and that the project assessment was one of the smoothest she had ever conducted. As a result, the AABIS IPT was the first SSC Atlantic project to be awarded Gold Level for successful implementation of the 17 prescribed CMMI-SVC process areas. AABIS continues to operate as a CMMI-SVC Maturity Level 3 compliant program in hopes of participating as a focus project in upcoming SSC Atlantic SCAMPI appraisals. ●

**FOR MORE INFORMATION**  
SPAWARSYSCEAN ATLANTIC  
[WWW.PUBLIC.NAVY.MIL/SPAWAR/ATLANTIC/](http://WWW.PUBLIC.NAVY.MIL/SPAWAR/ATLANTIC/)

# SSC Pacific First Navy Organization to Achieve CMMI-DEV v1.3 Maturity Level 3

By Ashley Nekoui and Sandy Van Densen

Space and Naval Warfare Systems Center (SSC) Pacific was formally rated at Level 3 of the Carnegie Mellon University (CMU) Software Engineering Institute's (SEI) Capability Maturity Model Integration (CMMI) for Development (DEV), becoming the first Navy organization to be successfully appraised against version 1.3 of the Standard CMMI Appraisal Method for Process Improvement (SCAMPI) A.

The Level 3 CMMI DEV rating was granted by the SEI as the result of a Standard CMMI Appraisal Method for Process Improvement (SCAMPI) Class A event, conducted May through June of this year.

CMMI is a process improvement approach that provides organizations with the essential elements of effective processes that ultimately improve their performance. An appraisal at Maturity Level 3 (ML3) indicates that SSC Pacific is performing at a level where processes are well-characterized, understood and are described in standards, procedures, tools and methods.

SSC Pacific's rating validates that the Organizational Set of Standard Processes (OSSP), the basis of ML3, is established, and the mechanisms in place to be improved over time. This allows the center to make systematic improvements to processes and assets in a repeatable manner, directly involving competency-aligned stakeholders.

The center's appraisal encompassed a comprehensive review of project management, engineering, engineering support, organizational and process management practices for 18 process areas implemented by sampled SSC Pacific integrated product teams and the organization itself. The appraisal team — composed of personnel from the Software Engineering Institute, U.S Air Force, SSC Atlantic and SSC Pacific — was presented with more than 12,000 pieces of evidence and interviewed 46 SSC Pacific staff members over a four-week period in the conduct of this detailed review against the CMMI industry-wide standard.

Personnel throughout the organization supported the three-year deploy-



A small sample of the SSC Pacific personnel who supported the center's goal for a rating as a CMMI-DEV v1.3 Maturity Level 3 organization.

Carmela Keeney, executive director of SSC Pacific; Richard Barbour, principal systems engineer at the Software Engineering Institute; and Capt. Joe Beel, commanding officer of SSC Pacific, sign the CMMI-DEV v1.3 Maturity Level 3 findings.



ment of this process and implementation of the OSSP and its infrastructure.

"This accomplishment is the result of many teams working towards the common goal of improving our system engineering and integration processes with the ultimate objective of reducing the cost of developing and maintaining our products, increasing quality, and reducing the rework of our products," said Carmela Keeney, SSC Pacific's executive director.

"Our CMMI-DEV ML3 rating demonstrates that SSC Pacific has an established, robust, and sustainable process infrastructure and OSSP in place to support information dominance and warrior decision-making, in alignment with the center's and SPAWAR's primary mission to the warfighter."

The results of SSC Pacific's rating can be verified at the SEI's Published Ap-

praisal Results System, located at <http://sas.sei.cmu.edu/pars/pars.aspx>, under United States Navy, Space and Naval Warfare Systems Center Pacific.

The Software Engineering Institute is a Department of Defense federally-funded research and development center operated by CMU. The SEI helps organizations make measured improvements in their engineering and management capabilities by providing technical leadership to advance the practice of engineering. ●

**FOR MORE INFORMATION**  
SOFTWARE ENGINEERING INSTITUTE  
[WWW.SEI.CMU.EDU/](http://WWW.SEI.CMU.EDU/)

SPAWARSCEN PACIFIC  
[WWW.PUBLIC.NAVY.MIL/SPAWAR/PACIFIC/](http://WWW.PUBLIC.NAVY.MIL/SPAWAR/PACIFIC/)

## LISA SEXAUER

Fitness, sports and deployed forces support program manager  
Commander, Navy Installations Command

The goal of the Navy fitness program is to create “Fitness for Life” for the entire Navy population, including active-duty Sailors, family members, retirees and Defense Department civilians. The fitness program maximizes the fun factor via a variety of health, nutrition and fitness resources. Participation is designed to be an enjoyable, as well as a healthy lifestyle choice through aquatic and intramural sports programs that enhance the readiness, retention and quality of life of the entire Navy family. MWR’s Deployed Forces Support Program boosts the quality of life for more than 180,000 Sailors and Marines at sea and forward-deployed Navy ground forces. Sports, recreational programs, physical fitness equipment, social activities (parties/picnics), tours, subsidies/rebates and gear locker checkout are just a few of the morale-enhancing opportunities offered.



Lisa Sexauer

Deployed Forces Support coordinators (DFSCs) are located at major fleet concentration areas throughout the world, and assist ships and forward-deployed ground forces with programming, financial management, recreation administration, procurement and property management. Coordinators are civilian recreation and fitness professionals exclusively dedicated to supporting the MWR needs of the fleet and forward-deployed ground forces.

The Navy’s MWR Civilian Afloat Program is comprised of afloat fitness (Fit Boss) and recreation specialists (Fun Boss) who serve aboard aircraft carriers, amphibious assault ships and tenders. Fit and Fun bosses work together in providing fitness and recreation programs for shipboard Sailors.

CHIPS asked Ms. Lisa Sexauer, fitness, sports and deployed forces support program manager for Commander, Navy Installations Command (CNIC), to talk about the Navy’s fitness program in August.

**Q:** You must have one of the best jobs in the Navy. Can you talk about what you do?

**A:** The beauty of my job is that it is different every day. Working from HQ means

everything from enlisting the expertise of our field to create large, impactful programs to soliciting and advocating for funding, thus ensuring our field [staff] have everything they need to serve their customers effectively. While sometimes initiatives take quite a while to roll out, the payoff in the end is worth it.

The fact is, this group of programs touches the lives of all those instrumental in operating the world’s greatest Navy, and it is powered by the world’s finest quality of life staff, at all levels. I am blown away by their dedication, work ethic and commitment. CNIC and Navy MWR is a collection of some of the finest people I know, and it has been amazing to work alongside each one of them. The opportunity to be involved in all of it is humbling and exciting!

**Q:** The Deployed Forces Support Program sounds like a great way to help service members reduce stress. Is there a method for measuring if the program is working? How do service members find out about the program?

**A:** Program measurement when it comes to quality of life programs is challenging. The most effective way to do so is to of-

fer it to a group of individuals and to not offer to another group, and I am not sure the Navy is willing to do that. In a recent survey conducted at the OSD level, the Navy’s Fitness and Deployed Forces Support programs rated the highest of all the services when it comes to customer satisfaction. Most importantly, most of our customers agree both programs enhance readiness and retention.

The challenge for Navy is delivering seamless programs from the shore to the sea. Essentially, we have to deliver programs at all shore installations and aboard the Navy’s operational platforms. After all, Sailors are deployed during times of war and peace on a regular basis. Thus, the demand for support is tremendous for Navy, and we manage to meet the needs in both environments with a lower cost per Sailor than any other service. That is an amazing accomplishment!

**Q:** Where did the idea of a fun boss and fit boss serving on ships come from? What do they do?

**A:** Our fun and fit bosses serve as recreation (fun) and fitness (fit) directors aboard our large decks (carriers and large deck amphibs). Essentially, they provide

all programming while at sea and coordinate all recreational activities during port visits. Fun bosses ensure that Sailors and all embarked units have opportunities for recreational stress relief. This may include anything from tournaments of all kinds, karaoke nights, talent shows, to coordinating trips and tours while in port. Fit bosses manage the fitness spaces aboard the ship, conduct a dynamic group exercise program, provide health and wellness training opportunities, support the physical readiness program and ensure all equipment is maintained in good working order.

Collectively, these two positions impact the lives of more than 100,000 Sailors and Marines. Since January 2012, over 4,700 recreational events were conducted with a total participation of 290,000. Additionally, there have been over 5,000 fitness events with a total participation of 66,899 and 3,500 preventative maintenance hours logged. This does not include those ships currently at sea as communication is difficult while they are underway. It blows my mind that all of this was accomplished by a staff of 35 people. I am not sure we could find a harder working group of people anywhere.

Afloat recreation positions began in the mid-80s and fit bosses were added in the late 1990s. I am not sure who inspired the stand up of the program as a whole but it was taken in by HQ in 2000 to better standardize the program. It has evolved into one of our flagship programs as it provides for service members at the tip of the spear, where they need it most.

**Q: Why did the Navy develop the Total Force Fitness concept and what does it include? Who was involved in the development and how do you get feedback from service members?**

**A:** TFF is a policy signed out by former Chairman of the Joint Chiefs, Adm. Mike Mullen. It is a comprehensive approach to wellness and is inclusive of much more than the physical aspects of wellness. Initially, Adm. Mullen challenged the

military's health and wellness experts to develop a total wellness program model, or in this case, [a] Total Force Fitness model (see Figure 1) that captures everything that impacts the readiness of an individual. The model includes spiritual, environmental, [and] physical among other wellness influencers. I think Adm. Mullen described it well in 2010:

*"As I see it, readiness is all about being capable of being able to accomplish something you are called to do. The combination of these components is a 'state of being.' From this state, individuals must be capable 'to accomplish something they are called to do,' not just pass a PRT test twice per year."*

In regard to feedback from the active duty population, I am not sure that they see all the components as a collective program. Rather, it is our responsibility as health and wellness professionals to ensure the Total Force has adequate resources in each of the TFF model areas to aid them in attaining and sustaining readiness at the highest level possible.

It is important to note that many programs and commands play a very important role in delivering programs and services that will complete the model for Navy. We are just one piece to the puzzle.

**Q: The Fitness, Sports and Deployed Forces Support website ([www.navyfitness.org/](http://www.navyfitness.org/)) is**

**a helpful resource in maintaining a healthy lifestyle. I like the exercise demos and recipes.**

**A:** The website provides information in each of our program areas, a one-stop shop, if you will. Sailors can gather information about the All Navy Sports program to include application procedures, upcoming sports participation opportunities and past results from All Armed Forces and CISM (multisport military world games Conseil International du Sport Militaire) events. Afloat commands can connect with their local DFS (Deployed Forces Support) offices to request support, gather recreation fund management best practices and download relevant policies.

On the fitness side, our over 40 active duty population can connect with one of our SHAPE (Senior Health Assessment Program Enterprise) program pilot sites and download the SHAPE monthly newsletter. Further, anyone can access the Navy Operational Fitness and Fueling Series (NOFFS) workouts via the virtual trainer or virtual meal builder.

For our field personnel, the website provides convenient access to the program standards and metrics (a vital program management tool) and all relevant policies, as well as our latest posters and marketing tools.

In the near future, along with the movement of the day, there will be a nutrition tip of the week which will

Figure 1. Total Force Fitness model that captures everything that impacts the readiness of an individual. The model includes spiritual, environmental and physical elements among other wellness influencers



broadcast via the Navy Fitness Facebook page (<http://www.facebook.com/pages/Navy-Fitness/368681091650>) as well. The NOFFS virtual meal builder will be further enhanced so users will be able to populate their daily meal plan with their favorite high octane foods and the healthy recipe section will continue to grow. Quite frankly, the potential is endless, and we have no intention to allow this website to become stagnant.

**Q: The CNO recently said that deployments will be longer due to an increased demand signal so will there be any changes to the Deployed Forces Support Program?**

**A:** We are currently working on a pilot program to aid Sailors, upon return from deployment, to focus their energies on positive outlets such as outdoor recreation opportunities. While it is very much in its infancy, we are excited about the possibilities. Our homeports are located in some of the most beautiful places in the world and offering up or enhancing existing opportunities for structured outdoor recreation for Sailors and their families is an exciting endeavor. We still have a lot of program development prior to a launch but there will be more information available at a later date.

Regarding the remainder of the DFS program, the last 10 years have allowed us to refine our services and programs. I feel we are very well prepared to meet deployed Sailors' needs in spite of any changes to the OPTEMPO (operational tempo). I think this applies to all MWR programs that service the fleet to include the Navy Motion Picture Service (<http://navymwr.org/mwrprgms/nmps1.htm>); Navy General Library Program (<http://www.facebook.com/USNavyGeneralLibraryProgram>); and Navy Entertainment ([http://navymwr.org/mwrprgms/entertainment/ent\\_home.htm](http://navymwr.org/mwrprgms/entertainment/ent_home.htm)).

The bottom line is our employees are dedicated and passionate about serving the Navy family and they have been stepping up to the plate for quite some time now. I know that won't change because that is just what we do.



ARABIAN SEA (March 1, 2011)-Brett Pelfrey, fit boss aboard the aircraft carrier USS Carl Vinson (CVN 70), and Airman Joel Metzger demonstrate an exercise to Sailors in the hangar bay during a tactical underway fitness program. The Carl Vinson Carrier Strike Group is deployed supporting maritime security operations and theater security cooperation efforts in the U.S. 5th Fleet area of responsibility. U.S. Navy photo by Mass Communication Specialist 3rd Class Christopher K. Hwang.

**Q: Do all ships and naval bases have access to the Navy's Fitness Program resources?**

**A:** Absolutely! Occasionally, those programs, which require trained field staff, may experience a short gap due to employee turnover. We stay on top of those situations and when there is a strong demand signal, we find a way to deliver. Even when it means dispatching HQ or other regional or installation staff to deliver the requested program.

**Q: What improvements are planned?**

**A:** We are currently working on a joint service family fitness initiative. We have completed extensive baseline research and will meet again in September. We plan to leverage current research and program best practices to develop a new program. In addition, we are putting the finishing touches on NOFFS 2.0. There will be three new workout series and corresponding nutrition resources. Further enhancements include an iPad app for NOFFS 1.0, an Android app for the same and the aforementioned enhancements to the fueling series apps.

We recently hired Nick Aures, a registered dietitian, to further develop our nutrition education resources. He has the opportunity to build on the existing resources put in place by our previous

dietitian. The weekly tips, performance nutrition articles, and Mission Nutrition Facilitator's Course updates will be his primary focus the next six months. Nick is a former Sailor and his active duty experience provides greater insight into the challenges associated with living life in the Navy.

In January 2012, the new Command Fitness Leader Certification Course curriculum was released and we anticipate minor adjustments based on instructor and attendee feedback. The curriculum was developed in partnership with the Physical Readiness Program office and the Center for Personal and Professional Development. Last year, MWR fitness professionals trained 1,850 command fitness leaders and assistant CFLs across the enterprise, and we anticipate that volume to continue.

Finally, our two-day nutrition education course (also delivered by installation Navy fitness staff) will be updated. We currently collect nutrition behavior surveys up to three months following the course and any changes will incorporate the information we have gathered to date. ●

**FOR MORE INFORMATION**  
Fitness, Sports and Deployed Forces Support  
[www.navyfitness.org/](http://www.navyfitness.org/)

CNIC Headquarters  
[www.cnic.navy.mil/](http://www.cnic.navy.mil/)



**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/](http://www.esi.mil/).**

## Software Categories for ESI

### Asset Discovery Tools

#### Belarc

**BELMANAGE ASSET MANAGEMENT:** Provides software, maintenance and services.

**CONTRACTOR:** Belarc Inc. (W91QUZ-07-A-0005)

**AUTHORIZED USERS:** This BPA is open for ordering by all Department of Defense (DoD) components and authorized contractors.

**ORDERING EXPIRES:** 30 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>

#### Carahsoft

**OPSWARE ASSET MANAGEMENT:** Provides software, maintenance and services.

**CONTRACTOR:** Carahsoft Inc. (W91QUZ-07-A-0004)

**AUTHORIZED USERS:** This BPA is open for ordering by all Department of Defense (DoD) components and authorized contractors.

**ORDERING EXPIRES:** 03 Nov 12 (Please phone the CHESS Helpdesk for extension information.)

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

**WEB LINK:** <https://chess.army.mil/Contract/Details/100085>

#### 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

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

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

## Database Management Tools

### Microsoft Products

**MICROSOFT DATABASE PRODUCTS:** See information under Office Systems on page 66.

### Oracle (DEAL-O)

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

**CONTRACTORS:**

**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

**Affigent, LLC** (W91QUZ-09-A-0001);

Small Business; (571) 323-5584

**ORDERING EXPIRES:**

Affigent, LLC: 29 Oct 12 (Please phone the CHESS Helpdesk for extension information.)

DLT: 01 Apr 13

immixTechnology: 02 Mar 16

Mythics: 15 Dec 15

**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](https://chess.army.mil/CMS/A/SW_DEAL_O_HPG)

**SPECIAL NOTE TO NAVY USERS:** See the information provided on page 67 concerning the Navy Oracle Database Enterprise License under Department of the Navy Agreements.

## Sybase (DEAL-S)

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

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

**ORDERING EXPIRES:** 15 Jan 13

**AUTHORIZED USERS:** Authorized users include personnel and employees of the DoD, Reserve components (Guard and Reserve), U.S. Coast Guard when mobilized with, or attached to the DoD and nonappropriated funds instrumentalities. Also included are Intelligence Communities, including all DoD Intel Information Systems (DoDIIS) member organizations and employees. Contractors of the DoD may use this agreement to license software for performance of work on DoD projects.

**WEB LINK:**  
<https://chess.army.mil/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>

### 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 Dec 12 (Please phone for extension information.)

**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: 14 Aug 15

DLT: 01 Apr 13

**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 63.

### 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](http://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](http://www.esi.mil/contentview.aspx?id=154&type=2)

**Advantaged Solutions, Inc**

[www.esi.mil/contentview.aspx?id=155&type=2](http://www.esi.mil/contentview.aspx?id=155&type=2)

**Carahsoft Technology Corp.**

[www.esi.mil/contentview.aspx?id=156&type=2](http://www.esi.mil/contentview.aspx?id=156&type=2)

**Oakland Consulting Group**

[www.esi.mil/contentview.aspx?id=157&type=2](http://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:** 07 Nov 12 (Go to Army CHESS website for extension information.)

**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](http://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, NIACAP, 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](http://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 Sigma 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](http://www.esi.mil/contentview.aspx?id=118&type=2)

**Softmart**

[www.esi.mil/contentview.aspx?id=117&type=2](http://www.esi.mil/contentview.aspx?id=117&type=2)

**SHI**

[www.esi.mil/contentview.aspx?id=123&type=2](http://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](http://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](http://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](http://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](http://www.esi.mil/contentview.aspx?id=301&type=2)

**CDW-G**

[www.esi.mil/contentview.aspx?id=302&type=2](http://www.esi.mil/contentview.aspx?id=302&type=2)

**Dell**

[www.esi.mil/contentview.aspx?id=303&type=2](http://www.esi.mil/contentview.aspx?id=303&type=2)

**Emergent, LLC**

[www.esi.mil/contentview.aspx?id=304&type=2](http://www.esi.mil/contentview.aspx?id=304&type=2)

**GovConnection**

[www.esi.mil/contentview.aspx?id=305&type=2](http://www.esi.mil/contentview.aspx?id=305&type=2)

**Insight**

[www.esi.mil/contentview.aspx?id=306&type=2](http://www.esi.mil/contentview.aspx?id=306&type=2)

**SHI International Corp.**

[www.esi.mil/contentview.aspx?id=307&type=2](http://www.esi.mil/contentview.aspx?id=307&type=2)

**Softchoice**

[www.esi.mil/contentview.aspx?id=308&type=2](http://www.esi.mil/contentview.aspx?id=308&type=2)

**Softmart**

[www.esi.mil/contentview.aspx?id=309&type=2](http://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](http://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](http://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:** 31 Mar 13

#### WEB LINKS:

**CDW Government, LLC**

[www.esi.mil/contentview.aspx?id=177&type=2](http://www.esi.mil/contentview.aspx?id=177&type=2)

**Dell**

[www.esi.mil/contentview.aspx?id=176&type=2](http://www.esi.mil/contentview.aspx?id=176&type=2)

**EnPointe Gov., Inc.**

[www.esi.mil/contentview.aspx?id=318&type=2](http://www.esi.mil/contentview.aspx?id=318&type=2)

**GovConnection**

[www.esi.mil/contentview.aspx?id=229&type=2](http://www.esi.mil/contentview.aspx?id=229&type=2)

**GTSI**

[www.esi.mil/contentview.aspx?id=235&type=2](http://www.esi.mil/contentview.aspx?id=235&type=2)

#### Hewlett-Packard

[www.esi.mil/contentview.aspx?id=114&type=2](http://www.esi.mil/contentview.aspx?id=114&type=2)

#### Insight Public Sector, Inc.

[www.esi.mil/contentview.aspx?id=173&type=2](http://www.esi.mil/contentview.aspx?id=173&type=2)

#### SHI

[www.esi.mil/contentview.aspx?id=178&type=2](http://www.esi.mil/contentview.aspx?id=178&type=2)

#### Softchoice

[www.esi.mil/contentview.aspx?id=174&type=2](http://www.esi.mil/contentview.aspx?id=174&type=2)

#### Softmart

[www.esi.mil/contentview.aspx?id=175&type=2](http://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 Defense and supported organizations that utilize the Joint Worldwide Intelligence Communications System, and (2) All non-DoD employees (e.g., contractors, volunteers, allies) on-site at the U.S. Department of Defense and those not on-site but using equipment furnished by the U.S. Department of Defense (GFE) in support of initiatives which are funded by the U.S. Department of Defense. Licensed software products available through the August Schell contract are for the commercial versions of the Red Hat software, not the segmented versions of the previous Netscape products that are compliant with Global Information Grid (GIG) standards. The segmented versions of the software are required for development and operation of applications associated with the GIG, the Global Command and Control System (GCCS) or the Global Combat Support System (GCSS).

If your intent is to use a Red Hat product to support development or operation of an application associated with the GIG, GCCS or GCSS, you must contact one of the 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](http://www.disa.mil/gcssj)

**ORDERING EXPIRES:** Nov 12; All downloads provided at no cost.

**WEB LINK:** [www.disa.mil](http://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](http://www.esi.mil/contentview.aspx?id=201&type=2)

**DLT Solutions, Inc.**

[www.esi.mil/contentview.aspx?id=200&type=2](http://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 13

**WEB LINK:**

[www.esi.mil/contentview.aspx?id=171&type=2](http://www.esi.mil/contentview.aspx?id=171&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, 2012. 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](mailto:daniel.mcmullan@navy.mil), for further review of the requirements and coverage.

This license is managed by the Space and Naval Warfare Systems Center (SPAWARSYS-CEN) 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:

- as part of a system or system upgrade, including Application Specific Full Use (ASFU) licenses;
- under a service contract;
- under a contract or agreement administered by another agency, such as an interagency agreement;
- under a Federal Supply Service (FSS) Schedule contract or blanket purchase agreement established in accordance with FAR 8.404(b)(4); or
- 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](http://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.peeis.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](http://www.doncio.navy.mil/PolicyView.aspx?ID=3777)

[www.doncio.navy.mil/ContentView.aspx?ID=3778](http://www.doncio.navy.mil/ContentView.aspx?ID=3778)

**USS Constitution, “Old Ironsides”  
participates in the U.S. Navy  
commemoration of the War of 1812 in  
Boston Harbor.**

**The U.S. Navy, a leader in energy  
efficiency, from sail to coal in the  
mid-1800s, coal to oil in the early  
20th century, oil to nuclear power  
in the 1950s, and now advanced  
biofuels, to fuel the fleet.**

