

CHIPS

JANUARY – MARCH 2013

THE DEPARTMENT OF THE NAVY'S INFORMATION TECHNOLOGY

BUSINESS CASE
ANALYSES

MOBILE
EFFICIENCIES

DATA
CENTER
POLICY

PERFORMANCE

MOBILE

COST

MANAGEMENT

PERFORMANCE

Sharing Information | Technology | Experience



EFFICIENCIES
PERFORMANCE

CENTER
BUSINESS
CASE
ANALYSES

COST
MANAGEMENT

BUILD
POLICY

EFFICIENCIES
ANALYSES



CHIPS

JANUARY – MARCH 2013, VOL. XXXI ISSUE I

DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER
MR. TERRY A. HALVORSEN

DEPARTMENT OF THE NAVY DEPUTY CHIEF INFORMATION OFFICER (NAVY)
VICE ADM. KENDALL L. CARD

DEPARTMENT OF THE NAVY DEPUTY CHIEF INFORMATION OFFICER (MARINE CORPS)
BRIG. GEN. KEVIN J. NALLY

SPACE & NAVAL WARFARE SYSTEMS COMMAND
COMMANDER REAR ADM. PATRICK H. BRADY

SPACE & NAVAL WARFARE SYSTEMS CENTER ATLANTIC
COMMANDING OFFICER CAPT. MARK V. GLOVER

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

SENIOR EDITOR/LAYOUT AND DESIGN
SHARON ANDERSON

ASSISTANT EDITOR
HEATHER RUTHERFORD

WEBMASTER
DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER

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

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.



16



DEPARTMENT

In Every Issue

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

Highlights

- 06 Navy Information Dominance Corps Human Capital Strategy
By Deputy Chief of Naval Operations for Information Dominance
- 08 Navy Cyber 2020
By Deputy Chief of Naval Operations for Information Dominance
- 40 The U.S. Military's Joint Tactical Radio System
By S.S. Kamal and John Armantrout
- 68 USS Enterprise (CVN 65) – "We Are Legend"
By Sharon Anderson

Q&A

- 12** Terry Halvorsen
Department of the Navy Chief Information Officer
- 18** John Pope
SPAWAR Director, Data Center and
Application Optimization
- 22** Rear Adm. Samuel J. Cox, Director, National Maritime
Intelligence-Integration Office
Commander, Office of Naval Intelligence
- 28** Capt. Tim Gallaudet Ph.D.
Superintendent, U.S. Naval Observatory



- 34** Rear Adm. Jonathan White
Oceanographer and Navigator of the Navy
- 46** Capt. Lourdes Neilan
Navy Warfare Development Command
Director of Cyberspace Operations
- 66** Navy Expeditionary Combat Command

FEATURES

- 16** Protecting Our Most Valuable Asset – Our People
By DON Enterprise IT Communications
- 39** Contract Award Paves Way for Agile Navy Recruiting,
Advances Vision of RF2020
By Sea Warrior Program

- 45** Get Ready, Get Set, Innovate!
By Sharon Anderson
- 48** Navy Doctrine Library System – Find the Information You Need
– When You Need It
By Sharon Anderson
- 52** Reducing the Use of Social Security Numbers
By Steve Muck and Steve Daughety
- 54** Navy Tactical Afloat Network Approved for Limited Deployment
By Sharon Anderson
- 56** SSC Atlantic Recipient of Prestigious USD(AT&L)
Workforce Development Gold Award
By Diane Owens
- 57** SPAWAR Engineer Honored with Multiple Prestigious Awards
By Patric Petrie
- 58** Enlisted Information Dominance Warfare Specialist Program
*By Deputy Chief of Naval Operations for
Information Dominance*
- 59** Large Number of Center for Information Dominance
Chiefs Pinned
By Gary Nichols
- 61** Hull Swap – A Sea Story
By Sharon Anderson
- 64** Microsoft Office Professional Plus 2010 Available for
Home Use to DON Military and Civilian Personnel
By Sharon Anderson
- 72** Norfolk Naval Station's Solar Electric System Project
By Heather Rutherford
- 73** ONR-Funded Microgrid Powers "World Green City"
By Eric Beidel



ON THE COVER

Some of the building blocks to achieve business information technology savings and efficiencies: data center consolidation, enterprise licensing, business case analysis and performance measurement.

The Building Blocks of Efficiencies

TWO EVENTS STAND out in the last few months as most pleasurable and inspiring. The first in November was a commemorative tour of the USS Enterprise (CVN 65) on the eve of her inactivation ceremony in celebration of her 51 years of legendary service.

There were so many goosebump-producing moments that it's impossible to describe each one, so I'll just say that the Enterprise's crew clearly made the most lasting impression for their dedication to duty and esprit de corps. You can read about the Enterprise on page 68.

In December, I had the honor of interviewing DON CIO Terry Halvorsen at the Pentagon. We talked about the DON CIO's ongoing efforts to reduce the department's business IT bill while modernizing and streamlining business systems and processes across the department. The DON CIO is working closely with many commands across the Navy and Marine Corps to ensure the department meets its efficiency goals. You can read Mr. Halvorsen's interview on page 12.

In step with efficiencies is the ability for the Navy and Marine Corps to operate effectively across all the warfighting domains, including cyberspace. In this issue, leadership from across the Information Dominance Corps provide their unique perspectives regarding intelligence, information warfare, meteorology and oceanography, and space.

Welcome new e-subscribers!



SHARON ANDERSON



NORFOLK (Dec. 1, 2012) Guests observe the inactivation ceremony of the aircraft carrier USS Enterprise (CVN 65). Enterprise was commissioned Nov. 25, 1961 as the first nuclear-powered aircraft carrier. The ceremony marks the end of her 51 years of service. U.S. Navy photo by Mass Communication Specialist Seaman Joshua E. Walters.international organizations.

EDITORIAL CORRESPONDENCE

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

Transparency: The Right Data at the Right Time



CHANCES ARE YOU'VE seen the TV ad for a used-car company that begins with a potential buyer looking for "a car." He is suddenly facing a sea of automobiles, which he narrows down by being more specific: "A red car. With good gas mileage. With four doors." And so on.

This is a good example of what we in the IT world call "transparency."

Contrary to common misconceptions, data transparency does not mean access to *all* data, which is too often the case — as "Megatrends" author John Naisbitt noted, "We are drowning in information, but starved for knowledge."

Transparency means greater access to the right data within our funding, budget, processes and data systems. This "right data" becomes actionable information, which becomes knowledge, and that knowledge is crucial to decision-making at all levels of the workplace. In the Department of the Navy, transparency fosters greater efficiencies and effectiveness of data-driven decision making and auditability requirements.

During the past year, we have

made significant strides in improving transparency.

We have instituted a department-wide dashboard used by Department of the Navy senior leadership and the Data Center Consolidation Task Force. The dashboard presents current cost data on IT initiatives targeted for savings gathered from authoritative data sources from industry and across the Department of Defense. It tracks progress on key efficiencies and helps inform future strategic decision making.

For mobility tracking and mobile plan optimization, the DON established enterprise wireless contracts in January 2011 with the intent of streamlining the department's mobile purchasing habits. These contracts enable the DON to pool its cellular purchasing requirements to drive down costs and gain greater transparency into purchasing habits. The savings to date amount to \$35.7 million.

Naval IT Exhibits/Standard Reporting (NITE)/STAR Line Item definition changes provide greater transparency into the IT budget by "binning" the IT spend more appropriately. This enables the DON to have far more visibility of its IT budget and more accurately reflects where its IT money is being spent. For example, prior to the updated NITE/STAR categories, 21 percent of the Navy's budget was recorded under Line 13 (Other Costs, Commercial). Today, that percentage has dropped to 4.5 percent. Similarly, during the same period, the Marine Corps decreased its reporting of Line 13 items from 51 percent to 23 percent.

DON enterprise licensing agreements (ELAs) build on the best practices of the DoD enterprise software agreements. They enable transparency of software cost savings, providing insight into the products being licensed by DON commands and programs. Addition-

ally, DON ELAs include the necessary software maintenance and vendor support items to ensure compliance with information assurance policies and prices to ensure sustainment of the software investment.

System and application rationalization is the systematic analysis and reconciliation of systems and their associated applications operating across the enterprise to determine gaps and overlaps in an effort to streamline operations and maintenance and realize cost savings. The DON has actively practiced system and application portfolio management for several decades, but the system and application rationalization effort is in its infancy. The DON CIO and DON Deputy CIOs (Navy and Marine Corps) will oversee and manage the system and application rationalization efforts for the Secretariat, Navy and Marine Corps, respectively. The Navy has merged its system and application rationalization effort with its data center consolidation initiative under the direct oversight of the Navy Data Center Consolidation Task Force.

Canadian philosopher and communications theorist Marshall McLuhan summed up our modern era in this way: "One of the effects of living with electric information is that we live habitually in a state of information overload. There's always more than you can cope with."

In such a world, having the right information at the right time is essential to making the right decision. Data transparency ensures that rather than drown in information, we satisfy our need for knowledge. ●

Terry Halvorsen

THE NAVY INFORMATION DOMINANCE CORPS HUMAN CAPITAL STRATEGY

A comprehensive plan to ensure an elite workforce retains the competitive edge in the Information Dominance warfare domain

BY THE OFFICE OF THE DEPUTY CHIEF OF NAVAL OPERATIONS FOR INFORMATION DOMINANCE (N2/N6)

In November 2012, Vice Adm. Kendall L. Card, Deputy Chief of Naval Operations for Information Dominance/ Director of Naval Intelligence, and Vice Adm. Michael S. Rogers, Commander, U.S. Fleet Cyber Command/U.S. 10th Fleet, signed the Information Dominance Corps Human Capital Strategy 2012-2017, (http://www.public.navy.mil/fcc-c10f/Strategies/Navy_Information_Dominance_Corps_Human_Capital_Strategy.pdf) which establishes a framework to drive programmatic initiatives, policy changes and supporting actions needed to achieve the vision for the IDC.

Recognizing the importance of information to maritime warfighting, the Navy established the Information Dominance Corps in 2009. In an unprecedented organizational change, professionals from the intelligence, information professional, information warfare, meteorology and oceanography communities, and members of the space cadre were combined under the leadership of the Deputy Chief of Naval Operations for Information Dominance (N2/N6). This transformation resulted in an aggregated, unified corps of professionals that produces precise, timely warfighting decisions.

Sustaining the Navy's human capital advantage in this group of highly skilled professionals is a challenge. But maintaining the Navy's operational and technological advantages depends directly on the continuous education, training and development of this elite workforce. The Navy requires an incomparable IDC workforce that is recruited, trained and educated on pace with technology that understands the maritime environment and can deliver integrated warfighting effects on demand.

GOALS AND OBJECTIVES

The IDC Human Capital Strategy provides a structured, balanced and deliberate approach for ensuring that the Navy's IDC is qualified, ready and sustainable. The strategy reinforces the Navy's commitment to leveraging the IDC's talent, developing its expertise, advancing the careers of its members, and promoting its ability to succeed in 21st century warfare.

The four goals of the IDC Human Capital Strategy are:

- Manage the Corps as a Total Force;
- Build competencies through training, education and experience;

- Strategically integrate and align the IDC workforce with mission and capability requirements; and
- Create a warfighting culture.

Each goal has a set of objectives that will help assure that goals are met.

WORKFORCE ALIGNMENT

The workforce is currently composed of 69 percent military (active and reserve) and 31 percent civilian personnel. A detailed study of the specific knowledge, skills and abilities afforded by civilian resources will inform decisions on the appropriate Total Force mix. The IDC will then develop strategies to attract, recruit and retain those with the needed skillsets based on a balance of requirements. This strategy will also ensure the IDC creates a diverse workforce, capable of meeting 21st century challenges, and engendering agility and adaptability. (Refer to the charts on the next page for a detailed workforce breakdown.)

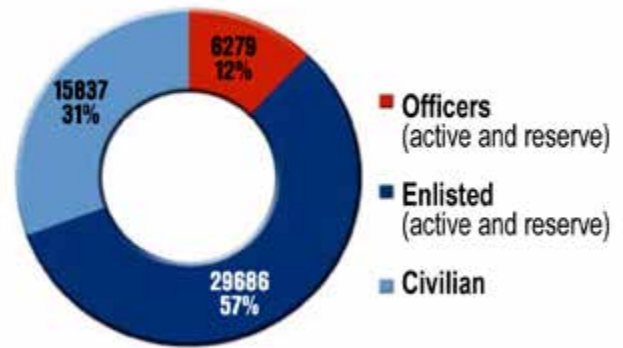
The Navy developed an ID competency framework describing the core competencies required for the workforce. The IDC has also conducted separate competency development initiatives (e.g., Human Performance Requirements Review) for each community. Though all billets within the Navy are important to mission achievement, the cyber and acquisition workforces are critical specialties. The Navy's ability to dominate cyberspace and respond to emerging security threats depends upon these workforce segments: (a) being sized correctly, and (b) having the requisite knowledge, skills and abilities to perform their missions and exploit new technology advances.

The strategy aligns with the Chief of Naval Operations' Sailing Directions and Navigation Plan, the Navy's Vision for Information Dominance, the Navy's Total Force Vision for the 21st Century, the Department of the Navy Human Capital Strategy and the Navy Strategy for Achieving Information Dominance. It was collaboratively developed by representatives from a dozen IDC organizations. Additionally, more than 240 military and civilian IDC members participated in the IDC Human Capital Capabilities Assessment, which was conducted preparatory to the strategy's development and provided valuable input on workforce challenges unique to the Information Dominance Corps.



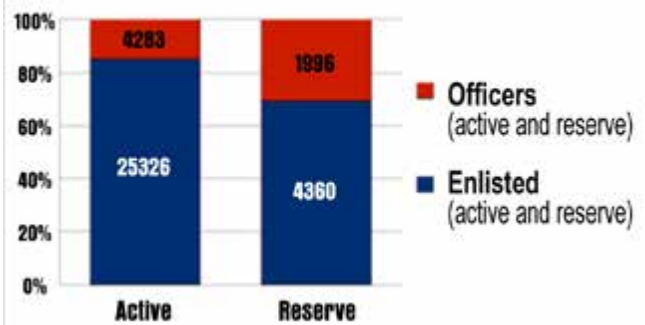
WASHINGTON (Nov. 26, 2012) Vice Adm. Kendall L. Card, Deputy Chief of Naval Operations for Information Dominance, seated left, and Vice Adm. Michael S. Rogers, commander of U.S. Fleet Cyber Command/U.S. 10th Fleet, sign three documents that set the course for the future of the U.S. Navy's Information Dominance and cyber warriors during a signing ceremony at the Pentagon. Looking on are staff members representing all those who had a part in putting these documents together. The U.S. Navy has a 237-year heritage of defending freedom and projecting and protecting U.S. interests around the globe. Join the conversation on social media using #warfighting. U.S. Navy photo by Mass Communication Specialist 1st Class Abraham Essenmacher.

Total Force by Status



Total Force according to IDC-coded billets

Military Force by Duty Status



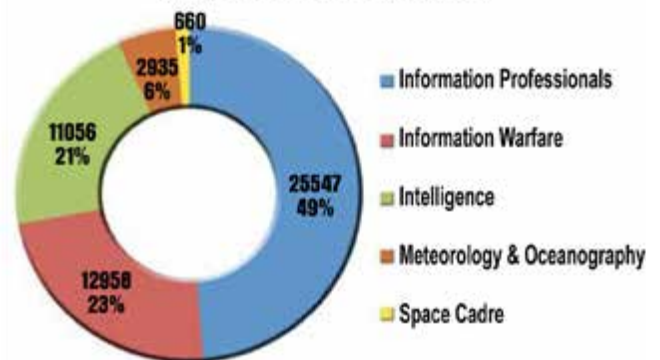
IDC Military Force

ACTION PLAN

The IDC Human Capital Strategy provides direction to the workforce and to the supporting manpower, personnel, training and education enterprise that ultimately supports the IDC as a profession. The strategy sets the IDC on a path toward actualizing information as a principal warfighting pillar in the Navy's arsenal. The IDC's success depends on agility, flexibility and adaptability to deliver the right people with the right skills, at the right time and place, and at the best value. See the charts at right for a IDC workforce breakdown.

A list of strategic guidance documents and appendices detailing specific areas for action and the warfighting effects to be achieved as a result of implementation of the strategy are included. This systematic approach and methodology for action plan development, management and monitoring will translate strategy into execution while ensuring ongoing accountability, ownership and progress evaluation. ●

Total Force by Community



IDC Workforce

FOR MORE INFORMATION

Please contact Sara Ratcliff, senior advisor for human capital, sara.ratcliff@navy.mil or (703) 604-5594.

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

NAVY CYBER POWER 2020

BY THE OFFICE OF THE DEPUTY CHIEF OF NAVAL OPERATIONS FOR INFORMATION DOMINANCE (N2/N6)

TO P NAVY LEADER-
SHIP, CHARGED
WITH ENSUR-
ING THE U.S.
NAVY REMAINS

A CRITICAL CONTRIBUTOR TO NATIONAL SECURITY AND ECONOMIC PROSPERITY, SIGNED A STRATEGIC PLAN IN NOVEMBER THAT PROVIDES THE FRAMEWORK AND VISION FOR THE INTELLIGENT USE OF CYBERSPACE TO ACHIEVE SUPERIOR OPERATIONAL OUTCOMES INTO THE FUTURE.

Vice Adm. Kendall L. Card, Deputy Chief of Naval Operations for Information Dominance/Director of Naval Intelligence (OPNAV N2/N6), and Vice Adm. Michael S. Rogers, Commander, U.S. Fleet Cyber Command/U.S. 10th Fleet, signed Navy Cyber Power 2020 (www.public.navy.mil/fcc-c10f/Strategies/Navcy_Cyber_Power_2020.pdf), which identifies distinct qualities the Navy must possess to succeed in cyberspace, and introduces methods to build a relevant and extremely capable Navy cyber warfighting force for the future.

U.S. maritime power is comprised of six core capabilities: forward presence, deterrence, sea control, power projection, maritime security and humanitarian assistance/disaster response (HA/DR). In today's highly networked world, each one of these core capabilities is enhanced by effective Navy cyberspace operations.

Navy Cyber Power 2020 (NCP 2020) is a strategy for achieving the Navy's vision for cyberspace operations. Navy cyberspace operations provide Navy and joint commanders with an operational advantage by:

- Assuring access to cyberspace and confident Command and Control (C2);
- Preventing strategic surprise in cyberspace; and
- Delivering decisive cyber effects.

NCP 2020 describes the key end-state characteristics that the Navy must create and the major strategic initiatives it will pursue to achieve success. It serves as a guidepost to inform enterprise architecture, investment decisions, and future direction in the cyber realm.

To this end, U.S. Fleet Cyber Command led an assessment of cyber threats, key trends, and challenges adversely affecting Navy cyberspace operations to identify decisive opportunities that will enable the Navy to maintain its advantages in cyberspace. To achieve this vision for cyberspace operations, the Navy will pursue strategic initiatives across four key focus areas: integrated operations; an optimized cyber workforce; technology innovation; and requirements and planning, programming, budgeting and execution (PPBE) and acquisition reform, which are summarized in Figure 1.

The Navy will continue to work with industry, academia, interagency and joint partners, as well with the other services, and allies to maximize cyber integration and ensure the most efficient use of defense resources. To measure success, the Navy intends to establish a set of strategic performance measures for each key focus area to evaluate progress and ensure it is achieving the desired effect.

Collectively, these efforts represent a fundamental change in the way the Navy conducts operations. Success requires an "all hands" effort, from the Pentagon to the deckplate.

Ultimately, the vision for NCP 2020 is that it will allow Navy cyberspace operations to continue to provide Navy and Joint commanders with an operational advantage by assuring access to cyberspace and confident command and control, preventing strategic surprise in cyberspace, and delivering decisive cyber effects.

CYBER THREATS

To defeat threats, one must understand the insidious nature of the threat environment. Cyberspace extends far beyond the traditional boundaries of Navy and joint networks. Practically all major systems on ships, aircraft, submarines and unmanned vehicles are "networked" to some degree. This includes most combat, communications, engineering, and positioning, navigation and timing (PNT) systems.

Additionally, cyberspace extends equally across joint and Navy business and industrial control systems. While connectivity provides Navy platforms and weapon systems with unprecedented speed, agility and precision, it also opens numerous attack points of entry for cyber adversaries.

At the same time, cyberspace provides a low barrier of entry for a wide range of state and non-state adversaries to effectively challenge and hold Navy forces at risk. Over the past several years, Navy networks have been attacked in cyberspace by a broad array of state actors, terrorist organizations, "hactivist" groups, organized crime, and individual hackers. Motivations include personal gain, information theft, discrediting the United States, sabotage, political gain, denial or degradation of the Navy's access to cyberspace, and mapping Navy networks.

Attacks have resulted in a leveling of the battlespace for adversaries, compromised security, and imposed stress on systems and personnel. The most troubling of these are advanced persistent threats (APTs) by state and non-state actors with the capability and intent to relentlessly probe and attack Navy networks as part of a larger anti-access/area denial (A2/AD) strategy. The Navy must be able to mitigate the impact of APTs through defensive, and when directed, offensive measures.

A large number of lesser cyber

threats also affect the Navy's effectiveness in cyberspace. Failure to adhere to long-standing information technology policies increases the spectrum of threats the Navy must address on a daily basis and distracts from identifying and defending against other threats intentionally targeting the Navy and Defense Department. These lesser threats can be mitigated by strict observance of Navy IT policies.

KEY TRENDS

While it is difficult to predict exactly what the 2020 cyber environment will look like, several key trends provide insight into the future: industry changes, IT efficiency efforts, vulnerability of the commercial IT supply chain, and an increasing complexity in configuration management.

INDUSTRY INNOVATIONS

Industry drives the accelerating pace of change in cyberspace, not govern-

ment. In practically all other areas of warfare, government investments drive innovations in new capabilities and weapon systems. However, in cyberspace, it is industry, driven by customer demand, which invests billions of dollars to enhance current and develop new cyber capabilities. Each innovation creates new potential vulnerabilities that adversaries will attempt to use to compromise security.

Conversely, innovation also creates opportunities to advance Navy cyberspace capabilities, but current requirements and budget and acquisition practices are not agile enough to take advantage of them in a timely manner.

IT EFFICIENCIES

IT efficiency efforts continue to drive consolidation and standardization of service networks across the DoD. The goal of these efforts is to create a Joint Information Environment. The JIE will consist of a shared IT infrastructure that

provides: a single, joint network architecture for each security level, consolidation of data centers and network operations centers, and a comprehensive security architecture. The capabilities to enable information sharing, collaboration, and interoperability will be provided as enterprise services across the DoD. Long-term savings from these efforts are expected, but the transition costs and additional bandwidth requirement costs will likely further strain existing budgets.

However, IT efficiency efforts also provide a unique opportunity to mitigate cyber risks. Network consolidation will reduce the number of defensive fronts and provide an opportunity to design in defensive measures from the start. It will also create greater opportunity for unity of effort across the DoD and the development of common doctrine and tactics, techniques and procedures (TTPs) across joint cyberspace operations.

FIGURE 1. CURRENT CHALLENGES FOR CYBERSPACE OPERATIONS.



SUPPLY CHAIN AND CONFIGURATION MANAGEMENT

The commercial IT supply chain, for both hardware and software, is increasingly outsourced overseas, particularly to Asia. Each node within the global IT supply chain presents adversaries with an opportunity to introduce a cyber threat or exploit the system for their own purposes. IT hardware and software developed all or in part overseas are used by Navy forces every day. The Navy acquisition system must have greater visibility and more effective controls across the entire supply chain.

As the Navy continues to evolve its warfighting capabilities, an expanding number of critical shipboard and airborne systems, including combat, communications, engineering and PNT systems, are becoming increasingly networked. This creates enormous configuration management challenges and increases the avenues for adversaries to deliver cyber attacks. The mindset of what is considered "part of the network" needs to expand to include all devices, systems, and components.

System development will require increased coordination within and across the systems commands to ensure interoperability and defensive measures are built in during the design stages.

CHALLENGES

Navy cyberspace operations face several challenges typical of other emerging warfare disciplines in the Navy's history, such as air and undersea warfare. Once again, a look at Figure 1 illustrates some of the more prominent challenges across the areas of operations, workforce, technology, requirements and PPBE and acquisition. Exacerbating these four challenge areas is a constrained budget climate. Overcoming these challenges will require careful prioritization of requirements and resources, tough fiscal choices, and program alignment decisions.

WAY AHEAD

The future of U.S. maritime power depends heavily on the Navy's ability to achieve its vision for cyberspace op-

erations. Strategy for achieving this vision is based on careful consideration of the threats, trends, and challenges facing the Navy in cyberspace. Success requires a comprehensive approach across the four focus areas that will yield desired outcomes:

- Fully integrated Navy cyberspace operations in support of achieving Joint Force objectives;
- Navy and joint cyberspace operations driven by an effectively recruited, trained, and positioned workforce;
- Industry, academia, and joint partnerships that assist in rapidly updating Navy cyberspace capabilities to stay ahead of the threat; and
- Enhanced cyber budgeting and acquisition to meet the Navy's cyber operational needs.

In association with the work being done in support of the four focus areas, the Navy intends to evolve cyberspace doctrine, TTPs, and operational plans to take full advantage of cyber capabilities across the full range of military operations. Further, the Navy will fully exercise all aspects of cyberspace requirements and operations in battle exercises, unit inspection, and all Fleet Readiness Training Plan (FRTTP) phases in tandem with other warfare areas to facilitate the transition of cyberspace operations into a seamless component of maritime operations.

ADAPTIVE NAVY FORCE MODEL

While the Navy maintains a workforce of cyber professionals who are proficiently skilled, appropriately trained, and effectively positioned to carry out cyberspace operations in support of Navy and joint commander objectives, the Navy must continue to develop a comprehensive cyber training and education model that can rapidly adapt to industry advances and evolving joint commander needs. The Navy must continue to be able to rapidly respond to evolving cyber needs through robust training and an agile force model that ensures the Navy's cyber workforce remains optimally aligned and personnel resources

are used most efficiently.

The Navy will be working to overcome cultural barriers impeding the full integration of cyber capabilities through communication, training, incentives, enforcement of policies and effective governance. This effort will focus on increasing awareness of cyber threats and continually improving cybersecurity practices across the Navy.

To diminish the challenges of emerging technologies, the Navy plans to institute a robust pilot program to aggressively seek out and test emerging cyber technologies in real world and cyber ranges, assess their operational impact, and be able to quickly integrate them across the Navy. This will require a coordinated effort across the Navy that focuses cyber technology pilots and demonstration projects on the most pressing operational needs.

ASSESSMENT AND COURSE CORRECTION

The Secretary of Defense's strategic guidance highlights the critical role cyberspace operations play in the success of the Joint Force across all mission areas. The Navy's success in the maritime domain depends upon its ability to project power and prevail in cyberspace. The NCP 2020 strategic initiatives provide the ways and means to achieve and sustain the Navy's advantage in cyberspace. To assist with implementation of Navy Cyber 2020, OPNAV N2/N6 and U.S. Fleet Cyber Command/U.S. 10th Fleet will issue a supporting roadmap detailing lead and support organizations for each strategic initiative and the major actions necessary to accomplish them. However, as cyberspace evolves Navy's leadership will periodically assess this strategy to ensure it effectively guides the Navy's efforts to maintain an operational advantage in cyberspace.

When necessary, the Navy will adjust course to respond to, if not anticipate, change that continues apace. ●

FOR MORE INFORMATION
FLTCYBERCOM/10th Fleet
www.fcc.navy.mil

Emailing Personally Identifiable Information

THE FOLLOWING IS a recently reported personally identifiable information (PII) data breach involving the transmission of an email containing 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

An unencrypted email was sent to three military members' government email accounts. Attached to the email was a roster that contained the names and full Social Security numbers (SSN) of 48 service members. Not all the recipients had an official need-to-know. One of the recipients had the email auto-forwarded to a personal commercial email account. Additionally, the attached document was not marked appropriately for privacy sensitive content in accordance with DON policy.

Actions Taken

Upon confirming there was a PII breach, all copies of the unencrypted email were properly deleted. A breach report was submitted and individual written notifications were sent to the 48 affected individuals.

Lessons Learned

When emailing PII, the sender must understand and apply the following rules:

- ➔ Emails containing PII must be digitally signed and encrypted.
- ➔ Recipients must have an official need-to-know.
- ➔ Rosters may not contain SSNs in any form.
- ➔ Storage of any form of PII is prohibited on personally owned laptop

- ➔ computers, mobile computing devices and removable storage media.
- ➔ Auto-forwarding email to a commercial account is prohibited.
- ➔ The body of the email should include: "FOR OFFICIAL USE ONLY (FOUO) – PRIVACY SENSITIVE. Any misuse or unauthorized disclosure may result in both civil and criminal penalties."
- ➔ As a best practice, the email's subject line should contain: "FOUO - PRIVACY SENSITIVE."
- ➔ Attachments should always be checked for PII. Excel spreadsheets can have multiple tabs. All tabs should be double-checked for content.
- ➔ PII once transmitted outside the security of the Navy Marine Corps Intranet or other government firewall cannot be safeguarded or controlled.

Commands should consider requiring PII awareness and PII refresher training for individuals who cause a breach. Both training sessions are available on Navy Knowledge Online, Total Workforce Management Services and the DON CIO website. The training will also soon be available on MarineNet. Refresher training is a new resource and consists of nine short scenarios. Each standalone scenario covers a single privacy-related topic. Commands can require an individual to take any number of the scenarios as deemed appropriate. Breach notifications not only cost scarce resources (time and money), but can also negatively affect morale and trust in an organization. ●

STEVE MUCK is the Department of the Navy privacy lead.

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

POLICIES AND GUIDANCE ON HANDLING PII

The following policies and guidance for handling PII can be found on the DON CIO website.

- DON CIO Washington DC 032009Z OCT 08, "DON Policy Updates for Personal Electronic Devices (PED) Security and Application of Email Signature and Encryption"
www.doncio.navy.mil/ContentView.aspx?id=782;
- SECNAVINST 5211.5E, "Department of the Navy (DON) Privacy Program"
www.doncio.navy.mil/ContentView.aspx?id=799;
- DON CIO Washington DC 171625Z FEB 2012, "Department of the Navy Social Security Number (SSN) Reduction Plan Phase Three"
www.doncio.navy.mil/ContentView.aspx?id=3757;
- DON CIO WASHINGTON DC 171952Z APR 07, "Safeguarding Personally Identifiable Information (PII)"
www.doncio.navy.mil/ContentView.aspx?id=1976;
- DON CIO WASHINGTON DC 031648Z OCT 2011, "Acceptable Use Policy for Department of the Navy (DON) Information Technology (IT) Resources"
www.doncio.navy.mil/ContentView.aspx?ID=2829; and
- DON CIO WASHINGTON DC 081745Z NOV 12, "DON Fax Policy"
www.doncio.navy.mil/ContentView.aspx?id=4267.

Mr. Terry Halvorsen

Department of the Navy Chief Information Officer

Mr. Terry Halvorsen is the Department of the Navy Chief Information Officer (DON CIO). Shortly after being named DON CIO in November 2010, Mr. Halvorsen was designated the department's IT/Cyberspace Efficiency Lead. As such, his focus is on improving the way the department manages business IT with the end goal of identifying and implementing opportunities for greater operational efficiencies and effectiveness to deliver increased cost savings. Prior to Mr. Halvorsen's appointment to DON CIO, he served as the Deputy Commander, Navy Cyber Forces, from January to November 2010. Before that, he was Deputy Commander, Naval Network Warfare Command.



Terry Halvorsen

Mr. Halvorsen responded to questions regarding the Department of the Navy's ongoing efforts to achieve improvements in business IT efficiencies in December at the Pentagon.

Q: Under Secretary of the Navy Robert Work's directive to save \$2 billion in business IT spending was a huge undertaking. How would you evaluate the success of the efforts so far?

A. Progress has been good. We still have a couple of things to work, such as how the department tracks dollars so that they actually come from the right places. And, we still have some work to do with data center consolidation to get that moving at a quicker pace. Overall, the numbers we have seen are right at what we predicted for 2012 and 2013. I'm very confident we will get to where we want to be.

Q: How do you think the workforce is responding to all the policy changes?

A. I think most of the workforce recognizes that we have to take cuts across the board given the financial challenges that face the department. They do believe the business side is the right place to find those efficiencies in order to protect op-

erational dollars for Sailors and Marines. By protecting those dollars, we can invest in the equipment and training they need.

Q: I noticed that you've issued policy jointly, for example, with the Assistant Secretary of the Navy for Research, Development and Acquisition; Assistant Secretary of the Navy (Financial Management and Comptroller); and the Deputy Chief of Naval Operations for Information Dominance (OPNAV N2/N6). We rarely see jointly signed IT policy memos. Can you explain why we are seeing this trend?

A. I'm glad you asked, and I hope this change is recognized across the department. We are a big bureaucracy, and big bureaucracies respond better when their senior stakeholders are involved. So if I issue a policy from the DON CIO, other parts of the organization may see it as something that pertains only to IT people and don't see the importance or relevance to them. But when their own senior leaders sign a document, they see the seriousness of it and it does influence the outcome.

In the past, we all wrote policies, but the fact that they were not signed by all the key stakeholders may have led some people to believe there was misalignment. In jointly signing policy memos,

we want everyone to understand that there is complete alignment between the finance groups, the acquisition group, the management team under (Deputy Under Secretary) Eric Fanning, the service teams and the DON CIO. Feedback I have received on the memos has led me to believe we have sent the right message, and we will continue to issue policy memos jointly.

Q: Besides implementing new policies or revising current ones, what innovations are being considered by the DON to achieve its goal of saving \$2 billion over the next five years? Have the policies sparked innovation or stifled it?

A. I think the drive to be more efficient has certainly helped us look at different ways to do things. It might not be obvious in that we didn't buy a brand new technology. Changing technology is only part of the equation. What we have done is refine our IT processes to make them more effective. The focus on budget reductions has made us more accepting of ideas that, in the past, we may have thought too extreme to consider. The next step will be a more fundamental change to the way we do business and the way we act as a business. For example, does the Department of the Navy need to be in the data storage business

and run its own data centers? Or could we turn unclassified data storage over to the commercial sector at a much lower cost yet continue to have oversight?

We should be sharing processes within the Navy and Marine Corps, and at the DON level, DoD level, and maybe with the other services. We know that similar communities have different processes for similar work. We are going to have to learn to share and standardize processes, which helps reduce costs.

Q: I noticed that you have a process for business case analysis, and you have asked the workforce to contribute suggestions. Have any good ideas bubbled up?

A. Yes, and we are still evaluating some of those ideas. For instance, ways to reduce printing costs have been developed through a combination of some of the DON policy work and input from the field.

Most people think we are just going to reduce paper use but it is more than that. It is a fundamental change to transmitting, moving and displaying data. For example, we are here in the CHINFO conference room where there is a nice big LED screen. If I were giving a brief, why would I provide printed copies of the brief? Why not display the brief on the screen and give everyone a tablet to take notes? Or better yet, change policy so that they can bring their own tablet PCs and take notes electronically, which is less expensive and moves data faster.

Ideas from the field involve expanding savings by reducing printers and fax lines. We want to get away from faxing since it is one of the most non-secure ways of transmitting data. Most people don't have faxes on their desk, so documents just wait in a queue somewhere for pick up. It is hard to verify who takes possession of the document.

A digitally signed electronic document is more secure and it moves faster. The Department of the Navy JAG (Judge Advocate General) and OGC (Office of the General Counsel) have led the way to make digitally signed documents legally binding. In addition, it saves money and

is more energy efficient, which supports Secretary Mabus' policy that the department should be as green as possible without negatively affecting the mission.

We have had some great comments from the field about using multifunction devices that print, copy, scan and fax. The good news is that we are also getting great support from senior leadership who has been willing to give up their own printers and walk the extra steps or look at data on the screen. From a business standpoint, printing hard copies costs money, so getting away from printing and doing everything electronically would be a big savings but it is a huge change. Some of the changes involve pushing these cultural boundaries.

Part of this fundamental change is the way we think about data. In addition to all the dynamics surrounding printing, Commander, Navy Installations Command (CNIC) has some interesting suggestions for saving energy using computers to monitor room temperature and turn lights on and off when people go in and out of a room. Some commands are already doing this. In fact, the lights in my Pentagon office go off automatically at 6:00 p.m. After they go off, I have to turn them back on, but they only stay on for two hours at a time so they will never burn all night. We could do this on an enterprise scale. These are just a few of the great ideas from the field; we are very happy about that and encourage people to keep thinking of new ideas.

Q: Can you discuss the scope of these two policies: Information Technology Expenditure Approval Authorities (ITEAA) (www.doncio.navy.mil/ContentView.aspx?id=2538) and Achieving Measurable Efficiencies Through Data Center Consolidation, System, and Application Rationalization Guidance (www.doncio.navy.mil/contentview.aspx?id=4163)? Specifically, is your intent to reduce the number of business IT systems as well as the physical footprint of business IT systems?

A. The drive is to reduce cost. Because

the department is so big, we have found that we often buy the same thing twice. The IT Expenditure Approval Authority provides a central authority to review and approve planned IT spending.

One of the things we looked at hard this year was storage capacity. Prior to the establishment of the ITEAA process, I signed a memo that said no one can buy data storage, because we already had so much extra capacity within the department. Program offices were buying storage, mostly because they didn't know about or know how to take advantage of the capacity we already had. So now we are leveraging the storage solutions we already own.

Storage is just one example of how having a centralized process, identifying duplication and requirements, and consolidating resources is allowing us to more effectively spend limited IT dollars and save money.

Q: There must be some risk in consolidating all your assets, so how do you evaluate the risk versus the benefit?

A. The same way you evaluate any risk equation. We don't want to go extreme and have only one data center. Sure, it's possible to pick a site and put all our data in one center; but that is probably not a good idea from a risk analysis standpoint.

Right now we are on the opposite end of the spectrum. Depending on the definition used, we have between 140 to 150 data centers in the Department of the Navy. We definitely don't need 150. The current target is to go down to 25 or fewer. Twenty-five provides enough redundancy so that the security risk is lower. If we decide to push the savings and go lower to 5 or 10 data centers, then that would be a more risky equation.

With application rationalization, the thinking used to be that if the applications were not 100 percent overlapped, we thought rationalization was not a good decision. Now the thinking is that if an application is 60 percent overlapped then that is a good starting point to do the analysis and possibly collapse the other apps. For example, we may have an

application which has a financial piece, and you see that different applications have the same requirements and use the same type of programming for those financials. We can decide that everybody is going to use this one financial module and eliminate all the others. This is hard. Commands and people are going to have to change their processes so they can comply, eliminate systems and get to one system inside the DON. Let me be very clear — we are doing that right now exclusively for business IT systems — not warfare or direct missions systems.

Q: How many data centers have been closed so far and how many more consolidations are anticipated? I've read some different numbers from different offices; how do you account for the differences?

A. Over the Future Years Defense Program (FYDP) [which covers FY13-FY17], we want to get down to fewer than 25 data centers. We will have to close 100-plus data centers to meet that goal. There are groups working on the closure plan who say we are going to close 20 to 30 data centers, but that might be in the 2013 to 2014 timeline. Based on your question, I can see where the confusion occurs. So, I'm going to ask people to be more specific and not only provide the numbers, but also their phased timelines.

In what I have reviewed to date, I have not seen any conflict. We are closing 100 over the FYDP, and 20 to 30 of those in the next two fiscal years. The different numbers come from the different timelines. How many are you closing over the FYDP? How many are you going to close in the next segment? And how many have you closed so far? Each question has a different answer.

To date, we have closed three to five, actually moving data and systems out of them. One of the things to recognize is that we have moved some systems and data out of some data centers, but haven't actually closed the entire data center yet. We're getting there. It may happen that we close five or six or ten at one time because all of the systems and data move out at the same time.

Q: Is the next step cloud computing?

A. The answer is yes. But, I don't like the word *cloud* because it means so many different things. The next step is more *distributed* computing. The data and apps you will be using will be in central locations. That will reduce the desktop infrastructure.

I am participating in a pilot for NMCI called HVD, hosted virtual desktop. It is basically the newest version of thin or zero-client. I don't have a computer. I have a little black box on my desk that pulls the data I need from servers, or 'the cloud.' This is both less expensive and 'green' in energy savings. The other big gain is security. When I turn off my device there is no residue, no data is stored on that device. The only way to get to the data is to break into the main servers. That is much harder than breaking into an individual device. It is a much easier footprint to secure at less cost, which is the best of both worlds.

Q: You have been a huge proponent of the Navy's "audit readiness" plan to achieve full financial auditability by 2017. Why is this important to the department and why does the DON CIO care about audit readiness?

A. Understanding how the money flows through our financial systems is more valuable than just saying the department's financial systems are auditable. It really means you understand the financial data, what you are spending and your projections. It will have a huge impact on us, not only for being more efficient but for being better able to make financial decisions.

The reason why the CIO organization is so involved is because the field of cyber and IT has the potential for more economic impact than other areas because much of today's money moves in the cyber environment. The DON is required to produce certified financial statements by 2017, but aside from the requirement, audit readiness is something to strive for because it produces

accurate financial controls and transparent business processes.

Q: Under Secretary of the Navy Robert Work released a memo focused on safeguarding personally identifiable information such as Social Security numbers, medical information and other PII. What is the DON CIO doing to comply with the intent of this memo, which is to protect Sailors' and Marines' PII?

A. We have released some good guidance about privacy data, protecting privacy data, and consolidating record systems. One of the efforts I am working on with Ms. Carla Lucchino (Assistant for Administration to the Secretary of the Navy) is how we can get to one records management system in the Department of the Navy. This will improve our efficiency and help identify where the data is and where it goes.

We are trying to emphasize to commanders that data is as valuable as a weapon. Anyone who has ever served knows that there are severe penalties for losing a weapon. We want to get to a point where we are able to hold people accountable for losing privacy data. Today, it can be more devastating to lose data than a weapon. We are trying to change the culture while at the same time providing better tools for managing data.

The more places I put privacy data, the more chances there are for unauthorized people to get to it. We are trying to better understand the physical location of the data — who has access to it, and whether they actually need it. Maybe they really need aggregate information about groups of people for analytics, but they don't need access to privacy information about specific individuals.

One of the things we need to enforce is that when you require data, you must get it from the authoritative data source. We have too many instances today of data being pulled from various data sources and stored in various systems, but none of the data is from an authoritative source. It's not updated and controlled, and there are no processes in

place to update or control it. How do we know who owns it? Or protects it? And is it even accurate data?

We just updated the policy on the reduction of SSN use. The most common method of identity theft is to use an individual's Social Security number. In the DON, in the services and in all of DoD, we put the SSN everywhere. Years ago when I was in the Army, I stenciled my SSN on my duffle bag. We have moved way past that; but, we have to go even further. We have to determine when it is absolutely essential to use an SSN or other privacy data, and how to securely store and display it. We have put out policy about the rules for collecting and using privacy data, and we will be issuing more guidance to hold people accountable if they violate the rules.

Q: It sounds like everything boils down to data management. Are you developing an overarching strategy?

A: It really is an overarching data management strategy. Data is our bread and butter. Besides our people, it is the most valuable thing we own. It really is a value statement about the kind of data, how much it costs to store and an evaluation of the real threat. It takes in all the things we have talked about in a comprehensive way. It is not just looking at individual pieces of data. During our discussions with industry, we found that it is a universal problem. It is about understanding all the key elements of data as a whole. Some data by itself is not valuable but when combined with other data elements, it becomes really, really valuable.

For example, many firms use shopping data to target potential customers for the types of things they tend to buy. Take that to another level and you can interpret lifestyle and personal information about people. Information is valuable; it allows you to make decisions. In the DON, we use data in business and warfare.

Q: Since the Department of the Navy established the DON Enterprise Wireless Contracts (www.navy.mil/navsup/ourteam/navsupgls/prod_serv/contracting/market_mgt) in January 2011, the DON has saved \$11.7 million in fiscal year 2011 and \$24 million in FY12 for a total savings of \$35.7 million. How did those savings come about and what else can mobile IT users expect to see in the future regarding mobile IT solutions and efficiencies?

A: We have found savings, and all of the credit for this goes to the Navy and Marine Corps Echelon II and Major Subordinate commands. I don't get the credit for what they have achieved. We helped put a spotlight on things so they could see their data better and we gave them the tools. It is becoming more of a success every day because we are becoming better at evaluating how many devices we need. We want to encourage commands to use the devices smarter and more efficiently.

If I can get to the full version of HVD, one of the possibilities is that personnel could use their own personal computer; therefore, we don't have to buy them one. You could be at home on any computer that meets the minimum requirements and log on to your unclassified email, access your folders and the only thing you would need is a CAC reader.

There is a lot of good work being done by the DoD CIO and at DISA (Defense Information Systems Agency) by (Director) Lt. Gen. Ronnie Hawkins and (Vice Director) Rear Adm. David Simpson to get to the next set of mobility policies and how we can take advantage of commercial applications.

We are not yet to a 'bring your own device' or BYOD state. I don't know if we will ever get to a pure BYOD environment. But I think in the not too distant future, we will be able to provide a list of several approved cell phones that you can purchase and have access to your work email and some of your files and applications. People will really like that because it will simplify their lives. For example, I have a both a personal Windows phone and a BlackBerry. In an ideal world, I could have one phone that would do everything I need.

The other thing senior leadership is working on is improving telework. We have learned from industry that there are both cost savings and quality of life improvements to be gained with telework. If you get enough people to telework, you lower space requirements, and perhaps reduce the amount of leased office space. In high-density traffic areas it reduces the number of cars on the road, and it's a huge savings to both employees and the country as a whole. It's green. We would like to get policies and processes in place to make telework more accessible to more employees.

Q: You wrote in your CHIPS column in the October-December edition that mandatory use of DON enterprise licensing agreements (ELA) will 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). Can you talk about the contracts that are available? Will enterprise licensing opportunities expand?

A: The enterprise contracts have done very well. The acquisition community gets huge credit. The Program Executive Office for Enterprise Information Systems (PEO EIS) had a lead in this, as well as the Marine Corps. They've done great work. We have the Microsoft Enterprise Licensing Agreement in place and are working several others. We are also improving the toolsets that commands can use to evaluate what other applications the department can buy as an enterprise.

We are talking to DISA and the other services. Sometimes you can get too big, but we are looking at some of these purchases and asking whether licensing for all of DoD would generate more savings. Maybe DISA can be the broker to gather the requirements and establish option contracts — not necessarily mandatory contracts — but contracts that can save money. ●

FOR MORE INFORMATION
DON CIO www.doncio.navy.mil



1st Lt. Eric J. Wilmot, assistant operations officer, 3rd Light Armored Reconnaissance Battalion, sits with his 2-year-old daughter Kayla during the 3rd LAR change of command ceremony at Lance Cpl. Torrey L. Gray Field.

PROTECTING OUR MOST VALUABLE **ASSET**

OUR PEOPLE

BY DON ENTERPRISE IT COMMUNICATIONS



ONE OF THE MOST IMPORTANT FUNCTIONS the Department of the Navy can perform on behalf of its Sailors, Marines, civilians and their family members, is to protect their personally identifiable

information (PII). The Social Security number (SSN) is one of the most common elements of PII, and its loss, theft and compromise can result in identity theft, financial difficulties and loss of privacy. In 2011 alone, identity fraud increased by 13 percent in the United States, affecting more than 11.6 million people according to the 2012 Identity Fraud Industry Report, released by Javelin Strategy & Research.

The Department of the Navy has taken significant steps to ensure the security of its most valuable asset — our people. The most notable of these steps came in the form of the Under Secretary of the Navy’s memo “Safeguarding Personally Identifiable Information” (February 2010) (www.doncio.navy.mil/ContentView.aspx?id=1583), which emphasized the importance of personal privacy and the safe management of the DON’s PII, including the SSN.

This is what has been done so far to limit the risk of identity theft from SSN use:

- In 2011, the department completed Phase One of the DON SSN Reduction Plan (www.doncio.navy.mil/ContentView.aspx?id=2089), as outlined in the memo, which requires the DON to justify the continued use and collection of SSNs on all official Navy and Marine Corps forms.
- In Phase Two, program managers and system owners identified information technology systems that could eliminate the collection of SSNs by substituting the Department of Defense (DoD) identification number — the Electronic Data Interchange Personal Identifier (EDIPI).
- Phase Three authorizes the use and substitution of the DoD ID number and provides strict guidelines for its use.

Yet, more remains to be done, particularly regarding Phase Three, which requires the DON to take three significant actions:

- Commands must follow strict guidelines for the use of the EDIPI. All DON business processes must meet specific criteria outlined by the DON for continued SSN use, elimination of the use of SSNs, or transition to the DoD ID number as a substitute for SSNs.
- All letters, memoranda, spreadsheets, hard copy and electronic lists must meet specific criteria if they collect SSNs.
- When changes to a process result in the elimination of the use of SSNs, DON directives and instructions shall be updated to reflect those changes.

Another significant aspect of Phase Three affects the use of fax technology to transmit PII/protected health information (PHI). The current policy states that, effective immediately, the use of fax machines to send information containing SSNs and

other PII by DON personnel is prohibited, except under the following circumstances:

- When another, more secure, means of transmitting PII is not practical;
- When a process outside of DON control requires faxing to activities such as the Defense Finance and Accounting Service, Tricare, Defense Manpower Data Center, etc.;
- In cases where operational necessity requires expeditious handling; or
- When faxing PII related to internal government operations only, such as office phone number, rank or job title.

However, external customers such as service veterans, Air Force and Army personnel, family members and retirees may continue to fax documents containing SSNs to DON activities but are strongly encouraged to use alternative means, such as the U.S. Postal Service to mail documents and scanning documents. Scanned documents must then be transmitted using a secure means such as encrypted emails or the safe access file exchange (SAFE). Details regarding the use of SAFE can be found at www.doncio.navy.mil/ContentView.aspx?id=4098.

Processes that require less modern transmissions techniques, such as faxing, have inherent risks and should be reviewed to minimize their use. The same review should apply to the associated products of these processes, such as paper copies. If the department can minimize the need to fax, we can reduce or eliminate the need for storage of paper copies, the cost of paper, equipment and supplies and the likelihood of PII/PHI being lost or stolen.

Federal privacy laws require agencies to establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records to protect against any anticipated threats or hazards to their security or integrity. As a department, and within the larger DoD, we need to ensure that our processes and policies provide the most appropriate level of security for this vital information. By using the most current technology, such as encrypted emails, we can increase our security while reducing the risk of loss of PII/PHI.

As Under Secretary of the Navy Robert Work stated in his 2010 memo, “Our Sailors, Marines, and civilians, along with their dependents, expect us to keep their PII safe, and it is our charge to ensure that all systems and processes we employ adequately safeguard this information. We cannot tolerate the continued loss of this data as it directly impacts the morale, security, and financial well-being of our personnel.”

For more information visit the DON CIO’s privacy tips located on the DON CIO website at www.doncio.navy.mil/ContentView.aspx?id=906 and the Defense Privacy and Civil Liberties Office website at <http://dpclo.defense.gov>.

To contact a privacy subject matter expert, please submit a request via the Ask An Expert section of the DON CIO website. Be sure to select the privacy topic area. ●

John Pope

SPAWAR Director, Data Center and Application Optimization

John Pope took on a new role as Director of Data Center and Application Optimization (DCAO) at the Space and Naval Warfare Systems Command (SPAWAR) in October 2012. In this capacity, he oversees the execution of the Navy's data center consolidation effort. Prior to assuming this position, he served 29 years in the U.S. Navy, most recently as the fleet support program manager within SPAWAR's Fleet Readiness Directorate. The Navy's data center consolidation effort is a little over a year old. Mr. Pope was interviewed by Tina Stillions in December. Edited excerpts from the interview follow.



John Pope

Q: Can you give a brief update on the Navy's data center consolidation effort? What has been accomplished so far?

A: Since the Navy's data center consolidation effort began in late 2011, the Navy has consolidated 18 data centers from across the country into three U.S. Navy Enterprise Data Center (NEDC) locations. We moved 107 systems and their 600-plus servers into an enterprise environment so that they could be hosted in a more efficient manner. As we transitioned systems, we refined our processes and captured some good lessons learned.

The NEDC sites are maturing in how they work together as an enterprise, and customers are seeing the benefits in terms of standard hosting services and lower rates. Although we are still experiencing some challenges in the NEDC, due to the consolidation of a variety of systems from inconsistent hosting environments, our data center technicians have been able to work with the legacy application owners to fix application hosting issues rapidly as they are identified.

In fiscal year 12, we were required to physically move servers and equipment for some systems due to technical limitations that prevented virtualization. We learned a lot about the health of the applications as we migrated them into the NEDC. It is not simply a matter of acquiring the software, copying it onto a disc

and moving it over — and it's certainly not like loading Microsoft Word on to your PC. We discovered that there are a lot of systems out there that need security help and NEDC transition engineering to get them to a state to be able to be hosted and functioning properly in an enterprise environment. This has provided us with the opportunity to increase the efficiency of the Navy's IT infrastructure and improve the security of our data.

By capitalizing on state-of-the-art virtualization technology and efficient data center management, we are saving money on both systems administration manpower and power usage. We have tracked the percentage of servers that we are able to virtualize through the transition process, with an internal target of 90 percent.

Reducing the number of data centers and using more efficient technology enables a net savings in maintenance costs. Additionally, bulk hardware and software procurements promote competitive pricing. When we take physical servers and virtualize them, we are able to ensure they are 'right sized' according to requirements, which saves the Navy money in terms of providing optimal space and computing power to run the systems effectively.

The NEDC sites have also established sophisticated information assurance monitoring techniques and disaster recovery processes to better protect data.

During Hurricane Irene, which impacted both the Charleston and New Orleans NEDCs, there were security protocols and continuity of operations measures in place to avoid any system outages. We plan to work with our future customers to provide proactive steps to prepare their systems for transition to NEDC sites, including expediting the transitions and reducing the time and resources needed to move legacy systems into their new hosting environments. We published a NEDC catalog of services and a common NEDC rate card, so system and application owners can clearly understand their service and pricing options. The rate card standardizes data center costs across our NEDC sites and provides system owners with more detailed cost information for each level of service.

There are a lot of players when it comes to running a system on a Navy network, including the hosting facility, the security accreditors, and those that support it day-to-day with information assurance patches. In many cases, these players have been working independently. Part of our role working with so many application owners is to bring the various players together. We have developed stronger relationships and our communication channels are getting better. Even though it's still not easy, this tends to minimize some of the uncertainty, builds trust among everyone involved and streamlines the whole process a little bit.

Q: What is the data center consolidation approach? Will your team work to execute a new plan, stay with the already established approach, or create a blended plan that encompasses a little of both old and new?

A: The team is following the same success formula that was in place when I came on board. We have a list of systems and legacy data center sites that need to be consolidated, closed or removed from the list. We are working our way through that list, and are going after the sites that provide the highest return on investment. We are also looking at the sites that are out there and are part of some other IT efficiency effort, so that we can optimize our efforts.

The current FY13 plan is to transition more than 150 systems from 22 data centers into consolidated government and possibly other hosting facilities. To the greatest extent possible, these will be full closures — meaning, data center operations will no longer be conducted in the facility and transformation of the facility or room to its final disposition state will be underway. Our objective during this process will be to provide the most cost effective, efficient and secure hosting services to our Navy customers and build on the momentum created in FY12.

We will continue to follow our four-step process for consolidation. As part of the assessment phase, transition and cost teams perform on-site visits to data centers and gather information on current capabilities, IT assets, system requirements and cost elements. During the engineering analysis phase, they conduct a more detailed analysis of the systems and hardware, identify any dependencies, and develop the transition plans to migrate systems to the targeted hosting facility.

In the transition phase, SPAWAR works closely with commands and data center system and application owners to prepare their systems for migration and the execution phase of transitions. During this phase, it is critical for the legacy data centers to have all the system security documentation in place and perform

"Reducing the number of data centers and using more efficient technology enables a net savings in maintenance costs. Additionally, bulk hardware and software procurements promote competitive pricing. When we take physical servers and virtualize them, we are able to ensure they are 'right sized' according to requirements, which saves the Navy money in terms of providing optimal space and computing power to run the systems effectively."



Special floors and energy-efficient cooling technology are part of the Navy's effort to realize fiscal and energy savings. Data center photos by Rick Naystatt/SPAWAR HQ.

any necessary mitigation actions. Finally, in the sustainment phase, the systems and applications are hosted based on the agreed-upon service levels and established NEDC rates.

We have also seen how important application rationalization is to the process. The Navy is focusing on application rationalization in order to fully understand the functionality and business value-added benefit for each application in the DON portfolio. If a system does not justify its up-front or support costs, then decisions must be made to remove it from the portfolio. Functional redundancies can be identified during the process and converged to create a reduced application count. From a data center consolidation perspective, it is very important to be involved in this process. As a technical advisor, our engineers will evaluate applications against technical criteria to help application rationalization decision makers. Ideally the decision to sunset applications will be made before they are consolidated into a NEDC, which will save us

time and money.

Because there are multiple groups addressing IT infrastructure issues and trying to optimize them, we will make every effort to work together. What I'm trying to do this year is work synergistically with other organizations in targeting IT efficiency savings. If we are focusing on the same site, we'll work to synchronize efforts to reduce redundant effort and site disruption. This is a positive change in the way we do business, and I think it will yield better savings for the taxpayer.

Q: Has the schedule changed? Is the effort on schedule or behind schedule?

A: We have developed a preliminary integrated master schedule for executing the 22 site closures targeted for FY13 and have completed nearly all of the site visits. Typically, the first third of the year entails conducting detailed engineering analyses where we verify system requirements and lay out a more detailed, risk-based

schedule. The remainder of the year will be allocated for executing the site transitions. My feeling is that we certainly have a challenging, but achievable schedule for FY13.

Q: Can you explain the Data Center and Application Optimization office alignment with the Fleet Readiness Directorate and the reason behind it? How will it impact the consolidation effort?

A: In November 2011, SPAWAR was appointed by Assistant Secretary of the Navy for Research, Development and Acquisition as the Navy data center execution agent and technical authority. The Data Center Consolidation Task Force was stood up to oversee the consolidation process and the sustainment of the transitioned systems. In November 2012, SPAWAR established the Data Center and Application Optimization (DCAO) office within the Fleet Readiness Directorate (FRD) to replace the task force with a more permanent organization.

The FRD provides a fleet focus on readiness and sustainment of in-service C4I systems. It was an ideal candidate home because the FRD was already working issues that affect fleet readiness, and certainly data centers are an element of that. The fleet modernization aspect of what we do in FRD is very similar to data center consolidation. The process of taking a ship, removing old capability, and putting in new capability and optimizing it is not unlike what we do when we go into a data center and move that application to a more efficient, modern system.

As we strive to make sure the Navy's data is secure and available, we also want to host it in the most cost-effective manner possible. By administratively aligning under the FRD, we can ensure the Navy's data center consolidation effort will have the resources and support required to achieve its mission. It remains a high-priority Navy IT efficiency initiative, under a different name.

Q: Have the Navy Enterprise Data Centers (NEDCs) changed, including expanded or

retracted? What is the current status?

A: Last year, we migrated systems to three NEDC sites located in Charleston, New Orleans and San Diego. We are currently working with the Department of Navy Deputy Chief Information Officer to evaluate other NEDC options, including Marine Corps facilities. In addition, we are reviewing commercial hosting options. As we anticipate growth and project forward, SPAWAR's chief engineer is developing the technical architecture for data centers. Part of this will determine the optimum lay down of Navy data centers, while also taking into consideration various technical factors, such as connectivity, people, power usage and data center location in relation to the customer. At that point, we can make some recommendations as to where we think the centers should be located. I expect the number of data centers will grow in some amount as a result.

Q: Are any figures available yet as to how much money the Navy anticipates saving with consolidation?

A: The short answer is: not yet. However, there have been some improved projections about savings. We are taking a look at some of the sites that were closed in FY12, the applications that are hosted today, and doing a comparison of the before and after hosting costs. When the applications were hosted at their old data centers, the site often did not keep data on exactly that one application, running on one server, sitting on one rack, located in one room. The [owners of the] site didn't know how much money it cost to run that one application. They were running several; not just one. We have to go back and estimate what the cost was for individual applications running on the old system, and do some analysis while it runs in our data center today, so that we can get a better estimate of cost savings.

There are some models available that can tell us what we should be saving. But it is kind of like the car mileage estimates we get from car manufacturers. There are

a lot of variables. Metaphorically speaking, I want to get some of those actual mileage estimates so that we can get a more accurate picture. In doing that, we can also help the modelers by telling them this is a better set of models and whether they are doing it right or not.

As other federal agencies have discovered — and the U.S. Navy is no different — accurately measuring cost savings is an extremely challenging effort. With our sites providing a computing environment, security and support services at an enterprise service rate, we hope to have a better understanding of what the hosting costs for consolidated systems will be. We are collaborating with the legacy data centers to gain an accurate characterization of the current operating costs, so we can determine actual cost savings. Moving forward, we are developing a good cost baseline from which to measure our efforts, so I anticipate we will have a better understanding of what our savings are in the near future.

Q: Have there been any technical challenges or glitches in the effort so far? Anything that wasn't anticipated but that was dealt with immediately to keep the effort on course? Do you foresee any technical challenges as you step into this new position?

A: Some of the technical challenges we are experiencing include trying to characterize the health of the applications that we are moving over. We are using a red, yellow, green status approach. Applications are green if they are modern, running smoothly, have security patches installed, everything is current, and it is just a matter of moving the application from one hosting environment to a more efficient environment. Then you have other application categories that are older and may need a more current operating system or security patch, or more engineering to clean them up a bit. If an application is in what I categorize as the red zone, the application may not be able to be moved.

The challenge occurs if I lay out a transition schedule that assumes a certain mix

of some easy, moderate and hard (green, yellow and red), but we do not see the full picture until I am well into transitions. At that point I may see a skewed picture of more yellow and red systems, in which case it starts to affect the overarching schedule. It is at that point that you begin to comprehend the difficulty of the task at hand and what impact it will have on perturbing the schedule.

Technically, however, the consolidation effort has been fairly straightforward. We documented quite a few of the lessons learned in FY12, so that our transition teams can draw from this year to refine our standard operating procedures. The certification and accreditation piece, and ensuring all the system security documentation was in place, was more time-intensive than originally planned. We spent a lot of time working to expedite the process without sacrificing security precautions. One of the significant lessons learned was the importance of engaging with our customers and stakeholders. We were able to see the need to keep them informed of our process and progress. We will continue to conduct site visits to most of the legacy data centers to meet with their leadership, address any concerns and gather feedback on the process.

Q: Have any green techniques and technologies being incorporated into the strategy to manage and minimize the Navy's carbon footprint?

A: We received funding from the Office of Naval Research to evaluate new technologies that can make the data center more energy efficient. One is a smart metering technology for our data centers in Charleston, New Orleans and San Diego. This technology enables the Navy to understand energy use, identify improvement areas and track energy consumption. The second project is a new self-cooling technology for servers. This technology is the size of a placemat that is placed directly on servers to cool them, rather than cooling all of the surrounding air. This is much more efficient than cooling the entire room. We are definitely trying to determine what drives

"We are definitely trying to determine what drives our cost, such as power and cooling. Prior to consolidation, a site may have metered power for the whole data center room and now we have technology that allows us to monitor our power and cooling better. I can cool more locally and that is certainly a big savings."



Data center facilities manager, Bobby Nutting, examines color-coded wires which replaced more expensive copper wires, at the NEDC San Diego.

our cost, such as power and cooling. Prior to consolidation, a site may have metered power for the whole data center room and now we have technology that allows us to monitor our power and cooling better. I can cool more locally and that is certainly a big savings.

Q: How will you measure success?

A: We will measure our success by how well we efficiently and effectively consolidate legacy data centers and maximize the Navy's return on investment. Transition progress will be tracked by reporting on metrics for site consolidations and system and server transitions. That level of detail will enable us to more fully understand the scope of our efforts. Another metric we will be tracking will be the percentage of savings in sustainment costs, which is the difference between the previous cost to host systems and how much it costs post-consolidation.

Another part of return on investment is the reuse of software and hardware. Our office is implementing processes that will

capture cost avoidance through the reuse of assets in the enterprise data centers and in offsetting new IT purchases across the Navy. I also want to track the number of physical servers that were virtualized, so that we can ensure the 'right-sizing' of existing applications and reduce the physical footprint required to sustain Navy applications. These metrics will provide leadership with a rounded picture of how well we are succeeding in our mission to consolidate the Navy's data centers.

This is a challenging job, and success isn't going to be easy. Now that the NEDC sites are up and running, we're already seeing enhanced security, efficiency and reliability. Data center consolidation isn't something we can succeed at with just a couple of years of effort. There are enterprise behaviors and results we are trying to achieve, and I think we are getting there a step at a time. ●

TINA C. STILLIONS is with the SPAWAR HQ public affairs office.

LISA HUNTER provides strategic communications support to SPAWAR's Data Center and Application Optimization office.

Rear Adm. Samuel J. Cox Director, National Maritime Intelligence-Integration Office Commander, Office of Naval Intelligence

As part of the Naval Intelligence realignment, Rear Adm. Samuel J. Cox, assumed command of the Office of Naval Intelligence (ONI) Nov. 30 and Director, National Maritime Intelligence-Integration Office (NMIO) Dec. 10 in separate ceremonies at ONI headquarters in Suitland, Maryland and the Office of the Director of National Intelligence in Washington, D.C.

The National Maritime Intelligence-Integration Office is the unified maritime voice of the United States Intelligence Community (IC). It operates as an IC "service of common concern" to integrate and streamline intelligence support, providing a whole of government solution to maritime information sharing challenges. NMIO neither collects nor produces intelligence. It breaks down barriers to information sharing and creates enabling structures and cultures to set the conditions for maritime partners to optimally share data.

NMIO works at the national and international level to facilitate the integration of maritime information and intelligence collection and analysis in support of national policy and decision makers, Maritime Domain Awareness (MDA) objectives, and interagency operations, at all levels of the U.S. government. Its goal is to enable maritime stakeholders to proactively identify, locate and track threats to the interests of the U.S. and its global partners.

Established in 1882, ONI is America's longest continuously operating intelligence service employing world-class analysts, engineers, technicians, leaders and managers. Consequently, ONI maintains a position of unparalleled leadership in the collection, analysis and production of foreign naval scientific, technical, geopolitical, and military intelligence, as well as transnational civil maritime intelligence.

ONI employs approximately 3,000 military and civilian Intelligence professionals including active and Reserve officers and enlisted Sailors and Marines and contracted personnel at the modern National Maritime Intelligence Center facility in Suitland, Maryland and at other strategic locations around the world.

Cox's previous flag assignments included head of the Multinational Intelligence Task Force investigating the sinking of the Republic of Korea warship Cheonan. He was a senior member in the Afghanistan-Pakistan Hands program, and director of Plans and Policy (N5) and Fleet Intelligence for Naval Network Warfare Command. Rear Adm. Cox most recently served as the Director of Intelligence (J2), U.S. Cyber Command.

Q: With the recent Naval Intelligence realignment, what is achieved by the end-state and what are the effects on NMIO and ONI?

A: From my perspective, the impact on the National Maritime Intelligence-Integration Office and the Office of Naval Intelligence is actually not going to be that great internal to these organizations. The N2/N6 realignment will have a significantly greater impact on the OPNAV staff. If you look at the Deputy Chief of Naval Operations for Information Dominance Vice Adm. Kendall Card, who is also the Director of Naval Intelligence and Deputy Department of the Navy Chief Information Officer for the Navy, he has quite a bit on his plate — [he wears] several different hats. Over the last couple of years there



Rear Adm. Samuel J. Cox

has been a minimal presence of senior intelligence professionals on the OPNAV staff. This reorganization fixes that with the creation of the Deputy Director of Naval Intelligence and also the assignment of a one-star naval intelligence flag officer to the OPNAV staff as basically the CNO's intelligence briefer, all of which should be a big help to VADM Card.

NMIO is a little bit different in that the organization is essentially administratively supported by the United States Navy with a memorandum of understanding with the Director of National Intelligence to serve as a service of common concern to the broader national maritime intelligence community, which we can define later in greater detail, but it is a very wide range of government and non-government, including federal, state, local, tribal and territorial governments, as well as commercial, academic and foreign partners, who all have a stake in maritime intelligence. But NMIO takes its direction from the Director of National Intelligence, and the Navy is just providing this service.

The money for NMIO, if you trace it back, comes from the national level. Essentially, National Intelligence gives the Navy money to do a variety of things, one of which is to run NMIO in support of National Intelligence requirements. So

NMIO will keep doing what they have been doing for the last four years since the organization stood up. As we do that mission we get better at it. As the connections with the rest of the Intelligence Community and our maritime intelligence partners get better, the mission just continues to improve.

Meanwhile, ONI is the source, or essentially the engine, for the Navy to produce intelligence for the Navy and maritime domain. It supports naval intelligence requirements, which, in turn, supports joint warfighting. But the analysis in ONI is the same analysis that informs the NMIO piece. So we actually get efficiencies by not having different analytic organizations that have redundancies or overlaps. We avoid that by having the national organization construct, NMIO, stay very small, very lean, kind of senior, focused on policy and maritime intelligence integration while ONI continues its traditional role of collecting, processing and analyzing large amounts of intelligence all for the purpose of achieving a decisive warfighting advantage for the U.S. Navy.

Q: NMIO and ONI are separate organizations with one leader. What are the synergies between them, and what are the principal differences?

A: The synergies are that I'm dual-hatted, I'm the commander of ONI and the director of NMIO and the initial savings is that I have one instead of two aides. Other than that they are separate and distinct organizations, but we are in the same building so there is extensive coordination and communications between the two entities, and that has been ongoing for a long time. It's less awkward now in the sense that since I control both organizations, when it comes to setting the priorities for whatever type of analysis is going to be done, I only have to argue with the guy in the mirror. That actually results in significant efficiencies and we avoid redundancies. The principal difference is the mission focus of each organization. NMIO is focused on a very broad, inter-agency government, commercial, foreign set of customers, where ONI is focused on support to the Navy. But having said that, ONI's analyses frequently gets incorporated into the president's daily brief. But essentially, whether it goes from ONI via a National Intelligence production cycle or via NMIO, it is the same source of the analysis. So we don't have any duplication or organizations fighting or competing with each other.

In general, ONI is very much focused on the warfighting requirements of the United States Navy, and NMIO is focused on, I would characterize it as, more on the security of the United States and our allies with a very strong homeland security flavor. But NMIO also focuses on other topics, for example, Somali piracy, which remains a high interest item for the National Security Staff. It is not something the Navy focuses a lot of time and energy on from an intelligence perspective but from a national requirement it is very high. So NMIO has the lead in coordinating with ONI and Coast Guard and other foreign organizations around the world to make sure we get the best product to the national security staff. Mostly, it is about the number of people doing the mission. NMIO has about 40 people total and ONI — when you add everything up, including special communications

The National Maritime Intelligence-Integration Office is the unified maritime voice of the United States Intelligence Community.

– <http://nmio.ise.gov>



centers and Reserve units — gets to about 3,000.

Q: Regarding NMIO and the Global Maritime Community of Interest, can you please describe the community's stakeholders and recent successes?

A: Yes. The Global Maritime Community of Interest, the acronym is GMCOI, is comprised of whoever has a need for intelligence and information to support security. It includes U.S. federal, state, local, tribal and territorial governments; the global maritime industry; academia; and our foreign partners. All of these have their unique maritime perspectives and requirements. NMIO's task is to facilitate collaboration and information sharing. It's right in our title, the integration of information. NMIO does not have authority to compel anyone to do anything. It is entirely a collegial work-together organization to identify common concerns and issues and find the most efficient and cost-effective solutions that help the greatest number of customers.

If you look across the U.S. government, for example, there are many organizations that have an important interest in maritime security. But within their particular organization, the maritime piece tends to be frequently relatively small and under-resourced. In the past, before NMIO was stood up, all these different smaller maritime organizations were pretty much on their own in trying to get national-level intelligence support. With the creation of NMIO and our ability to reach out and work with all of those folks and establish common requirements, we can go to the National Intelligence level with a much stronger position that will support a broader range of customers rather than every man for himself — which is how I would characterize it before NMIO.

In many cases, these maritime organizations were under-resourced, out of sight and out of mind from the primary mission of their parent organization, and they weren't effective in breaking through the bureaucratic impediments within their organizations. Now they have access without circumventing their own chain of command. Because we don't have the authority to compel anyone to do anything, we are not a threat to other organizations' budgets. This actually results in a much more effective approach to intelligence support to maritime security for the United States and its allies because we are viewed as an impartial source of maritime intelligence expertise.

Q: What is your vision for the NMIO-ONI dual-hat directorship? What do you most want to achieve while in this historic position?

A: My primary purpose right now is to stop the constant reorganization and put my foot on the accelerator and let people actually get some things done. There is a lot of work that has taken place in getting NMIO up and running and off the ground. Anytime you establish a new organization in the Washington bureaucratic environment, particularly one that I would define as working for the common good, as the saying goes, the common good has no resource sponsor. So it's very susceptible in the early stages to being strangled in the crib from a bureaucratic perspective. NMIO has done a lot of work with getting up and organized and getting the right alignment. There have been a couple of changes that had to be made over time, but I think it is about right now so the intent is to move forward rapidly.

The end state, if I can be very blunt, is for NMIO to do everything we possibly can to ensure that there is never a 9/11 that originates from the maritime environment. If I can put it in the basest possible terms, it is mostly about homeland security, counterterrorism and counter-proliferation [of weapons of mass destruction, illegal firearms and narcotics]; those are the main focus areas for NMIO.

For ONI, the bottom line is to know the enemy and potential enemies and the intent is to create a decisive warfighting advantage for the United States Navy. We do that primarily for ONI at the strategic and operational level to understand current enemies and potential future enemies and inform our acquisition and organizational processes so we have the right resources to conduct our operations, and from an information advantage to make sure we have not been surprised by anything — including potential adversaries operating in the maritime domain.

Q: **The Intelligence Community has an interesting strategy to "move to the cloud." Would you describe ONI's involvement in transitioning to the cloud concept and the effects for Naval Intelligence?**

A: ONI is definitely moving toward the cloud. That is our intention, and we have been working with both ODNI, the Office of the Director of National Intelligence, and the National Security Agency to move in that direction. Having just come from a year and half at U.S. Cyber Command and Naval Network Warfare Command before that, which has now evolved into Fleet Cyber Command, my view is that from the enhanced security perspective alone it is enough of a compelling reason to move toward the cloud. There is also the promise of resource and personnel resource synergies that will result in savings in going this way. I've been around long enough not to cash that check yet; although, I think eventually we will be able to achieve those savings.

But the security aspect is critical. The other piece is that by going to the cloud it allows much greater ability for all the intelligence agencies to be able to quickly share a wider range of data that will enhance everybody's ability to do analysis and still be in a very secure environment.

Some of the difficulty is that in order to share data, there is a lot of up-front work that has to be done to tag data so that you have the classification, security and declassification in each discrete

The Office of Naval Intelligence is America's premier maritime intelligence service and a core element of the U.S. Navy's Information Dominance Corps.

—www.oni.navy.mil.



piece of data so that it all can work effectively within the intelligence cloud. Another challenge in going to the cloud is that while there is the promise of future savings projected, there are up-front costs in getting there. At the same time, you are trying to sustain legacy systems that in many cases are costing more and more to maintain but you don't have the option of stopping them until the cloud gets going. Many of these databases are supporting ongoing warfighting and they have to work until the cloud is up and running. It causes a significant budget crunch in the short term. So trying to get the money to make the transition so you can achieve the savings down the road is a significant challenge.

Q: **Have you been given a timeline to complete certain parts of the process to move to the cloud?**

A: We have been working with an I2 prototype effort with ODNI's pilot cloud, and without getting too much into technical terms, it involves getting maritime intelligence into a data cloud that can be combined more rapidly with information from other agencies. The term for this is *ghost machine*; our part of this is projected to be up and running in March 2013. In terms of when we all get to the cloud, I don't know of any specific task and timeframe that we are required to do that. My direction to the folks at ONI is that my intent is not to be at the cutting-edge of IC's transition to the cloud, but I don't intend to be the guy lagging behind last either. I want to be in the sweet spot of where we learn from the experiences and mistakes of others but I don't want to be the last one to get on board the train.

Q: **How do you envision the realignment in Naval Intelligence and bringing together the diverse expertise from the intelligence, information professional, information warfare, meteorology/oceanography and Space Cadre communities will help leverage all the talent of these disciplines and provide the best support to Information Dominance, and ultimately Navy warfighters? What will be the ultimate benefit to warfighters?**

A: I'm a big believer in the information dominance concept and the community that we developed. There is great synergy that occurs by having the intelligence professionals in the same community as the information professionals, Space Cadre, oceanography and metrology professionals in one team. It works especially well at the force provider and man, train, equip level.

There are issues at the tactical warfighting level. If I could just back up a little, each of the communities within the Information Dominance Corps brings critical expertise that operational commanders require to fight. When you look across the 21st century, the drive is to increase specialization but also have the ability to quickly network those specializations into a common product.

So our challenge on the intelligence side is to supply people who report to the operational commander who are no-kidding experts at intelligence and not having to spread their expertise too broadly too soon in their career and, therefore, not be particularly good in any one area. The idea is that up until the time someone has completed their commander O-5 level, we call it a milestone, but you can think of it as a sea tour within the intelligence and IDC community, and then after that we start branching out more to do cross-detailing and cross-pollination of the skill sets. If we do it correctly, it works. It makes the acquisition processes for all this a lot better. We will also improve the ability to do warfighting at the tactical level.

But in some instances, you can have too much of a good thing so this has to be done very, very carefully and not lose the expertise that results in another layer of generalists. In many respects, historically, the Intelligence Community believed it wasn't very well supported by the naval communications community. The communications officer had a whole other set of problems and intelligence wasn't viewed as one of them. So the result was that over time independent stovepipe intelligence networks were created to move intelligence from one place to another because the regular communications systems couldn't handle it.

With the IDC, intelligence and communicators are in the same boat now. So we can solve these problems from the get-go, from the very beginning of the systems acquisition process and not try to do Band-Aid [fixes] later in a warfighting environment. So from that perspective alone I think there is a heck of a lot of benefit that will result in operational commanders getting much better support to do their mission.

Q: The IDC is a couple of years old now. Do you think operational commanders in the fleet recognize the benefit?

A: That's a good question. I would say right now it's mixed. A number of operational commanders do, then some will ask the question: "What's broke that needs to be fixed?" Others say we need to radically change. So we have the whole spectrum of views. I think what will happen over time is that the IDC will have to prove the value added that it brings to naval warfighting. Then as the commanders become convinced that this is the right model, and again I would state that the IDC organizational structure at the OPNAV force provider, man, train and equip level and the IDC structure at the tactical warfighting structure won't and shouldn't be the same. They need to be tailored to support those particular levels of war. If we do that correctly, the operational commanders will then see the benefit and become believers.

Certainly the senior leadership right now clearly recognizes

the information domain and C4ISR as a critical warfighting pillar. It's not support, it's not tail, if fact, if you look at the tooth to tail argument, I would argue that we don't fit into either, we are the eyeball and ear and part of the brain. Some of the debate is over the fact that it's critical to every warfighting area, so the air warfare commander, surface warfare, subsurface, all have an important stake in the things that the IDC does and how well this pillar works and integrates with the other domains of warfare. So those are all the things that will have to be worked out very carefully, trained and exercised over the years to make it all work.

Q: Beyond the organizational and personnel changes, will there be changes in roles and responsibilities, changes throughout Naval Intelligence and in doctrine as well? How important are unmanned platforms in the changes?

A: The realignment results in some organization changes but the fundamental building blocks of Naval Intelligence are still essentially the same. Particularly from ONI's perspective, we go from Echelon II to Echelon III, but other than that ONI is still the same as it was before except with the enhanced capability of a two-star being able to get into more decision-level meetings than the previous commanders did as an O-6. That will be a big help. It's also a signal to the IDC, the Intelligence Community, and to the operational community that the Navy is placing increased significance on this organization by having a two-star flag officer in charge of it.

I don't think there will be any big changes in doctrine. In many respects, Naval Intelligence, and any other intelligence, has been recognized for 2,000 years as being critical to successful warfighting going back to Sun Tzu. You can change the titles, but it still comes down to knowing the enemy in sufficient time to act. That's the essence of what we do.

As to unmanned platforms, they are going to have a big impact in the future. I would argue that the use of the term 'unmanned' creates a very false impression on people. I would prefer to call them 'remotely piloted' but in terms of unmanned platforms there is a big investment in TPED, tasking, processing, exploitation and dissemination, that's the term we use. As there are more of these platforms with more and more capability, you get inundated by information and intelligence that you don't have the manpower or the systems to adequately process so that back-end piece of it is actually a pretty significant investment in order to be able to take advantage of the increased capabilities that these supposedly unmanned systems bring.

Frequently, those exploitation pieces are not initially factored into acquisitions. They are viewed as an afterthought and someone will come up with a way to do this. But when you look at the vastly increased data that comes in, and it is not a trivial problem, and it's not as though you can have an IS (intelligence specialist) look at 10 screens instead of two and expect that he is actually going to be able to detect something of significance in time. That is the significant challenge because that costs a lot of money in either getting the systems and automation right or to

"ONI is a national treasure with some of the most extraordinarily capable, dedicated, experienced analysts that you would ever find in the United States Intelligence Community. In some areas, like acoustic intelligence, as an example, nowhere else on the globe can anyone come even remotely close to what this organization can do in that domain. The folks who work here do incredible service to the nation and to the Navy."

be able to compensate for not having enough people or getting enough people if the automation isn't where you need it to be. So that back-end TPED piece is still a very significant and critical problem.

Q: You recently completed a tour as the Director of Intelligence (J2) of the U.S. Cyber Command. What role do you see ONI playing in supporting cyber warfare? Do you anticipate any other changes in Naval Intelligence when the Defense Department releases the rules of engagement that will govern military action in cyberspace?

A: Let me start from a general perspective. Whether you are supporting air warfare, surface warfare or cyber warfare, the primary purpose of intelligence is to penetrate as deeply into an enemy and potential enemy's research and development, training, education and their acquisition process so that from a strategic sense we know long in advance what they are going to do before they do it. The same principle applies at the operational and tactical level as well. The same thing is going on in the cyber domain to penetrate adversaries' research and development in cyber before they develop the tools so that we can have countermeasures in place before we get hit.

Cyber is particularly challenging in warfare because of the speed in which things happen. Because if you don't have this advanced understanding of what the enemy's going to do to you well before they do it then you have almost no hope of doing actual defense because it all happened too fast. For human recognition of the problem, in many cases, it is too late. From the Navy's perspective, we are as dependent as anyone else in DoD on networks and the Internet to do our work and our business. So defending Navy networks from cyber-attacks is critical. So we have a significant role in the intelligence to enable those in the Navy who defend those networks to have advance warning of what's going to happen before an enemy can do it.

I don't want to talk in an unclassified forum about the offensive side other than to say that there is a lot of work to be done to prepare for those kinds of operations and it's not a matter of you want to do them or not, or intend to do them or not, it is just the things as military professionals you have to do in order to be ready should the call ever come to do something like that. So we will be engaged in that. There are other organizations; the National Security Agency is by far the nation's premier place that has the capability to do the intelligence collection and exploitation to support cyber warfare. Our intent is in no way to dupli-

cate anything they are doing, but to focus our efforts on those specific threats to Navy networks, as well as specific things that Navy cyber capability could be used for supporting other warfare domains.

It is a huge task and we are just getting started with a new department called Spectrum at ONI's Nimitz Operational Intelligence Center. They don't do strictly cyber; they do the full range of non-kinetic warfare intelligence, which is consistent with how our potential adversaries are organized to do this. Many of our adversaries don't stovepipe cyber into a separate thing but rather the broad range of EW (electronic warfare), C5ISR (command, control, communications, computers and combat systems intelligence, surveillance and reconnaissance.) So, as our purpose at ONI is to understand the enemy, we organize the way they do because it is a better way to understand what our adversaries are going to do. Nevertheless, there is a lot of work that will go into the cyber piece to generate the intelligence Navy forces need.

Q: Defense Secretary Leon Panetta has repeatedly discussed America's cyber vulnerability. He warned that the U.S. faces a catastrophic attack if its digital defenses are not strengthened, but some have accused Mr. Panetta of exaggerating such a threat. Since military networks ride on the publicly controlled Internet, does the possibility of a crippling attack concern you?

A: Yes. Two things. Secretary Panetta is definitely not exaggerating the threat. In fact, I think if people could see the classified data they would be very, very worried. Now having said that, there are issues that adversely affect the way people view this and one is the sloppy use of the term attack. There is a tendency to view everything that happens in cyberspace as an attack. The reality is that most of it is nuisance activity, and then a big chunk is criminal activity, and the thing that affects us most now is espionage activity via cyberspace which is an extremely serious threat. As you go up the threat spectrum, you get to disruptive attacks which are using botnets and things to disrupt. They don't actually destroy anything, but if the disruptive event is large enough it could have a serious impact.

Then you have those cyber events which are actually destructive, either they destroy significant amounts of data or they cause a kinetic effect on computers by turning off power or causing machines to explode or go into asymmetric vibration and be potentially lethal. Those destructive types of events are extremely rare but the disruptive ones are increasing. For example, we say



The National Maritime Intelligence Center, located in Suitland, Maryland, is home to the NMIO and ONI, and its four Centers of Excellence: the Nimitz Operational Intelligence Center, the Farragut Technical Analysis Center, the Hopper Information Services Center and the Kennedy Irregular Warfare Center.

in the cyber world those “attacks” are increasing by a very large amount, but people see life goes on so what is the big deal? What we are, in fact, worried about are those events, which so far are extremely rare, but have the potential to be extremely damaging.

To be able to shut down the world’s Internet, that’s not going to happen. Turning off the power to the entire United States, that’s not going to happen. But well within the realm of possibilities are smaller things that if coupled with, for example, a sophisticated information operation — a psychological campaign — could have profound effects. You’ve seen in the press, attacks on Wall Street businesses. If those were to get effective enough to cause an uncontrolled run on the banks, that would have potentially devastating effects on the U.S. economy. A low-end, unsophisticated attack could have a psychological effect that would have very profound impact. Or even an attack that could shut off the power to lower Manhattan for a short time could have a profound impact. The economic disruption is immense.

Turning off traffic lights in a major metropolitan area would result in people being killed. You could easily have a cyber-event that could have a disruptive and political impact on the scale of [Hurricane] Katrina. It may not result in deaths but it could have a serious, serious effect. The threat is only accelerating right now. So the dangers from these destructive and disruptive events are increasing at a very rapid rate.

Q: **It is very shocking to read in the press that emanations and eavesdropping can still occur even when a computer is turned off when the previous thinking was that a shut-down computer is safe.**

A: The things that can occur in cyberspace would blow most people’s minds. Just because you think your computer is off and that camera is off, and it may look like it is off, maybe it is not. People need to be very, very concerned about that. They also need to be concerned about the role of oversight. Many countries around the world that have this capability are using it to track and oppress their own people. So those people who are concerned about their liberties have every reason to be, and it’s critical that our nation gets the oversight piece right. So that we can be both effective in the speed to operate in cyberspace, but yet still truly protect the liberties of the American people.

Gen. Alexander (Commander, U.S. Cyber Command) very much dislikes the idea of balancing the security requirements of cyber versus the civil liberties requirements because it implies that you have to sacrifice one for the other. In his view it is like rails on a train track, you have to do both or else it doesn’t work. Those are important issues and very difficult ones with legal issues [to consider].

Q: **Is there anything else you would like to discuss about the important Naval Intelligence changes?**

A: I would just add that NMIO is a relatively recent organization that is doing great and critical work that is really a new endeavor. In many respects it is a ‘herding cats’ job, but it is work that has to be done if we are going to close up the seams to protect our nation from threats from the maritime domain.

ONI has been around for a very long time. The name has existed for a long time. The actual organizations that were called ONI have evolved over time. Obviously, I’m the commander so I am a bit biased, but ONI is a national treasure with some of the most extraordinarily capable, dedicated, experienced analysts that you would ever find in the United States Intelligence Community. In some areas, like acoustic intelligence, as an example, nowhere else on the globe can anyone come even remotely close to what this organization can do in that domain. The folks who work here do incredible service to the nation and to the Navy.

Frequently, it is unsung because what we produce gets briefed by other people and other organizations but the actual creation of the intelligence used in many, many places occurs here. It is very difficult because you just don’t turn the knob on the intelligence mission and intelligence pops out. These folks look at the chicken bones and the bits and pieces, and, in many cases, it’s essentially deceptive data because we are dealing with a thinking adversary that is trying to fool us. We are very good at looking through that and presenting to the Navy a pretty clear picture of what the future threats are going to be in time for the Navy [to respond].

I’m doing what I love with people who are a dream to work with. ●

Capt. Tim Gallaudet Ph.D.

Superintendent, United States Naval Observatory

Capt. Tim Gallaudet assumed duty as the 53rd Superintendent of the U.S. Naval Observatory Sept. 8, 2011. He graduated with distinction from the U.S. Naval Academy in 1989, receiving a Bachelor's Degree in Oceanography. He received a Master's Degree in Oceanography from Scripps Institution of Oceanography in 1991. After receiving a Doctorate in Oceanography from Scripps Institution in 2001, Capt. Gallaudet reported onboard USS Kitty Hawk (CV-63) which supported Operations Enduring Freedom in 2001 and Iraqi Freedom in 2003, for which he was awarded the 2003 Commander, Naval Air Forces Leadership Award. For Gallaudet's complete biography go to the USNO website: <http://www.usno.navy.mil/USNO/tours-events/ChangeOfCommand2011Release.pdf>.



Capt. Tim Gallaudet

Q: Can you talk about the USNO's mission and the services it provides to the Navy and public at large?

A: The United States Naval Observatory's mission is to provide astronomical and timing data that is essential for accurate and effective navigation, command and control, communications, targeting, and operation of space and cyber systems. USNO's operations are vital to the Navy and Department of Defense, the Intelligence Community (IC), other government agencies, and the public at large.

USNO's mission of Precise Time and Astrometry (PTA) is really part of the key infrastructure upon which DoD operations are built, and USNO is the only organization with the mission to provide PTA. The interesting thing about infrastructure is that most people take it for granted, until it's degraded or gone — just talk to the people recently hit by Hurricane Sandy.

Q: Does the GPS and time data that the USNO provides interface with the Navy navigation system?

A: Yes, it does. Are you familiar with ECDIS, Electronic Chart Display and Information System? Our ships that use the electronic charting system currently receive their

time through a ship's internal navigation system called NAVSSI (Navigation Sensor System Interface); it is in the process of transitioning to the GPS Positioning, Navigation, and Timing System (GPNTS). Their time is provided primarily by the GPS constellation through an onboard GPS antenna. We provide that time to the GPS constellation.

Q: So any Navy system that uses GPS and time data, for example, combat systems and Navy networks, rely on data provided by USNO, and it doesn't matter which vendor developed it or what system it is?

A: Yes, and that is the Defense Department policy. There is a Joint Chiefs of Staff Instruction and an OSD CIO instruction that directs the department to use our time and directs us to provide the time as the authorized provider of DoD time, and that is for all the services.

Q: As the official timekeeper for the Defense Department, can you explain the concept of an atomic clock? How do warfighters use the precision time data that USNO provides?

A: Our atomic clocks are based upon the fact that atoms such as cesium, hydro-

gen and rubidium are composed of electrons that have spin, and that spin can be aligned with their nucleus's spin in more than one way. As the electrons switch between different spins, they give off or absorb a very precise amount of energy. By a law of quantum mechanics, the energy can take the form of microwave radiation whose frequency is directly proportional to the energy (via Planck's constant). We measure the frequency of these microwaves. Once we know the frequency, it is a technologically simple matter to compute time.

In practice, the atomic microwave frequencies are converted to a 5 MHz signal, which is an electric signal that goes up and down five million times a second. Then we feed that signal into equipment that is designed to output a voltage spike every five millionth time the 5 MHz signal goes up. The rising edge of that spike signals the start of each second — to an accuracy of a billionth of a second.

Our Master Clock is actually a system with dozens of independent free-running atomic clocks. In any given system the more independent numbers or elements you have in the ensemble, the better the information you get when you average them; that's why we have so many clocks. We have different types because each type of atomic clock has a different characteristic. Clocks that use the cesium

atom are very noisy on the short term but very stable on the long term, always centering around the correct average time. Another type of clock we employ uses hydrogen and has very low short-term noise but in the long term it tends to drift off, so we use a balance of different clocks with different characteristics to produce what is called an operational time scale.

We've also just added four new clocks, with an atom called rubidium, which are the most precise operational clocks in the world. We designed them ourselves primarily because the GPS III program, the next GPS system, has a more stringent time requirement, which is precision to a nanosecond, which is a billionth of second. So to meet that requirement we had to build our own clocks; we just reached initial operational capability this year. We call them the Navy Rubidium Fountains (NRF).

Many of the world's labs that provide time don't run continuously, but because we have a Defense Department requirement, our clock system is always operational, 24/7, always online, and it is the most precise operational clock system in the world. Warfighters use the precise time we provide them for communication systems, command and control systems, intelligence operations, network operations, and data fusion.

Q: There have been a lot of press reports lately about hackers being able to spoof or hack GPS data; I imagine your security is very stringent?

A: It is, and that is the purpose of the new GPS III program. We participated in the development of the monitor station receivers for this system because of our expertise in timing technology, through which we monitor time of the GPS network. The new signal that GPS III will use is more robust to jamming. In terms of computer hacking into the system or the vulnerabilities of GPS, I can say we are making efforts at a DoD level to reduce those vulnerabilities.

Another interesting thing — GPS operates through a system of satellites that transmit radio signals to the user's

receiver where a trilateration is performed to determine a position based on the time difference of arrival of those signals. The signals are electromagnetic waves that travel at the speed of light. The speed of light travels about a foot [in one nanosecond], so if the precision of our clocks is within a billionth of a second, that provides for the theoretical positioning accuracy of one foot.

For any kind of positioning and consequent targeting applications, if you want to be accurate within a small area, precise time is important. The same goes for any kind of communications or command and control, whether satellite, sea or shore based: to communicate effectively, a source and a receiver must be synchronized. When you lose synchronization, you lose 'comms.' The term is drop sync; that's the frequent reason why a shipboard radio, for example, might lose comms — whether through an error or signal delay or loss — and why precise time is so necessary to maintain continu-

ous communications. The same goes for computer networks too.

Q: Speaking of atomic clocks, the U.S. Army Research, Development and Engineering Command is developing miniature atomic clocks to be used by Soldiers. Is the USNO playing a role in this development? Are they used in the Navy?

A: We call these Chip Scale Atomic Clocks. We have assisted OSD and DARPA (Defense Advanced Research Projects Agency) in preparing their program, in evaluating the development proposals, and in measuring progress. USNO has also been involved in measuring the performance of CSAC technology against the master clock. Since then we have consulted for other DoD groups in specific implementations. They aren't used much operationally in the Navy now but much research is being done. They are not as accurate and precise but at a tactical level



The Navy Rubidium Fountain Clock No. 3, one of four such devices that are now part of the Master Clock system. This device and its companions are the most precise clocks currently operating in the world. All USNO photos by Geoff Chester/USNO public affairs officer.

(for the dismantled Soldier or SEAL team member) they may meet certain applications and that's why a lot of research is being done.

The Army and Navy labs are looking at them, and we have advised them both. We have a team of atomic physicists and engineers that work in our time department that have been asked about performance standards and certain research issues.

Q: USNO's website states that "the highest precision and accuracy in time dissemination is provided through Two-Way Satellite Time Transfer (TWSTT)." Can you explain how the two-way time transfer method works?

A: The idea is that we send time signals up to a geostationary communications satellite, which retransmits them to the user in the field. The user simultaneously shoots time signals towards us. Because the two signals travel over the same section of sky and ionosphere, the atmospheric distortions are almost the same each way. Therefore they cancel, and that makes it easier to compare our clocks with the remote clocks so as to keep users on time.

To put this in context, we begin with our master clock that keeps precise time. But we then have to disseminate that time to users. We have several ways of disseminating time that vary with respect to accuracy. Some of your readers might remember dialing the number for time on rotary phones several decades past. We still provide a telephone time dissemination service that about 60,000 customers use each week. That is only accurate to a fraction of a second. Then there is Network Time Protocol (NTP), accurate to about 1 millisecond, for dissemination to DoD computer networks.

Dissemination via GPS is the most prevalent means used globally by our forces, with an accuracy of about 10 nanoseconds. The most accurate is TWSTT with nanosecond level accuracy. Our customers within the Intelligence Community use this form of time dissemination.



The USNO 26-inch "great equatorial" refracting telescope is located on the grounds of the U.S. Naval Observatory in Washington, D.C., and it is included as part of the Monday night tour when skies are cloudy.

Q: The "great equatorial refracting telescope" was first used in 1873. What updates have been made to this telescope? Does it work exactly the same way as it did when it was first built, aside from the added cameras?

A: The telescope is interesting. It is the oldest piece of Navy operational equipment still in commission. Of course, you have the USS Constitution in Boston — but that historic vessel is not really operational — it doesn't deploy and lacks modern combat capability.

This telescope has been used for Navy astronomical needs and data collection since 1873. Then it was the largest telescope in the world. A number of great discoveries have been found with it, including the two moons of Mars by a USNO astronomer.

A major update of the telescope was performed back in the 1890s when the USNO moved from the Foggy Bottom area of D.C. up to our current location in Georgetown Heights. Of course, the telescope has been periodically refurbished since then, but you are correct, to a large extent the telescope works in much the same way it did when it was first built.

However, the real heart of an astronomical telescope is the device at the end of the telescope that records the focused

image. Initially USNO astronomers used their eyes and notebooks to record what they saw through the telescope. Photographic film was used with great success with the 26-inch throughout the years, and had the advantage that film is more sensitive to light than the human eye.

Currently, we use a high speed digital camera with the 26-inch telescope and utilize a technique called 'speckle interferometry' to compensate for the blurring effect of the Earth's atmosphere. One interesting aspect of the science of astronomy is that a very old telescope like the 26-inch, when coupled with a modern camera, produces a cutting-edge instrument. NASA did the same thing with the Hubble Space telescope, performing several servicing missions to replace and modernize Hubble's cameras, providing new and exciting capabilities in a very cost-effective manner.

Although it looks like a late 19th century piece of equipment (because it is!), and it is not like some of the state-of-the-art telescopes that we have in our dark-sky Site in Flagstaff Arizona, it still remains relevant. It has a great lens and we still use it to collect bright star data for catalogs used by Trident missiles to navigate.

What is a star catalog and why does DoD care? To explain, we get into this topic of astrometry — not astronomy. Astrometry is concerned with determin-



Panoramic view of the U.S. Naval Observatory shot in honor of its 182nd birthday in December.

ing the very precise positions, motions, and brightnesses of stars. We use those for navigation, positioning and targeting applications. An example is that we use the astrometry data that we collect with the 26-inch refractor telescope for the Navy's Trident missile program that I mentioned before. Trident missiles have star trackers on them that use the star catalog information basically to navigate and reach their targets. That's how it was done in the early days of the U.S. Navy during the Age of Sail using celestial navigation. There were tables constructed based on the given position of astronomical bodies, stars and planets, to chart your position on the Earth. We have missile systems still using that technology today.

Q: Fascinating. I read on the USNO website, that the Naval Observatory is one of the oldest scientific institutions in the U.S.?

A: That's true, it was originally established in 1830; it predates the Smithsonian and national labs. It is a great place with a lot of history and a great mission. The contrast is interesting, we have this 19th century telescope and the superintendent's original house (now the vice president's house at Number One Observatory Circle) — it's a wonderful Victorian-era mansion. But then next door, we have the very modern, cutting-edge Nobel Prize-winning physics and engineering that goes into the master clock system. This year's Nobel Prize in physics went to Dave Wineland. The physics he won it for is central to our

clock system. He works for a collaborator of ours, the National Institute of Standards and Technology, and he was working in atomic clock development. So we have recent Nobel Prize-winning physics work being done here juxtaposed against this Victorian-era beautiful setting.

Q: I read that a new survey camera was incorporated into the astrograph telescope. What can you tell me about the advantages of the new camera?

A: A typical digital camera you can buy online or in an electronics store has about 10 to 20 million pixels. The new camera we are using with our astrograph telescope has almost 500 million pixels. With a camera that large, we can image a much larger area of the sky in a single exposure, and in the end produce much more accurate star positions and star catalogs for the nation. Our astrograph with the new camera is currently observing the northern sky from the USNO dark-sky site in Flagstaff. Part of the USNO PTA mission is to produce astrometric catalogs of the entire sky.

The neat thing about it is it has the largest charged-couple device (CCD) array in the world. Again, we developed this technology in-house. In the Navy, there is no supply system stock number for an atomic clock or astrograph telescope. So we had to develop it ourselves. We get some help from DARPA and ONR, but much of it is so specialized, a niche area, so we do most of it ourselves. The

traditional DoD acquisition system is tailored to large platforms and weapons systems, and not necessarily the unique applications we address. We circumvent that difficulty by speeding technology to operational applications quickly with our own internal research and development efforts.

Q: Are there any other new technologies that will affect the products USNO provides?

A: I did talk about the rubidium fountain clocks. It would be hard for me to simplify the advances in physics for the atomic clock system. We don't like to advertise [our advanced technologies] because we don't want to give adversaries a competitive advantage. We tend to talk about advances in generic terms so we retain that expertise and advantage.

As far as the astrometric telescope that we are putting online, the technology is very new and we are working to spread the technology across the DoD at large. There are DoD systems that use our star catalogs with star trackers. There are a number of strategic air systems that use our star catalogs, the B-2 and the RC-135 Rivet Joint are strategic aircraft and there are a couple of other applications as well. The star trackers have to be accurate just like the star catalogs. We are working across DoD and the national military labs to improve the detectors and sensors.

Q: In 1989, the USNO developed the Navy Precision Optical

Interferometer to produce space imagery and astrometry. Could you talk about its capabilities and how it differs from its predecessor, the Mark III Interferometer?

A: Using the modern technique of astronomical interferometry, the USNO produces very precise astrometric images of celestial objects, both at the radio and optical ends of the electromagnetic spectrum. The NPOI is our optical wavelength interferometer located in Flagstaff. The Mark III, located on Mount Wilson near Pasadena, California, was the developmental predecessor of the NPOI.

The technique of interferometry works by combining the light from a number of separate individual telescopes into a coherent single data stream, and the more telescopes that are used in that combination the better the result. So the principal difference between the NPOI and its predecessor, the Mark III, is in the number of telescopes that can be combined; the NPOI can combine the light from six separate telescopes simultaneously to make higher quality images and improve astrometry.

It really is a telescope array with a number of elements that when you add them together produce a highly resolved image. You can apply the same principle for acoustic arrays on Navy ships. You have receiving elements or transducers and that's how Navy ships or submarines find other ships or submarines, they use these arrays of sensors. We do the same thing at USNO, we have an array of telescopes and this one is our most precise telescope.

We are trying to determine the accurate positioning of stars and the best way to do that is by using angular width. To understand this, the angular width of the entire sky from horizon to horizon is 180 degrees. But that's a pretty wide [measurement] and we need to determine star positions much more precisely. Each degree in the 180 degrees is composed of 60 minutes, and each minute is composed of 60 seconds, and a thousandth of a second is a milliarcsecond. That's about the angular width of Neil Armstrong when he was standing on the moon, as seen from the Earth. The NPOI has a resolution

of about 16 milliarcseconds. It is a very minute resolution.

We have a number of different telescopes for different targeting and positioning applications, all of which require catalogs of different types of stars. We support the Air Force Space Command, and we give them star catalog data for what they call SSA, or Space Situational Awareness. They track space objects so our satellites don't run into them. So how do they know what those objects are? They need a reference background so they know that an object, for example, is an asteroid and not a satellite or space junk — and there is a lot of space junk out there. So we update that reference background every year because the stars move. We are in a galaxy that is rotating and moving. Stars in the galaxy move [in orbits] around the center, stars outside the galaxy move apart, and they all change which is why we continuously sense their positions.

Q: USNO has an amazing mission — is there anything else you would like to discuss?

A: The Naval Observatory is under the Commander, Naval Meteorology and Oceanography Command (CNMOC), which is under U.S. Fleet Forces Command, and we are part of the larger information dominance community. Our role, much like the CNMOC, is that we characterize the battlespace. Conventionally, the maritime battlespace consists of surface sea and undersea missions to the seabed, and it goes up in the atmosphere if you are doing BMD, ballistic missile defense, strike, ISR, and other missions.

But in today's information age, with increasing demands for faster communications and more precise positioning, our battlespace has extended far beyond the atmosphere to include the stars in the sky that we use to position our own satellites and sensors.

Our role is predictive battlespace awareness so my command covers the battlespace that is above the atmosphere out to space — and we not only determine their current positions and movement, but we also predict their future positions

and movement. Also, USNO represents an extremely high return on investment. For a modest annual budget of less than \$20 million a year for all types of appropriations, we ensure the effective and safe operation of numerous multibillion-dollar DoD capabilities, including GPS, ISR satellites, the department's unclassified and classified computer networks, and the navigation and targeting systems that depend upon them.

The time thing is really interesting; it is becoming more and more important for us due to the increased requirements for precise time and its dissemination in the DoD. That is why I was named the DoD PTTI (Precise Time and Time Interval) Manager, with direct reporting authority to the OSD CIO for all requirements, S&T plans and policies regarding DoD precise time.

Even in the days of the Pony Express, information traveled slowly. We are approaching the 200th anniversary of the Battle of New Orleans, which didn't even have to be fought because a peace treaty had been signed in England two weeks earlier. Nowadays, information is so much more pervasive and it travels so much more quickly; now we can't function without precise time. If we didn't have precise time and rapid exchange of information we wouldn't be able to do our mission. There is a book by a guy named James Gleick, called 'Faster' ('The Acceleration of Just About Everything') that talks about how that is just the nature of modern life.

Q: I was reading about how the U.S. pivot to Asia is going to require better satellite and communications coverage.

A: Yes, and as I discussed, our role is to support that capability with precise time. But a related issue is the anti-access, area denial (A2/AD) threats in the region that might prevent communications and even navigation with GPS through jamming. So we are involved in a number of efforts to provide for the ability for PNT, positioning, navigation and timing, in these A2/AD environments. Our focus is to better leverage the alternate, non-GPS means of

PNT I mentioned; TWSTT is one example.

I want to conclude with a frequently quoted phrase 'People are our most valuable asset.' Nowhere is this more true than at USNO. Highly skilled, trained and educated. Innovative and disciplined. We conduct much of our own research to speed technology to capability.

Q: Is everyone a scientist at the observatory?

A: No, but we do have the sharpest atomic physicists, mathematicians, astronomers and engineers in the Navy. Several have worked with a number of Nobel Prize-winning physicists and are doing cutting-edge work. I am very proud to represent such interesting, hard-working people. But, we also have financial, personnel, and IT professionals all working as a team. We have a former yeoman in the Navy running personnel. It is very diverse command in that respect, a wonderful mix of people.

Q: Do you worry about recruiting scientists for USNO?

A: I do. It is a concern everywhere. The DoD pay scales can't compete with industry or the big national labs but our staff is committed, and it isn't about the money for them. It is a lot of work, but we know where to go to find the scientists and engineers we need.

Q: Have you always been interested in science?

A: I always wanted to be an oceanographer, but I generally like science. Coming to this command has been a blessing for me. I watch shows on the Science Channel, like 'Through the Wormhole' and shows about space and cosmology at home. So working here doesn't feel like work — it's fun. ●

FOR MORE INFORMATION

USNO_PAO@navy.mil
www.usno.navy.mil
Public tours of the U.S. Naval Observatory are available on a limited basis.



The 61-inch Kaj Strand Astrometric Telescope, the largest telescope located at USNO's Flagstaff Station in Arizona.

The U.S. Naval Observatory

USNO is a fourth echelon operational command reporting to the Commander, Naval Meteorology and Oceanography Command (CNMOC). The observatory's headquarters are located in Washington, D.C., with field activities located at the Naval Observatory Flagstaff Station (NOFS) in Flagstaff, Ariz., and the USNO Alternate Master Clock located at Schriever Air Force Base near Colorado Springs, Colo.

The U.S. Naval Observatory performs an essential scientific role for the United States, the Navy and the Department of Defense. Its mission includes determining the positions and motions of the Earth, sun, moon, planets, stars, and other celestial objects, providing astronomical data; determining precise time; measuring the Earth's rotation; and maintaining the Master Clock for the United States. Observatory astronomers formulate the theories and conduct the relevant research necessary to improve these mission goals. This astronomical and timing data, essential for accurate navigation and the support of communications on Earth and in space, is vital to the Navy and Department of Defense. It is also used extensively by other agencies of the government and the public at large.

The observatory consists of four scientific departments: Astrometry, Astronomical Applications, Earth Orientation and Time Service. Each Department is responsible for specific products and services tailored to end-users within both the DoD and civilian environments.

Rear Adm. Jonathan White Oceanographer and Navigator of the Navy

Rear Adm. Jonathan White holds the position of “oceanographer of the U.S. Navy” and is the 20th person to do so since its inception in 1960. Assigned to the Chief of Naval Operations staff, White is head of the Oceanography, Space and Maritime Domain Awareness directorate (OPNAV N2N6E). He 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 DoD Executive Agent for Maritime Domain Awareness.

The nation's quality of life and economic well-being are both critically dependent on the security of the global seas. On the heels of superstorm Sandy and Arctic Sea ice at its lowest extent ever recorded, CHIPS asked Rear Adm. White to discuss the consequences of climate change in regard to navigation and naval infrastructure and national security.



Rear Adm. Jonathan White

Q: Can you talk about your role as director for the Oceanography, Space and Maritime Domain Directorate under the Deputy Chief of Naval Operations for Information Dominance (N2/N6E)?

A: My code on the OPNAV staff is N2/N6E, where the 'E' stands for environment. As part of the Information Dominance Corps, my responsibility is to provide information about the physical environment to enable the Navy and joint force to make the right decisions faster and better than the adversary — to provide decision superiority. We also play an important role in making decisions for the safe and effective operation of our fleet on a day-to-day basis — so ships are not running into hurricanes or typhoons, not running aground — and making sure that our aviators operate safely as well.

There are two parts to that. When I say environment, I mean oceanography, meteorology, and the timing and navigation parts of the environment. I mean space, as well, in how we are using objects in the space environment to allow us to do our job better. Maritime domain awareness is just this all-encompassing

mission, knowing everything about the physical environment but also understanding where all the ships are that travel around the oceans. We do a great job of keeping track of all the aircraft around the world. If an aircraft launches, it has to have a flight plan. People know it's out there, they track the aircraft. We've done that all over the world pretty much, except for maybe a few people who've built things in their garages and don't go above a couple thousand feet.

We don't have the same level of knowledge for all of the ships, but as you can appreciate, given the threats of terrorism and criminal activities, we need to have a good picture of basically everything that's out there, on the surface of the ocean and undersea. When you put all that together, it's a big job. It's [about] knowing as much as we can about the physical environment and what's out there in the maritime world.

Q: Does the Navy still use the Electronic Chart Display and Information System - Navy (ECDIS-N), introduced in 2005?

A: Yes, we do. It is the system that is man-

dated right now for our surface forces. But not all of our ships have it yet, Sharon. Across the Navy, there are 285 ships that range anywhere from over 30 years-old to brand new. It takes a while to get these updated, to get all of our systems and our Sailors and civilians certified to use them, so we're in progress towards making that our standard for navigation. We've come a long way, but we have a ways to go.

Q: How many ships have the system installed?

A: I think it's close to 80 percent right now.

Q: As far as some of the problems with ships running aground and collisions in the past, is one of the problems not having the added safety feature of the electronic navigation system?

A: That's a complicated topic. There's a couple of different navigation systems that basically tell you where you are at a given time, that keep you from running aground or going somewhere that you're not supposed to be, like inside of some-

body else's territorial sea. It's making sure that you're in the right place at the right time. As far as traffic, we have different systems that allow COs and bridge watchstanders to know where other things are in terms of radar and other types of contacts, so we don't have collisions at sea.

With navigation, it's where you are, and how to get from point A to point B safely. Electronic navigation systems have actually helped that. But it's like anything else, whether you're using paper charts, electronic charting, an iPhone or a Garmin, your knowledge of where you are and where you're going is only as good as the data and information that's inside of it.

I'm sure you, just like all of us, have used a Garmin, iPad or iPhone and found yourself basically saying, 'This thing isn't right.' It's telling you to go somewhere that doesn't exist, or it's telling you to go down a street that may be one-way. Data is not infallible. This applies to paper charts as well. What electronic charting has done is put the most up-to-date information at our fingertips when we need it. So, I think it has really improved our ability to navigate safely on the high seas, but unfortunately, I also believe there's a danger with electronic navigation. We tend to rely on it as being 100 percent accurate all of the time, and it's not. We still need to double-check and ensure that the information that was provided to us from electronic systems is accurate and updated. If we find things that are wrong, we've got to make sure we let the authorities know so that they can send updates out to other ships to navigate safely and make corrections as necessary.

Q: In 2009, Task Force Climate Change created the Arctic Roadmap to address the changing Arctic. What would you say is the greatest threat to our environment in regard to the changes in Arctic weather?

A: That's a tough one. The Arctic is sort of like a thermostat of climate change, if you will, but there are other ones out there, as well, including glaciers and the Antarctic ice shelf. So we use it as one of the tools to monitor what's happen-

ing with global climate change, but if you look at the Arctic and what is happening, there's a couple of things that come to mind. One is that as land-based ice melts, we end up adding more water to the ocean. Add that to thermal expansion as the oceans warm, and the result is sea level rise, which could be very dangerous to global coastlines. We know there are many nations — including ours — that have a high population density in coastal areas that are not much above sea level. I recently moved here from just north of the city of New Orleans. New Orleans is actually below sea level. Even a small amount of sea level rise could have a major impact. Long term — that may be our most dangerous risk.

Nearer term, we have issues with people trying to get into the Arctic. The Arctic promises a wealth of resources. There are natural gas, oil and mineral resources. We're seeing increases in fish populations in the Arctic as warming oceans allow fish to migrate from lower to higher latitudes. Transit routes are opening up, so we see more shipping traffic. More of our population is going to be up in the Arctic. That is hazardous because we don't fully understand the Arctic environment and some of the perils of operating in the high latitudes. Arctic weather is harsh and changes rapidly; there could be dangerous ice floes even though the Arctic may be melting in terms of overall ice coverage.

Consider the Deepwater Horizon spill, and how hard that was to respond to. What if we had an oil spill of that volume, that magnitude in the Arctic? Think of all the towns and all [of] the infrastructure we have on the Gulf Coast, the cities that had oil booms, ships that could help contain the oil and treat it with the disbursement chemicals. What do you do if there's an oil spill north of Alaska, north of Russia, or north of Canada? We have limited means to be able to respond.

A lot of cruise ships are going into the Arctic. There are not that many from the U.S., but many other nations, especially the European nations, are sending more and more cruise ships. What if there was an accident, like we had with the Costa Concordia cruise ship from Italy about

"Maritime domain awareness is just this all-encompassing mission, knowing everything about the physical environment but also understanding where all the ships are that travel around the oceans."

a year or so ago? What if that happened in the Arctic? We don't have the type of emergency access and rescue equipment assets to be able to respond. So I've given you a whole laundry list of hazards from the long-term ones associated with climate change and sea level rise to the shorter term ones, like more of our human population living or operating in the Arctic, probably in the near future, at least within the next decade or two.

Q: I know there's still a lot of study to be done and decisions to be made, but some people say that there could be benefits to the Arctic opening up. Are you looking at any positives that the open seas in the Arctic may help the Navy or help the nation?

A: I'm not sure it's going to help the Navy or not. That's another ocean we will have to be involved in — we may have to build more ships and that would be more expensive — I don't know. That's above my pay grade, by the way. Certainly Congress would have something to say about that as well. But more seriously, I think it does have great benefits. I talked about some of them. We do have resources in the Arctic that could be a great boon to our population, which is so reliant on oil and other petroleum-based resources. We know that you can save a lot more time by transitting route through the Arctic than you can by going through the Panama Canal or Suez Canal. Shortening the transit times for some nations will be a great benefit.

Q: I understand that CNO has placed a great deal of importance on the Arctic and climate change — can you talk about any of the organizations that you are part-

"Consider the Deepwater Horizon spill, and how hard that was to respond to. What if we had an oil spill of that volume, that magnitude in the Arctic ... We have limited means to be able to respond."

ARCTIC OCEAN (March 19, 2011) Sailors and members of the Applied Physics Laboratory Ice Station clear ice from the hatch of the Seawolf-class submarine USS Connecticut (SSN 22) as it surfaces above the ice during ICEX 2011. U.S. Navy photo by Mass Communication Specialist 2nd Class Kevin S. O'Brien.



nering with or any other groups that you'd like to reach out to?

A: First, I'm going to talk about the national level. We have a very close partnership with NOAA, the National Oceanic and Atmospheric Administration. They deal with U.S. domestic concerns regarding the Arctic and climate change. As with any ocean, the Navy's focus is on national security. The Coast Guard, which falls under the Department of Homeland Security, is focused on the security of our territorial waters, including our Arctic waters, and also the interests of the overall security of our homeland and people. There is a partnership effort between Navy and NOAA and the Coast Guard in terms of trying to understand how climate change in the Arctic, as well as the rest of the world, will present challenges near term and long term, and the impacts that might have on global society.

So, those are two that we're in close partnership with right now. We are also partnering with other governmental agencies like NASA, the Department of Energy, the Department of the Interior — all these agencies have a role in understanding the impact of climate change and an ice-free Arctic. Climate change has had a big impact on the Department of Energy in terms of the energy that will be required to possibly deal with more

extreme temperatures and weather. There are a lot of pieces involved, and we work very closely with them.

One thing that I am an advocate for is taking a more cohesive approach among all the interagency partners to understand and predict changes in our atmosphere and oceans, from daily forecasts of severe weather events to long-term climate forecasts. If we pool our resources, I'm convinced that we can do a better job, that we can have the world's foremost capability to make a forecast for a specific place less than one hour from now, or to describe climatic conditions there in 30 years. We ought to have a national plan to be able to do that. So we're working with our partners to try to get to that end goal.

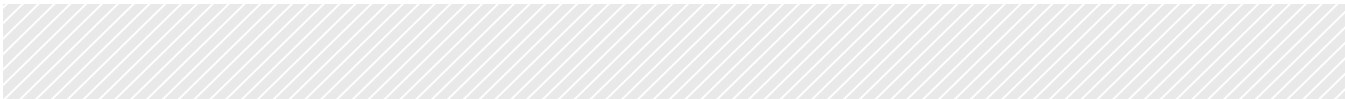
On the international side, we have the Arctic Council. There are eight Arctic nations involved — I think you probably know who they are — the U.S., Canada, Norway, Iceland, Finland, Denmark, Sweden and Russia. Those eight nations either have coastlines in the Arctic or they've operated in the Arctic for many years. We're focused in trying to partner with those nations to understand how we [can] work together to resolve the issues. We've been able to make a lot of progress. For example, the Arctic Council sponsored the Arctic Search and Rescue Treaty, which divides search and rescue responsibilities for the entire Arctic. We're

looking to do a similar type of thing for oil spill incidents or other types of natural or manmade disasters.

Partnerships will be critical because it's expensive to operate in the Arctic. It's a long way up there, it's very cold, and there are not a whole lot of places where you can build a base, an infrastructure, a deep water port, and those kinds of things. It's extremely expensive. Just to buy things at a grocery store in Alaska, not even in the Arctic, costs about twice or three times what it would cost to buy it here in D.C. How can we make sure that we can partner with other nations to share responsibility, leverage each other's bases, ice-breakers and assets to make sure we're doing everything efficiently as partners?

Q: **Though concern over climate change affecting national security has long been an issue, the most recent hurricane (Sandy) has brought the issue to the forefront. Five military installations are directly threatened by their proximity to anticipated higher sea levels, including Norfolk Naval Station. Is the Navy taking any steps now to protect its bases?**

A: Sea level is currently rising a few millimeters a year, so we see this as a challenge of the future but not a crisis. We



must consider future sea level rise and enhanced storm surges when doing infrastructure development planning, but this subject is fairly new and we're not sure of the best way to do it. The Office of the Secretary of Defense is sponsoring a series of studies to develop a proper methodology for future assessments.

In the near term, we're more concerned about storm surges. We do a good job of predicting storm surges from hurricanes now. For instance, we knew what the storm surge level was going to be in New Jersey and New York for Hurricane Sandy. We knew roughly what it might be with Hurricane Katrina back in 2005. But even though we sometimes know what the level is going to be, we don't exactly know which inlets, which rivers, which creeks, which harbors or whose backyard is going to be impacted by that much water. When it comes down to localized effects, it's extremely hard to model. It's like spilling a glass of water or a cup of coffee and trying to predict which way the spill is going to go and what's going to get wet. There are a lot of variables in trying to model something like that.

From a civil engineering perspective, we need to know where things fail, like electrical infrastructure or roadways, for example. That's been a longtime issue in Florida, where I grew up. You know, the hurricane evacuation route is I-95 up the East Coast. What happens if I-95 gets inundated? What happens with I-10, the evacuation route along the Gulf Coast, which, by the way, was shut down after Katrina because of the bridges that were wiped out?

So looking at the points of impact is very important to our nation. Are we concerned? Sure we're concerned. Like I said, Norfolk, San Diego, Jacksonville and New Orleans are at risk, as well as overseas bases like Diego Garcia. Look at some of our territories, like American Samoa and Guam. In the global environment, look at Myanmar or Bangladesh, for example. Hundreds of thousands of people living within a couple of inches of sea level without a lot of infrastructure.

It's not just Navy infrastructure, it's also DoD infrastructure. Bear in mind, if Norfolk floods due to a hurricane or a

nor'easter, there's an Air Force base down the road called Langley, the headquarters of the Air Combat Command, which usually gets flooded worse than the Navy base in Norfolk because of the way the water comes inland up through the Chesapeake Bay. Another point, is that we don't want to spend money before need. We want to take a deliberate and responsible approach to our strategic planning to prepare for the challenge before it becomes a crisis that results in knee-jerk reactions.

Q: Are there any new technologies in the science of meteorology to help predict massive storms such as Hurricane Sandy?

A: Yes, there are, there always are. We in the Navy, with our interagency partners, do a pretty good job in weather prediction, but I think we could do better in long-term predictions. But in terms of weather forecasting, for hurricanes, typhoons and nor'easters, big snow events, big rain events, flooding and those kinds of things, we've come a long way.

One way to look at this in terms of weather forecasting is that every 10 years, over the last 50 years or so, we've gained a day in accuracy. What was accurate as a three-day forecast back in the 1980s is now accurate as a five-day forecast. And that's true with hurricanes and typhoons as well. Back in the 80s, we didn't even do five-day forecasts in the western Pacific for tropical storms or for hurricanes in the Atlantic and in the Gulf of Mexico. We only did three-day forecasts.

Now we do five-day forecasts and they are darn accurate. Look at the forecasts for Hurricanes Katrina, Sandy, Irene, Isabelle, and other ones we've had over the last 10 years or so. They were extremely accurate forecasts in terms of speed and direction, but they were not always as accurate in terms of intensity. It's very hard to forecast the intensity of these storms, so that's one effort that we're putting a lot of research into: what are the factors that either cause these hurricanes to really intensify, to maintain their intensity, or in some cases, to fall apart right before they come ashore? A lot of

experts that work for universities — that are funded by the National Science Foundation, by the Office of Naval Research, the Air Force Research Laboratory, Army Research Laboratory, or privately funded by the Weather Channel and others — are doing significant research.

What's the impact? What's the impact on a local area, town or city if you get a lot of rain, if you get four days of about three inches of rain per day, what's going to cause major flooding and what's not? If you have a storm surge of 12 feet along the coast of New Jersey and New York, which areas are going to be the hardest hit? How can I predict that in advance so I can make sure that we get the people out of there, make sure they're warned?

Another area of interesting research is in regard to human behavior. How do people react? How do we influence them to evacuate or not? How do we get the information to them? How do we make it clear and decisive in nature? If there's a hurricane coming right now, people are going to four or five different weather sites on the Internet, on different cable channels, whether it's CNN, NBC, Fox News, your local news. They're hearing all this and sometimes there's an information overload, and they're not sure what to do. So the human factors are another piece.

The Navy has made huge gains in being able to understand the probability of the outcome of an event. Not just the forecast that you're going to get 60 knots of wind, but what's the probability of 50 knots? When do I need to get ships out of the way? If I tell you it's a 50/50 chance, it darn sure could happen. But if I say it's a 95 percent probability that there is not going to be 50 knot winds in Norfolk, the fleet commander will probably take that risk and not evacuate all the ships from port.

These are the kind of decision-based tools that we're putting into play in the Navy. Ensemble forecasting and probabilistic forecasting are helping to make better decisions in the future. Extend that out to when our children are our age, a 10-day forecast may be able to tell them whether or not they're liable to have a hurricane.

Q: Do you have any concerns from the Navy perspective about the gap in the weather satellite coverage?

A: I do have some concerns. The cost of things in space has increased astronomically — pardon the pun — it just seems like it costs more and more and takes longer and longer to get something in space. Fuel costs, the cost to build instruments, or whatever it is. I don't really understand why it costs so much, but I think we're about a decade behind on the technology we need to have in space.

I could take you to laboratories that are building instruments that give you an amazing amount of information about what's happening in the atmosphere, in the ocean, and over land, but it seems like it takes a long time to get that technology into space. I am concerned about the space program. Earlier I mentioned building a zero-hour to 30-year model of the atmosphere, the ocean and of ice. The name of that initiative is the Earth System Prediction Capability, or ESPC. It's largely a partnership between Navy and NOAA right now, and we're both investing in it. In the future, we're hoping to bring other agencies in as well to have a common national investment toward this goal.

Q: Can you talk about the new Navy Space strategy that your office is developing?

A: I can talk about it in general. First, I'll tell you that space is a vacuum and it sucks much of my time away from me while I'm in the Pentagon. Other than that, it's interesting in that it provides us with great capabilities for looking at what's happening on the Earth, and also outside the Earth. Once you get out of the Earth's atmosphere, you can see a lot more clearly into space. We need to be able to operate in space as a Navy to facilitate effective communications, like voice communications, emails, sending information and imagery. So we need high bandwidth.

The Navy and DoD, just like everybody else, are starved for bandwidth. A lot of information moves through space,

and we're certainly going to need more bandwidth in the future. We use the ability of satellites to monitor what's happening around the world, to basically look at things. The imagery actually comes from space, whether it's satellite imagery of atmospheric and oceanic factors, or intelligence imagery, like threats to our Soldiers and Sailors on the ground.

There's another piece that I talked about earlier — our ability to navigate accurately. GPS is a space tool and we have a GPS satellite constellation. Other nations are putting a lot of things into space as well. It's expensive to get stuff into space but the return on investment is great, so we're seeing other nations put their own communication satellites in space, their own imagery satellites, and their own navigation systems. Consequently, space is becoming crowded.

Our superior level of information dominance is based, in part, on our investment in space assets. As other big players begin to populate space with their assets, we may need to figure out how to get along and ensure our common national priorities are being met. A lot of my job is figuring all this out, determining what is needed by our Navy and our military today, and investing wisely in those capabilities.

Q: Is part of your space strategy working on how to best utilize the Space Cadre to implement the Navy strategy?

A: Yes, we are and there are some senior leaders in the Space Cadre right now who are looking at what it means to be part of the Space Cadre, what are the qualifications? One of the things that we have to deal with in terms of the cadre is that it includes people across platforms who have diverse skills that are gained through education and experience — aviators, oceanographers, intelligence professionals — they all have skills and experience that give them a certain level of specialized expertise.

We need to understand how to put the right people in the right job to take the best advantage of space. A lot of times this is based on acquisition, getting people

who have experience in space technology, who have worked in space environments, who have been educated in satellite systems, or whatever it may be. After five, ten years, they're the people who will be making the right decisions on how we attain the capabilities that are going to give the actual best return on investment. The Space Cadre is engaged in that, and we're looking at how to more effectively manage that in the future. I would say it actually goes across all the services as well. The joint force needs to do a better job in managing its space expertise.

Q: Is there anything that you want to talk about?

A: The only other thing I'd like to mention is the Navy's merging of information professionals into OPNAV N2/N6 and the Information Dominance Corps. We brought together oceanography, intelligence, cyberwarfare and the information technology that we use to keep our networks working, and it is actually working out quite well. We have to maintain the information networks to move information around, and we have to defend the networks, understanding that cyber is a whole new type of domain with a lot of people out there trying to attack us.

We have to be as effective in cyberspace as we are in the physical environment. In terms of intelligence and environmental knowledge, one way to look at that is battle space awareness. That's the awareness of what's happening in the physical battle space, that's what I've largely talked about today.

It also means understanding what's happening in the human battle space, and that's intelligence work, the content largely of what's in our networks. You take the physical world and the human world, and you merge that together to make the best possible decisions that you can, whether it's peacetime or war. Having the ability to move that information around securely, effectively and rapidly to get it to the right people — that's information dominance. This is actually working quite well, and I'm pretty excited about the future of information dominance in the Navy. ●

Contract Award Paves Way for Agile Navy Recruiting, Advances Vision of RF2020

By Sea Warrior Program

The Sea Warrior program (PMW 240), within the Navy's Program Executive Office for Enterprise Information Systems (PEO EIS), is pleased to announce a contract award for up to \$65 million to modernize key systems supporting the Navy Recruiting Command (NRC). The new Recruiting and Accessions Information Technology (RAIT) services contract helps lay the IT foundation for Recruiting Force 2020, a strategy that relies on agile, paperless technology to recruit quality applicants for America's Navy.

"The RAIT contract award is an important next step toward realizing the Navy Recruiting Force 2020 strategic plan of 'anytime, anywhere' recruiting," said Mr. Kevin Sullivan, NRC chief information officer. "One of the first task orders under the RAIT contract will be the PRIDE Mod (Personalized Recruiting for Immediate and Delayed Enlistment Modernization) Increment II, which focuses on a Navy enterprise solution for recruiting and accessing enlisted and officer active duty and Reserve candidates."

Currently, the management of NRC officer programs is a manual, paper-based process for both active duty and Reserve personnel across 14 officer program categories, each with specific candidate selection criteria and a unique set of detailed qualification forms. As a result, NRC's 38 officer program managers maintain standalone spreadsheets on their various designators and programs. In addition, the configuration of candidate forms — roughly 147 — is managed separately by the Navy's 26 Recruiting Districts.

"The PRIDE Mod Increment II will change the manual application process into a data-driven process supported by workflow management and electronic forms. As a result, we anticipate the error rate for officer applicant processing, which is now around 35 percent, to decrease dramatically because of better data quality. Also, the time to enlist an applicant or commission an officer will be shorter, reducing the chance we'll lose

SAN ANTONIO (Oct. 20, 2012) Recruiters from Navy Recruiting District San Antonio speak with students during the 3rd Annual George Gervin Youth Center College Extravaganza at the campus of Our Lady of the Lake University. The College Extravaganza connects junior and senior high school students with the military, colleges, universities, and trade schools from across San Antonio. U.S. Navy Photo by Burrell Parmer.



good candidates due to a lengthy process," Sullivan said.

Under the RAIT contract, selected applications and systems will be migrated over time into common components that will yield a more flexible, interoperable solution for today's mobile and agile Navy recruiting force. The RAIT team has initially identified cross-cutting capabilities from nine legacy stove-piped systems for modernization and integration into several core web-based applications built on a services-oriented architecture. Examples of these capabilities are PRIDE Mod II to support officer and enlisted processing for active duty and Reserve forces, recruit marketing research and analysis, applicant medical waiver review, investigative data for applicant security clearances, and other key functions.

"The SOA-driven approach to RAIT modernization is the right course of action because it lets us leverage current applications as services; thereby, safeguarding our existing IT infrastructure investment," said Ms. Laura Knight, program manager of the Sea Warrior program. "The SOA has proven effective for the implementation of PRIDE Mod I, which was launched in May 2011. Recruiters in the field now have a web-based capability that enables a faster, more automated process to seek and admit future Sailors into the Navy."

PRIDE Mod's complex data exchange environment interfaces core recruiting, accessions, training and personnel appli-

cations. With PRIDE Mod Increment I successfully in operation, NRC seamlessly shares real-time accessions data with its business partners and key Navy human resources and training systems.

PRIDE Mod II will also support technical and data exchange requirements anticipated in 2013-2014 for the U.S. Military Entrance Processing Command (MEPCOM) Integrated Resource System (MIRS) enhancements. This includes the capability to capture personal identification about recruits such as fingerprinting and other biometrics.

The RAIT services contract was awarded Nov. 1, 2012, to Stanley Associates, a wholly-owned subsidiary of CGI Federal, Inc. It focuses on developing interoperable IT solutions to support recruiting and accessions business processes. The contract award was the culmination of a collaborative effort by the Sea Warrior program, PEO EIS, Navy Recruiting Command and the Space and Naval Warfare Systems Command. The solicitation was a full and open competition as a single award indefinite delivery/indefinite quantity contract. ●

FOR MORE INFORMATION

Please contact the PMW 240 public affairs office at (703) 604-0192 or email to PMW240_PAO@navy.mil.

The U.S. Military's Joint Tactical Radio System

It is More Valuable Than Ever to the US Navy

By S.S. Kamal and John T. Armantrout



Much is being discussed these days within the defense community about the legacy of, and investment in, the Joint Tactical Radio System (JTRS) program and its transition to the Joint Tactical Networking Center (JTNC). A key to understanding this evolution is to look at the original concept through a strategic lens: What was JTRS intended to do? Where is it today? How may the new JTNC serve the U.S. Navy's strategic goals in tactical networks? This article explores the program's powerful business model and how best to exploit what it offers. We will examine technological, operational and programmatic dimensions to JTRS, a program that's scope was never intended to produce "yet another generation of tactical radio."

THE VISION

Lengthy details of the JTRS program history can be found in numerous public references, but a brief recap of that history provides a valuable foundation for this discussion. The genesis of the program lies in the concept of exploiting advances in technology to separate the hardware of a wireless or satellite communications device from the software that shapes the radio signal over the air; allowing information to be transmitted and received between the devices (aka the waveform software). This not only transformed the form and function of the communications devices, but the very nature of military tactical mobile networking itself.

The hardware/software separation was largely facilitated by advances in programmable semiconductor chips with the ability to be programmed to behave differently, perform at unprecedented speeds, able to store large amounts of information while costing less every year. This concept of a software definable radio (SDR) was further facilitated by advances in standardizing the software communications architecture (SCA), enabling small blocks of specialized soft-

ware to be assembled to deliver complex networking capabilities. These two technology improvements: better chips and better software design produced a highly capable tactical radio. These same technology advances are also enjoyed today by the telecommunications carrier and cellular industries and smart devices in virtually every sector. They unleashed four powerful enabling capabilities for the military:

1. Different devices of size, weight and shape can now be developed for widely different specialized purposes, yet be interoperable while hosting the same software. The market continues to innovate to meet the needs of military planners and warfighters.

2. The waveform software itself is developed once but reused many times as developers produce new innovative physical forms that meet the military's varied missions and different platforms. A wireless device on a ship can connect to a miniature device on an unmanned aircraft, which itself can be exchanging information with even smaller sensor devices or a dismounted Soldier's handheld radio on the ground.

3. Not only are development costs reduced by reusing the software, but the recurring per-unit production costs are kept low by multi-vendor competitive market forces. The military now has options without being wedded to a specific vendor.

4. Lastly, but of paramount importance to the military's modernization efforts: forces, teams, services, and even coalition countries, can all deploy tactical networking devices that suit their special needs, yet are assured of interoperability when they come together in joint exercises or live missions.

These developments led to the vision, depicted in Figure 1, of a battlefield consisting of multiple different physical devices based on mission and platform requirements, all employing the same "family of waveforms" to ensure interoperability; eliminating stove-piped vendor-dependent networks. The form factor and physical configuration of the radio device itself is no longer defined by the network, but by how it will be used in the mission. For a different mission, these same physical devices can be configured to host different waveforms; but

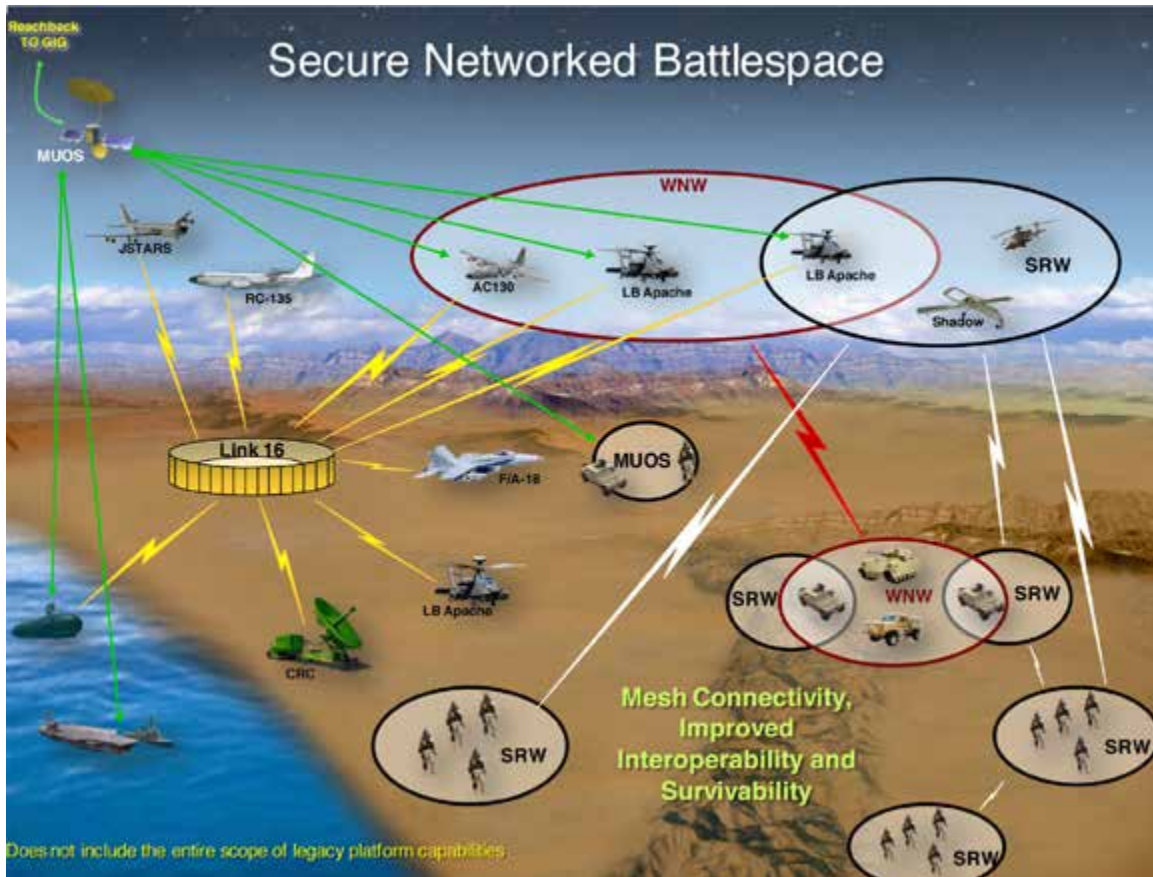


FIGURE 1. VISION OF A MISSION-CENTRIC JTRS TACTICAL BATTLEFIELD. •SRW, SOLDIER RADIO WAVEFORM, FOR DISMOUNTED SOLDIERS, SENSORS AND SMART-WEAPONS •WNW: WIDEBAND NETWORKING WAVEFORM, FOR GROUND MOBILE VEHICLES AND AIRBORNE PLATFORMS •MUOS, MOBILE USER OBJECTIVE SYSTEM, FOR GROUND, MARITIME AND AIR PLATFORMS VIA SATELLITE • LINK-16: EXISTING WAVEFORM FOR AIRBORNE PLATFORMS.

still continue to interoperate. For the first time, mission planners can now configure networks that are mission-centric; not net-centric, device-centric or people-centric.

To realize this vision, the JTRS program incubated the technologies, concepts and processes that would implement and sustain this business model because industry would not venture into this ambitious new world on its own. JTRS was essentially embarking on overhauling how the military services define their communications requirements, translate them into acquisition strategies to buy what they need (not what is offered) and acquire equipment that meets their requirements in a stunningly different way.

To prove the business model, JTRS was structured as an umbrella organization that encompassed not one, but five Major Defense Acquisition Programs (ACAT-ID) shown in Figure 2. Four of them developed hardware architectures for the tactical SDRs. The fifth focused on developing the waveform software and net management software that

could be hosted by these devices and any other devices developed for the future battlefield.

Collectively, these five programs under JTRS validated the JTRS enterprise business model (EBM), its processes and technologies. Once completed, the waveforms and net management software were available to be hosted on any variety of physical devices to meet platform, weight, battery power and size requirements. Military programs of record (POR) and independent vendors then requested to reuse this software on a recurring basis.

As a demonstration of the full range of SDR possibilities, JTRS chose to develop two categories of waveform software. The first category of software mimicked existing legacy radios currently deployed in the field, focusing on Single Channel Ground and Airborne Radio System (SINCGARS), Enhanced Position Location Reporting System (EPLRS), Ultra High Frequency Satellite Communications Demand Assigned Multiple Access (UHF SATCOM/DAMA) and HF radios.



FIGURE 2. STRUCTURE OF THE JTRS PROGRAM GMR: GROUND MOBILE RADIO (NOW MID-TIER NETWORKING VEHICULAR RADIO (MNVR)); HMS: HANDHELD, MAN-PACK & SMALL FORM FIT; MIDS: MULTIFUNCTIONAL INFORMATION DISTRIBUTION SYSTEM RADIO;AMF: AIRBORNE/MARITIME FIXED RADIO.

The second category of software presented new and advanced capabilities to the U.S. military, focusing on the Wide-band Networking Waveform (WNW), the Soldier Radio Waveform (SRW) and a new beyond-line-of-sight (BLOS) satellite waveform called the Mobile User Objective System (MUOS).

Why demonstrate two categories of software? It would have been simpler to prove an SDR can mimic SINCGARS, or to ignore the large inventory of legacy radios and simply point to the future networking features of WNW or MUOS. But central to the JTRS business model was, and still is, the concept of providing a technology development roadmap showing the military how its legacy capabilities coexist with its modernization efforts.

The JTRS model offers a powerful yet easy-to-understand transition roadmap. Whether speaking to an Army Brigade or smaller platoon, an Air Force squadron or entire wing, a U.S. Naval fleet or a smaller formation of naval assets, each software-defined communications network can evolve at the “speed-of-need.” For the first time U.S. operational forces can determine their budgets, timetables, capability gaps and priorities and chart their own course for modernizing their tactical networks. What they are assured of is the consistency of the devices’ interoperability across the tactical battlefield.

Examining Figure 1 closely reveals that the family of JTRS waveforms depicted extends the Defense Information Systems Network Global Information Grid to the very edge of the tactical battlefield. Information exchange and battlespace awareness can occur nearly instantly. Now, missions need to be planned in ways that exploit these new “info-weapons.” This requires equally innovative changes to training, mission planning and military doctrinal processes while preparation for and waging battle enter a new era.

EXECUTING THE VISION

Much of the JTRS vision and mission have been accomplished, including the following:

- The software depicted in Figure 1 for all the waveforms (legacy and new) now resides in the JTRS Information Repository (IR), along with design and test documentation, to assist vendors and program of record of-



FIGURE 3. TRANSFORMATION OF JTRS- STAGE I.

fices use of JTRS products in their preferred devices.

- The Handheld, Man-pack & Small Form Fit (HMS) program has delivered handheld radios (AN/PRC-154) hosting the new SRW waveform to the following U.S. Army units: 75th Ranger Regiment; 2nd Brigade, 1st Armored Division; 173rd Airborne Brigade Combat Team; and the 3rd and 4th Brigades, 10th Mountain Division. A manpack device (AN/PRC-155) hosting SRW, SINCGARS and SATCOM 181 is currently under limited production and testing. The same manpack device will also host DAMA and MUOS waveforms shortly.
- At their own cost, several industry vendors have “checked out” waveform software from the JTRS IR and are porting it to their radio form factors. So reuse of JTRS software has begun, with several vendors’ devices passing interoperability testing at government test facilities.
- JTRS has defined and validated detailed engineering processes for ensuring the affordability, reusability and interoperability of government-owned software on multiple ven-

dors’ devices. These processes were not developed overnight and were revised and improved as lessons were learned throughout the lifespan of JTRS programs. High impact components of these processes include:

- Access to an Information Repository that provides for each waveform: the source code; detailed design documentation; test specifications for how the waveform should be tested on any platform; and all previous test results conducted by government or vendor labs.
- The establishment of standard JTRS application programming interfaces (APIs) and defined software communications architecture (SCA) standards that help vendors and developers port the waveform software to different hardware devices.
- JTRS collaboration with the DoD Joint Interoperability Test Command (JITC) to select and upgrade its labs and test fixtures enabling JITC to conduct independent testing of a vendor device hosting a JTRS waveform.
- Quarterly technical exchange meetings convened to foster collaboration among a “community of develop-

ers” who have a vested interest in their devices interoperating with each other, as well as training industry to step up and meet the rules of the new business model which includes affordable, interoperable and secure tactical devices that reuse software in which the government has invested significant funds.

- JTRS aligned its processes for improving, evolving and expanding its suite of waveforms to the Defense Department’s policies for future SDR development.

With much of its original mission completed, the JTRS program began a planned transition from an incubator to a maintainer and governing body for the reusable software it developed, completing the transition Sept. 30, 2012.

Having funded the body of work that defined unique hardware needs for these new advanced networking waveforms, it was time to exit the hardware business. The Joint Program Executive Office (JPEO) for JTRS transformed into an organization that facilitated the expansive, yet disciplined reuse of the software in its Information Repository; oversaw the evolution of these waveforms and expansion of the suite of waveforms, and certified security and interoperability compliance.

Figure 3 depicts the first stage of this transformation: All hardware program offices have now been transferred to the services that will deploy them first. Going forward, the military services can choose to port JTRS software to their own unique devices, reuse devices already deployed by other services or modify commercial off-the-shelf devices to suit their needs. Cost and mission objectives will dictate each decision, but interoperability would not be compromised.

Stage II of the transformation, shown in Figure 4, reorganized the remaining parts of JPEO JTRS to fulfill its future mission into the Joint Tactical Networking Center (JTNC) consisting of three components:

- Product Manager Joint Tactical Networks (JTN) to support the current software life cycle management and develop new waveforms as needed.
- Joint Reference Implementation Laboratory (JRIL) to assist programs of record and vendors in testing waveforms as they are ported or upgraded and assist DoD in evaluating ideas and technologies for new waveforms as they are developed by

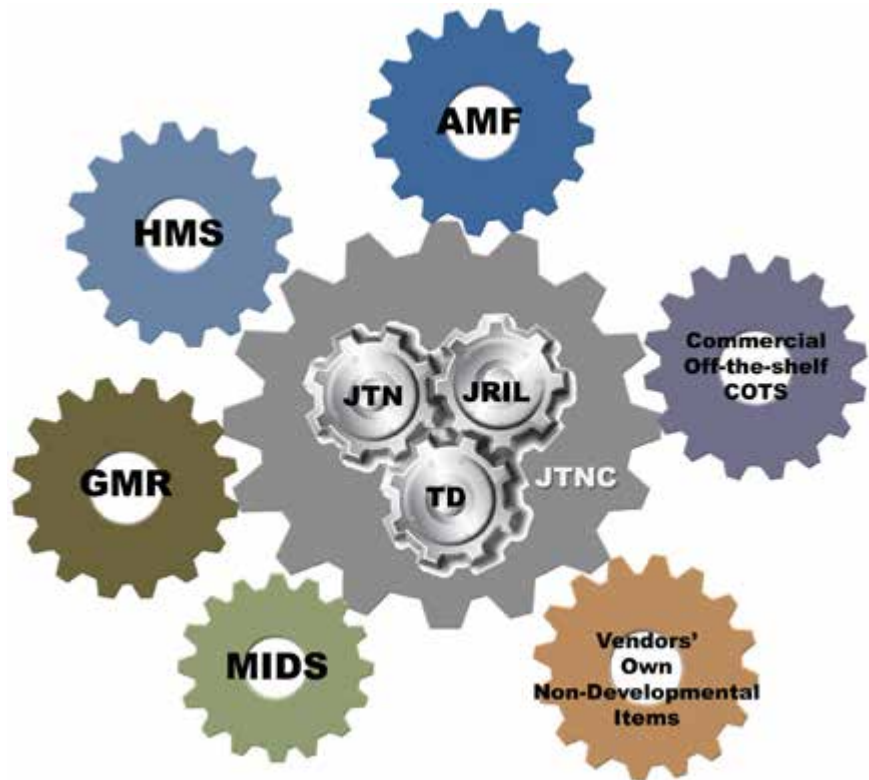


FIGURE 4. TRANSFORMATION OF JTRS JPEO – STAGE II.

“As Naval warfare enters the 21st century the balance and role of naval operations is changing drastically. Gone is the potential (at least for the foreseeable future) for Great Fleet clashes between carrier or battleship groups. Instead the new role of naval forces is participating actively in the land war.”

Tristan Dugdale-Pointon

industry. JRIL leverages government test labs.

- A technical directorate that will serve two principal roles: (1) oversee the engineering processes that ensure the security and interoperability that DoD expects vendors and PORs to implement for the waveforms; and (2) interface to the science and technology communities (inside and outside the DoD) to bring in new advanced capabilities to the current family of waveforms.

Although JTNC was placed administratively under the U.S. Army, DoD’s acquisition decision memorandum directed that all service branches leverage JTNC waveforms. With this new focus, JTNC has become the gearbox that drives the execution of the military’s acquisition for advanced tactical networks for modern warfare. These networks will host secure interoperable software on

whatever physical devices serve their missions.

NAVY RELEVANCE

Many lessons were learned in executing the JTRS vision. While JTRS launched technology innovations and next generation communications capabilities to the military, it used equally innovative acquisition strategies, business models, test and evaluation processes, and test, modeling and simulation tools that virtually did not exist anywhere in network labs around the world. Valuable lessons were learned in all of these areas. How does the Navy leverage these capabilities? A closer examination of Figure 1 offers a clue.

The Navy’s study of littoral combat refers to operations in and around the littoral zone, within close distance of shore, including surveillance, mine-clearing and support for landing operations and

other types of combat shifting from water to ground and back. Interoperability must extend seamlessly between ground, air and sea platforms.

Today, the U.S. Navy is building on its adoption of the software-defined MIDS radio shown in Figure 5. This radio has already incurred thousands of hours of flight testing, hosting the Link 16 waveform. Its four-channel radio can carry any mix of legacy or networking JTNC waveforms.

Hosting a tactical data link (TDL) allows naval airborne assets to communicate with ground forces. Hosting the new MUOS satellite waveform allows the device to provide BLOS reach-back to tactical Link 16 platforms and to ground forces.

Equally, the Navy is taking advantage of another JTRS-incubated program: the AMF radio, shown in Figure 6. This two-channel radio is a smaller form factor than MIDS, for smaller airborne platforms.

Hosting MUOS and any other ground or airborne waveform, this device can be another component for the Navy's new role in littoral warfare. Whether interoperability is sought between the Navy's air and sea platforms, across the services or with coalition and friendly forces, hosting the same family of waveforms on any radio device that fits the Navy's mission allows it to participate up close and personal with mission partners.

PROGRAM KEY CHARACTERISTICS

Interoperability is defined as "the ability of diverse systems and organizations to work together." Ultimately, this is a people challenge, not a device or technology challenge. JTNC has developed detailed processes for testing and verifying interoperability before a new device is inserted into the field.

Without interoperability, the business model breaks down and we risk regressing back into the costly and fragmented networking morass that DoD is resolved to fix.

Affordability is achieved by being able to reuse the same family of waveforms so that DoD's return on investment increases as more devices host the software. JTNC has developed APIs and SCA guidelines and test tools to facilitate reuse and maximize return on investment.

Security is safeguarded by protecting the membership of the family of waveforms. JTNC's waveforms are certified by the National Security Agency for each and every platform that hosts them, which guarantees the trustworthiness of the network fabric across the battlefield.

Interoperability, affordability and security are designed into each waveform. Each waveform encompasses a clear architecture, disciplined configuration management process and vigorous verification and validation



FIGURE 6. THE AMF RADIO, COURTESY OF LOCKHEED MARTIN.

testing to ensure compliance and certification before radio devices are launched into the battlefield.

Some parties resist assigning such a role to JTNC, viewing it as too much consolidation of authority into one organization. This argument misses the point. With the Defense Department revamping its policies for development of radio software and overhauling its acquisition practices to buy smarter, the legacy groundwork laid by JTRS should be exploited to get the maximum investment return on scarce defense dollars.

JTNC stands ready to sustain and further innovate the JTRS-developed, fully capable, secure and interoperable family of waveforms. ●

FIGURE 5. THE U.S. NAVY'S MIDS RADIO



S. S. KAMAL is the chief scientist for engineering at SAIC International.
JOHN T. ARMANTROUT is the technical director of the Joint Tactical Networking Center.

THE JOINT TACTICAL NETWORKING CENTER PROVIDES AFFORDABLE, INTEROPERABLE AND SECURE TACTICAL WIRELESS NETWORKING IN SUPPORT OF SERVICE, MULTI-SERVICE/JOINT AND COALITION FORCES.

[HTTP://WWW.JTNC.MIL](http://www.jtnc.mil)

Get Ready, Get Set, Innovate

Navy Warfare Development Command – Navy Center for Innovation

By Sharon Anderson

Shrinking budgets and old ways of doing things don't have to stifle innovation. In fact, in many ways austere budgets and impatience with inefficient processes can actually be catalysts for forward thinking and transformational change. The U.S. Navy is counting on the "young turks" — young people, junior officers and those full of new ideas and impatient for change to raise their ideas through their command channels to increase the effectiveness of maritime operations or even perhaps to revolutionize warfighting concepts.

To this end, Rear Adm. Terry Kraft, commander of Navy Warfare Development Command (NWDC), published *The Innovator's Guide* (<https://www.nwdc.navy.mil/ncoi/Innovation%20Reading/Innovator%27s%20Guide%20Book.pdf>) which outlines the path to creative thought and the generation of new ideas.

In early 2012, Adm. John C. Harvey, then-commander of U.S. Fleet Forces Command, challenged Kraft and NWDC to jumpstart and formalize innovation efforts across the Navy. Since that time, much has been done, including the establishment of the Navy Center for Innovation and CNO's Rapid Innovation Cell, both hosted at NWDC. In essence, the cell serves as a mechanism to transform game-changing ideas into solutions and as an alternative path to fielding solutions.

Other efforts by NWDC have included a Maritime Innovation Symposium 2012, Junior Leader Innovation Symposium and Pacific Rim Innovation Symposium. The NWDC website also hosts an innovation blog: <https://www.nwdc.navy.mil/ncoi/blog/default.aspx>. NWDC is known for its stellar reputation as an enabler for the

rapid generation and development of innovations in naval warfighting concepts and doctrine in the joint and coalition arena. So establishing a Navy Center for Innovation at NWDC is a logical choice to advance fresh ideas in maritime operations and naval doctrine.

Young leaders are encouraged to read *The Innovator's Guide* as a first step "to apply the American spirit of ingenuity that is ingrained in all of us" so that they have a solid understanding of what innovation is and why it is essential to the Navy. It is also important to become familiar with proven techniques that will help young leaders become more innovative thinkers.

Young leaders are encouraged to:

- Think deeply.
- Question continuously.
- Debate rigorously.
- Read broadly.
- Write boldly.
- Never give up on a good idea.

NWDC is the Navy's executive agent for the concept development and concept generation program. The program provides a collaborative method for harvesting and transforming ideas into new capabilities by creating a channel for innovation that stimulates creativity and participation from the deckplates

"ONCE A NEW TECHNOLOGY ROLLS OVER YOU, IF YOU'RE NOT PART OF THE STEAMROLLER, YOU'RE PART OF THE ROAD."

- STEWART BRAND

as well as to meet leadership demands for new capabilities.

As the Navy Center for Innovation, NWDC is the entry point for ideas and manager of the process. Through the center website, you can submit an idea, see examples, and follow your idea as it is reviewed by an appropriate organization for adoption or further study.

To keep the momentum going, NWDC periodically conducts live and online forums to increase awareness for innovative thinking, to harvest new ideas and to promote a culture of innovation in the Navy.

To submit a proposal or idea, please use the template located on NWDC's website (<https://www.nwdc.navy.mil/ncoi/Lists/Proposals/NewForm.aspx>) and return the completed form to NWDC_NRFK_INNOVATIONS@navy.mil. ●

FOR MORE INFORMATION
NAVY WARFARE DEVELOPMENT COMMAND
[HTTPS://WWW.NWDC.NAVY.MIL](https://www.nwdc.navy.mil)
NAVY CENTER FOR INNOVATION
[HTTPS://WWW.NWDC.NAVY.MIL/NCOI/](https://www.nwdc.navy.mil/ncoi/)

SHARON ANDERSON is the senior editor of CHIPS. She can be reached at chips@navy.mil.

Capt. Lourdes Neilan

Navy Warfare Development Command Director of Cyberspace Operations

From 2005-2008, Capt. Lourdes Neilan served as the knowledge manager for Carrier Strike Group 8, and then fleeted up as the N6 during the strike group's eight-month deployment to the 5th Fleet area of responsibility. She was selected for promotion to captain in 2008 while assigned to Naval Network Warfare Command as a subject matter expert in fleet communications and information technology. Neilan is the assistant chief of staff overseeing cyberspace operations, information operations and intelligence for information dominance at NWDC, which is also the home of the Navy Center for Innovation. CHIPS asked Neilan to share her ideas about innovation and her work as the head of NWDC's information dominance directorate.



Capt. Lourdes Neilan

Q: Can you talk about your job as the director for cyberspace operations for NWDC?

A: What we're trying to do with cyberspace operations for the Navy is to integrate it into Navy doctrine and assist in the concept development for [the] future of the Navy and how we use cyberspace operations. I'm one of two Information Professional officers at the command, but we are represented across the Information Dominance Corps, although we are very small in numbers. The intel community has the largest representation, but that's because they play a part in exercises playing the red team—the opposition team — so the intel community is represented a little more, but it's working really well.

Q: Red teams?

A: They make up the adversary — terrorist, nation state — playing what-ifs, almost like a chess game. It is really like a chess game when you look at it. War games have moves. Cyberspace is the newest piece. Everyone wants to find a way to make that piece fit into something we've traditionally done — surface warfare, anti-submarine warfare, air warfare — all those areas.

With the addition of cyberspace, the Navy has been integrating it within the traditional warfare areas, done through

doctrine and tactics; more is needed in experimentation. It's interesting, interesting work. It's new for the senior leaders. Some great ideas come from the younger generation but the tactics and way we fight come from the senior generation.

Systems or tactics that used to exist individually between the different communities are now starting to be integrated together. For example, the weather material that comes into the ship is now getting integrated into the other systems that the information warfare community puts on the ship. The Information Dominance Corps [components] are just not stovepipe entities anymore; we're really making it work.

Q: Can you tell us about the Symposium and Pacific Rim Innovation Symposium NWDC hosted. NWDC Commander Rear Adm. Terry Kraft is a strong advocate for innovation; will there be other events in the series?

A: Our campaign to reinvigorate a culture of innovation throughout the Navy started in March with a Maritime Symposium attended by fairly senior leadership from the War College, Office of Naval Research, academia and more. We recognized during this symposium that the senior leadership has to help clear the path to innovation, but the real

innovation often comes from the deck plate — junior leaders — so that's why we held the junior leader symposium.

We had over 400 people on Defense Connect Online (DCO) and in-person at our headquarters. We held a similar event on the West Coast in October for the Pacific Fleet. A lot of the discussion was theoretical, although the two junior leader symposiums included practical workshops on certain problems that the fleet identified during the Pacific Rim exercise. Some very good ideas came out of several brainstorming sessions.

Admiral Kraft personally brought a couple of ideas back from the Pac Rim event and is closely looking at them. We are now moving away from the theoretical and educating junior leaders toward helping them develop their [skills] and get [their ideas] assessed through the proper channels. We're looking at things like online crowdsourcing type of events through [DCO].

We've also stood up a Navy Center for Innovation site on the NWDC website. We want to be a conduit for junior leaders to submit ideas directly to us, which can be done through the site. Since June, we've seen the number of ideas submitted through the site gradually increase. We've also set up some blogs to open a discussion. There's a Navy Center for Innovation blog at <https://www.nwdc.navy.mil/ncoi/blog/default.aspx>.

We're about to launch one on the SIPR

side, too. To really to get down into the tactics we need to move forward on, you need a classified environment. We will continue to look at symposiums and some micro events — probably warfare specific type of events. It's very much alive and kicking.

We want to communicate to people [that] we're not just here to collect information or to collect your great ideas; there's a proactive process to review every submission and either act on it internally or send it to the proper subject matter experts to assess or collapse into other similar initiatives.

Rear Adm. Kraft has also been tasked by the CNO to set up a CNO Advisory Board charged with rapidly assessing ideas and getting them into the pipeline to be acted upon for the fleet.

Q: You mentioned that NWDC empowers employees to think outside the box. In what ways is NWDC encouraging its employees to go beyond the confines of the proverbial box?

A: We are operating and collaborating between directorates all the time to keep ourselves outside the box. For example, our lessons learned and analysis teams created a meta-analysis process for post-deployment briefs that is now be looked at by the fleet.

Technology is also keeping us moving forward. For example, our simulation team is starting to put full motion video into simulation exercises now. And, as I mentioned earlier, some of our war games and exercises now have cyberspace effects built in to stretch the training audience on how to deal with that. That's about where we are.

I think everybody's got to think a little differently in the current environment not because it is your job, or part of your command's mission, but because what [you] do affects other people or other commands. That's the part I think we really need to get better at because it is such an information heavy world now that sometimes you'll come across a piece of information that is relevant to somebody else, but they won't know

"That's the generation that's coming up. They're not like us. And we should celebrate it and let them go ahead. Not to be disrespectful or not understand that there's a basic foundation, but [to know that] yes, you can deviate from what people are doing today because maybe what's happening today may not be the best way to do it. "

that because you have it. So that whole piece of the right information to the right person at the right time is getting worked through now. Because we are able to search and analyze structured and unstructured information, the need to follow rigid rules on storing and discovering information is going away.

Q: One of the main themes of your presentation centered on the next generation, not only taking the helm in development of new products for the warfighter, but also leading the way. What steps do you think the Navy should take to attract the next generation of leaders who want to mimic Steve Jobs' way of thinking?

A: Well, definitely getting out of their way is one thing. Sometimes these ideas just get stifled somewhere as they go up the chain of command to somebody who actually can do something about it. When we had the Junior Leader Innovation Symposium, it was very interesting because I was watching from DCO. As I was watching Adm. [John] Richardson give his presentation, I was also watching to see if there was any relationship between what was being chatted [about on DCO] and what was being presented. So this generation is able to think and observe at the same time. They're thinking a different thought at the same time they're watching a presentation and you wonder if they are [paying attention].

But I really think it's because they're able to multitask so much better. That's the generation that's coming up. They're not like us. And we should celebrate it and let them go ahead. Not to be disrespectful or not understand that there's a basic foundation, but [to know that] yes, you can deviate from what people

are doing today because maybe what's happening today may not be the best way to do it. And then, of course, there's the issue of tools. You know, they want the digital tools. I think Adm. Cecil Haney said it best when he had his innovation symposium: 'Let's give these guys a digital sea bag.' Let them have all the applications that they're going to need to do their job. It's not resident in somebody's head; it's not resident in some analog book. Let them have it the way they understand it. And that's the way they understand it — in an app.

And I think that's great because it's possible in our world that you could lose [connectivity]. When you look at these [natural] disasters, you could lose your communication connectivity and your ability to get your information. But you've got to have it somewhere near you so you can reference it. The one thing that I think Adm. Haney knows for sure about this generation is that they're in the digital world, so give it to them the way that they understand it.

Q: In your opinion, can the constraints the military must operate under be relaxed to allow development and testing of technology products more quickly? Is there any controlled environment in which this can happen?

A: I think DoD recognizes the need for rapid acquisition. NWDC is ready to support new initiatives to deliver the latest technology to the fleet. We always have the fleet in mind when determining where our efforts should be focused. Our only constraint is to not *break* an operational platform. It would be neat if you could take a ship that's being decommissioned and use that as your testing platform and also a training platform. ●

Navy Doctrine Library System

Find the information you need – when you need it

By Sharon Anderson

The first thing you notice about the much improved Navy Doctrine Library System homepage is an image of Alfred Thayer Mahan, United States Navy rear admiral, geostrategist and historian, who has been called “the most important American strategist of the 19th century” and the father of the “sea power” doctrine which is based on the concept that countries with greater naval power will have greater worldwide reach. The concept has had an enormous influence in shaping the strategic thought of navies across the world, especially in the United States. So Mahan’s image is a fitting gateway into the Navy’s library system which aims to empower the fleet and warfighter to carry out the Navy mission more effectively.

FEATURES

The Navy Doctrine Library System is hosted by the Navy Warfare Development Command (NWDC), the Navy’s lead for developing, correlating and disseminating all Navy doctrine. Bob Wilhelm, NWDC’s publishing division manager and Roger Webster, NDLS information manager, demonstrated the library system in late November and explained the redesign was the result of feedback from users who said that information was difficult to research and retrieve on the legacy site.

Former commander of NWDC, Rear Adm. John Kelly, championed a more user friendly system in 2005, explained Wilhelm. The idea was to create an intuitive system based on popular, personalizable sites, like Yahoo, that users are familiar with and use at home, Webster said.

Early prototypes encompassed

XML and widgets and were based on the Semantic Web concept.

Current NWDC Commander, Rear Adm. Terry B. Kraft, initiated the current redesign focused on making it even easier for fleet users to locate information and save it for future reference, like the personalized bookshelves permit. Now Microsoft’s sophisticated ASP.net Web server forms the basis of the user interface with an Oracle 11g database for the back-end.

The NDLS website is well-organized and the information indexed similar to that of a library’s card catalog system. Navigation is within a few easy clicks and the user interface is clean and simple. The top navigation bar has five main tabs that include: Home, Library, Terminology, Tactical Tasks and Links with sub-tabs that delve deeper into mission areas, such as ballistic missile defense and humanitarian assistance/disaster relief.

The Library tab includes folders that expand with information regarding Navy general reference categories and doctrine and tactics, techniques and procedures (TTP) related to intelligence; operations; logistics; planning; command and control; fleet exercises; TACMEMOS (tactical memos); tactical bulletins; Naval Doctrine Publications (NDPS); Navy Wide OPTASKS (operational tasks); mission area bookshelves; allied, multinational and joint doctrine, the Universal Naval Task List; Concepts of Operations (CONOPS); U.S. Coast Guard; and Commander’s Handbooks.

There is a tab that provides the 523 Navy Tactical Tasks (NTA) and the ability to link the Navy Mission

Essential Task List (NMETL) with the Universal Naval Task List.

Within the Terminology tab, users can look up acronyms and cross-reference terms that may mean one thing in the U.S. Army but have a different meaning in the Navy.

A Navy terminologist reviews documents each month and works with the Joint Staff terminologist when necessary to identify and resolve any inconsistencies. A panel of subject matter experts vets all information posted to NDLS so users can be assured that information is authoritative, accurate and timely, Webster said.

According to Wilhelm, information is not meant to just sit on a bookshelf. Users are encouraged to comment and recommend changes through the social networking function on NDLS. For example, each pub has a commenting feature, lists a Stock Number (to order a hard copy in the case of special field manuals, for instance), a Primary Review Authority (PRA) that specifies the issuing command, and an action officer’s (AO) email address. If a user makes a comment, the action officer is prompted to respond and a dialogue ensues with the commenter.

There are about 343 Navy publications and official documents and about 1,000 joint documents, Wilhelm explained. The plethora of information is easily accessed by robust search and filtering capabilities that allow users to fine-tune search features.

CUSTOMIZABLE, EASY-TO-USE

Users can customize their workspace by adding and sharing books with other users in the Bookshelves

area. They can create bookmarks and be alerted to pub changes or any changes in any of the library categories by going to the Subscription tab and selecting the pubs and mission areas that interest them. When a change is made in the categories users select, they are alerted by email. In the What's New tab, users can set a filter to see the new documents that have been approved or issued as a draft in the last 30 days, or, for example, the number of days since they last visited the site.

NDLS SUPPORT

Although the NDLS has a strong search capability, there are two librarians that can assist in conducting research for information that may be hard to find. Wilhelm explained that NDLS includes legacy information and canceled and superseded doctrine and many other pubs which can be useful to users who may be conducting research on legacy equipment that may still be used in the fleet or for users who may be interested in old air or anti-submarine warfare doctrine, for example. Also, publications are frequently renamed or renumbered when they are updated, and users can benefit from the knowledge of an experienced librarian. Webster said, "We have the two best librarians in the Navy."

NDLS is available to any U.S. military or civilian government user with a Common Access Card. The system is available in a classified and unclassified version. The user base is about 5,000 to 6,000 unclassified and 14,000 classified users. Some documents have limited distribution and are closely held, for example, by Special Operations Forces.

Through a Java mapping interface function, users can view spider diagrams of relevant documents on any search topic, as illustrated in Figure 1. By using this functionality, users can find documents they may not have even thought of referencing in their search for information.

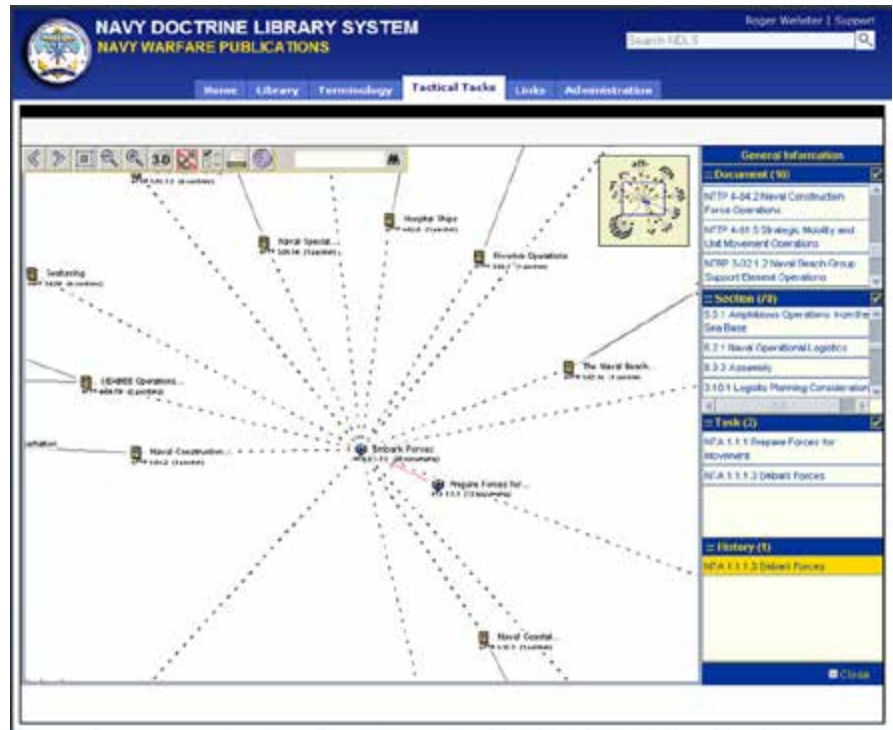


Figure 1. Through a Java mapping interface function, users can view spider diagrams of relevant documents on any search topic, as illustrated in Figure 1.

The Navy Doctrine Library System is available to any U.S. military or civilian government user with a Common Access Card. The system is available in a classified and unclassified version.

There is a "Support" link in the upper right-hand corner of the homepage where users can ask for assistance or provide feedback. At this link, users can find answers to frequently asked questions about NDLS.

Fleet users access a scaled-down version of NDLS through Collaboration at Sea to overcome the limitations of limited bandwidth while operating at sea.

Improvements to NDLS are ongoing and Webster said there is a plan to provide fleet users with more capability. There are five full-time staff members to support NDLS, including two librarians and three employees that maintain the website.

Both Bob Wilhelm and Roger Webster, who incidentally has the perfect

last name for someone working in a library system, are enthusiastic about the improvements to NDLS and encourage and invite CAC holders to visit the Navy Doctrine Library System and provide feedback about their experience. ●

FOR MORE INFORMATION
NAVY WARFARE DEVELOPMENT COMMAND
[HTTPS://WWW.NWDC.NAVY.MIL](https://www.nwdc.navy.mil)

CAC HOLDER ACCESS
NAVY DOCTRINE LIBRARY SYSTEM
[HTTPS://NDLS.NWDC.NAVY.MIL](https://ndls.nwdc.navy.mil)

SHARON ANDERSON is the senior editor of CHIPS. She can be reached at chips@navy.mil.

Remarkable Professionals Ensure Command and Control of Electromagnetic Spectrum

THE DEPARTMENT OF the Navy's highly skilled electromagnetic spectrum professionals are more vital to the mission today than ever before. Without access to the electromagnetic (EM) spectrum, much of the technology that is so integral to our daily lives and military operations could not function, and never before have both peacetime and battlefield access to electromagnetic spectrum been more contested.

High-bandwidth wireless networks in homes, businesses and public spaces and satellite Internet access for ships at sea and troops on the ground have made spectrum an integral part of computer networks. We use remote EM transmitters to control televisions and unlock cars, and cell phones (EM transceivers) to talk, email and text. We rely on radio (EM receiver) and TV for news and entertainment. As inescapable as the EM spectrum is in our personal lives, however, it is essential to military operations. Unprecedented advancements in wireless technology have resulted in critical shortages of this unseen and finite resource. Without the DON's EM workforce's dedication to ensure spectrum access, the department would be unable to maintain, train and equip combat-ready naval forces capable of winning wars, deterring aggression and maintaining freedom of the seas.

Electromagnetic spectrum, the radio frequency (RF) a system operates on, is a common wireless enabler for many, if not most, new communications-electronics systems. Whether acquired as commercial off-the-shelf products or developed specifically to support naval operations, virtually all spectrum-dependent systems require some action by spectrum professionals before they can be brought into operation.



Sgt. David Evans of Hedley, Texas monitors the data traffic and servers that support high-tech satellite communications in the Combat Operations Center.

I AM CONSTANTLY IMPRESSED BY THE COMMITMENT AND THE PASSION OF THESE FOLKS. THEY REALLY, REALLY WANT TO DO GOOD. THE DESIRED DRIVE OF THE FOLKS AT EVERY LEVEL OF THE WORKFORCE FROM THE BOTTOM TO THE TOP SHOULD NOT BE UNDERESTIMATED.

CHRIS KELSALL, DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER, BRANCH HEAD, CYBERSPACE/IT WORKFORCE

New spectrum-dependent systems must comply with national and international regulations meant to protect existing users and ensure equitable spectrum access. Ensuring a new system will not interfere with current users is essential

to prevent interruptions, degradation or limitations to the effective performance of a system.

Because spectrum is a finite resource, sometimes a frequency band is not available for an emerging technology.

PHOTO BY MASTER SGT. PETER WALZ.

To accommodate the entrant, a process called "reallocation" is employed. Spectrum reallocation can be arduous, requiring years of careful national or international negotiations. Spectrum professionals must be vigilant to ensure that agreements reached in negotiations do not negatively affect DON operations. So, in addition to being exceptional technical experts, DON spectrum professionals are skilled negotiators.

One of the spectrum workforce's most fundamental duties is continuous review and evaluation of the DON's radio frequency use to ensure naval forces' ability to operate effectively with minimal impact to the electromagnetic environment. New commercial and consumer uses of spectrum are introduced almost daily, increasing global demand. The resulting changes to national regulations and international treaties demand constant reevaluation and reassessment. The management of increasingly complex systems and their access to the finite EM spectrum in a chaotic environment is just business as usual for the DON's incomparable spectrum management professionals.

The entire DON electromagnetic spectrum workforce of military, civilian and contractor personnel totals fewer than 500 individuals. However, when combined with professionals from the other military departments, federal agencies, the Federal Communications Commission, as well as commercial and private spectrum users, a large workforce of dedicated professionals ensures that the United States EM environment supports cutting-edge wireless technology. Through close coordination and skillful negotiations, these professional spectrum managers are able to ensure consumer wireless technology is able to operate in the same environment along with high-powered commercial and military systems.

IN 1967, WHILE ATTACHED TO THE CHIEF OF NAVAL OPERATIONS, VICE ADMIRAL JON L. BOYES FAMOUSLY STATED: "RADIO FREQUENCY (RF) MANAGEMENT IS DONE BY EXPERTS WHO MELD YEARS OF EXPERIENCE WITH A CURIOUS BLEND OF REGULATIONS, ELECTRONICS POLITICS AND NOT A BIT OF LARCENY. THEY JUSTIFY REQUIREMENTS, HORSE TRADE, COERCE, BLUFF AND GAMBLE WITH AN INTUITION THAT CANNOT BE TAUGHT OTHER THAN BY LONG EXPERIENCE."

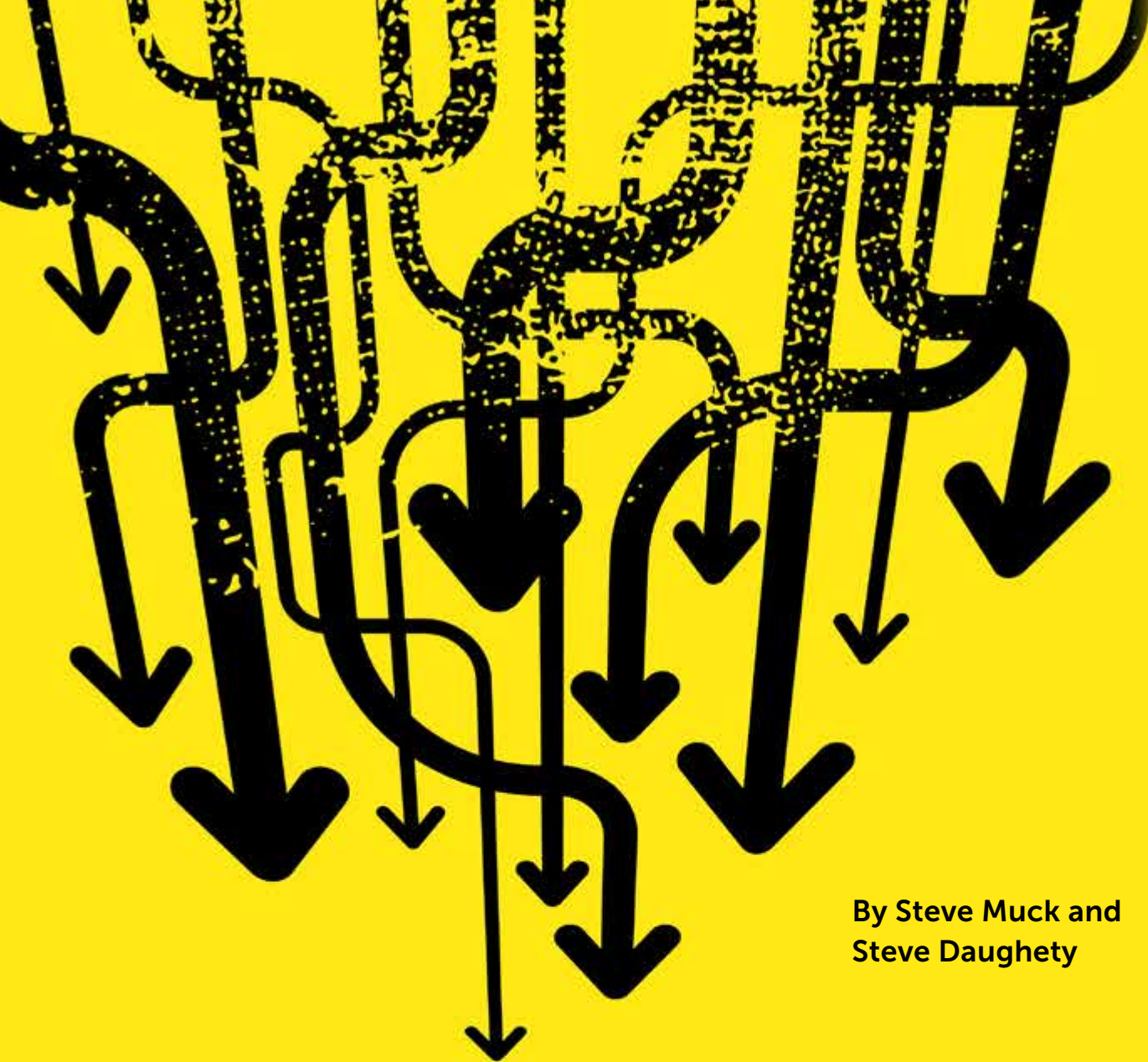
Most spectrum managers learn their skills through specialized technical schools while others got their start in the military. A spectrum manager must develop a mastery of general communications policy, as well as the technology and approved architecture, in order to function as a technical authority. Spectrum managers' technical mastery must extend beyond the ability to recommend certain frequencies or frequency bands.

The scope of training includes: regulation of spectrum management; principles of spectrum management administration; mathematics of spectrum management; communication-electronics principles; spectrum planning for line-of-sight, troposcatter and satellite communications systems; navigational aids, radar and non-communications systems; electromagnetic environmental effects; spectrum management in a joint environment and training in service-automated tools.

The DON has long supported professional development. DON spectrum

management professionals give back to their community as instructors for the Electromagnetic Spectrum Management Course on Keesler Air Force Base in Biloxi, Miss. Such schools produce a workforce capable of ensuring that the DON's latest acquisitions are employed to their maximum effectiveness with the least possible impact to the electromagnetic spectrum. Continuous curriculum revision at these schools ensures that new spectrum managers graduate with the knowledge and skills necessary to make immediate mission support contributions to the DON. Ongoing professional development helps the electromagnetic spectrum workforce keep pace with the frenetic pace of innovations in spectrum dependent technology. ●

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



**By Steve Muck and
Steve Daughety**

REDUCING THE USE OF SOCIAL SECURITY NUMBERS

A GOOD NEWS STORY

IN ACCORDANCE WITH FEDERAL LAWS requiring agencies to establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of personally identifiable information, the Department of the Navy (DON) continues to make progress in reducing the use of Social Security numbers (SSN) in business processes under the department's control. As the department's Senior Military Component Official for Privacy Safeguards, the DON Chief Information Officer has instituted a series of policies and steps that commands must take to be applied to information technology systems, shared drives, computer networks, email, paper records and websites to ensure privacy of personal information. The following success story illustrates how an organization developed a strategy to significantly reduce reliance on SSNs and better protect the privacy of DON personnel.

The Naval Education and Training Command (NETC) directed a complete review of all forms, IT systems and processes to determine and establish a baseline. Each NETC form, IT system and process was reviewed and recorded. The review identified:

- Where SSNs were collected;
- What authority allowed continued SSN use;
- If SSNs could be eliminated, masked or truncated; and
- If SSNs could be replaced with the Department of Defense identification number or other unique identifier.

The goal was to reduce the collection and use of SSNs to the bare minimum across the command without negatively affecting the NETC mission.

A program manager was assigned, teams were established, charters were developed, timelines were created, and processes were validated. After eight months of hard work, NETC was able to:

- Justify continued collection of SSNs in specific required instances;
- Begin replacing SSNs with DoD ID numbers;
- Eliminate the collection of SSNs where possible;
- Crosswalk SSNs and DoD ID numbers to allow substitution in IT systems; and
- Coordinate substitution with interfacing IT systems.

NETC rejected the notion that substituting an SSN with another unique identifier "is too hard." Instead, the NETC team established a baseline, determined their resources, and discovered ways to significantly reduce the collection and use of SSNs. As a result of their efforts, the NETC team considerably improved the protection of DON employees' privacy. The process is ongoing and significant progress continues in the reduction and use of SSNs.

Commands that would like to benefit from the experience NETC has gained through this process may contact Ivan Rivas at ivan.rivas.ctr@navy.mil. Additionally, SSN reduction resources can be accessed on the DON CIO website: www.doncio.navy.mil/privacy. ●

STEVE MUCK is the Department of the Navy deputy privacy officer.

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

THE DON'S THREE PHASE SSN REDUCTION PLAN

PHASE 1: In July 2010, the DON Chief Information Officer (CIO) released DON CIO Washington DC 192101Z Jul 10, "Department of the Navy Social Security Number (SSN) Reduction Plan for Forms Phase One," requiring commands to:

- Review all DON forms to identify those that collect SSNs and justify continued collection if necessary; and
- Identify forms that are not official DON forms and discontinue or take steps to make the form official.

PHASE 2: In June 2011, the DON CIO issued a tasking for commands requiring:

- Review of all IT systems to identify those that collect SSNs;
- Justification to continue collection of SSNs in accordance with the Justification Memo for the Continued Collection of the SSN issued by the DON CIO and available at www.doncio.navy.mil/ContentView.aspx?id=2423;
- Identification of those systems that could eliminate collection; and
- Identification of those that could substitute another unique identifier.

PHASE 3: In February 2012, "Department of the Navy Social Security Number (SSN) Reduction Plan Phase Three," DON CIO Washington DC 171625Z Feb 12, (www.doncio.navy.mil/ContentView.aspx?id=3757) was released and:

- Authorizes the use of DoD ID numbers as substitutes for SSNs;
- Requires that collection of SSNs in memorandums, letters, spreadsheets, hard copy lists, electronic lists and surveys meet acceptable use criteria and other Privacy Act considerations;
- States that any form of an SSN will now be treated with the same sensitivity as the full SSN and considered a reportable breach if compromised;
- Prohibits SSNs in rosters; and
- Provides new policy when scanning and faxing PII.

In November 2012, the DON CIO revised the fax policy to make it less restrictive with the release of "Department of the Navy Fax Policy," DON CIO Washington DC DTG 081745Z NOV 12 – www.doncio.navy.mil/ContentView.aspx?id=4267.

Navy Tactical Afloat Network Approved for Limited Deployment

CANES to the Rescue

By Sharon Anderson

FIVE LEGACY NETWORKS, EACH WITH A DEDICATED INFRASTRUCTURE, WILL BE REPLACED BY THE NAVY'S CONSOLIDATED AFLOAT NETWORK AND ENTERPRISE SERVICES, OR CANES, A STREAMLINED COMMON COMPUTING INFRASTRUCTURE FOR C4I — COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS AND INTELLIGENCE APPLICATIONS — AND HARDWARE COMPONENTS THAT WILL DELIVER VIDEO, DATA AND NETWORK SERVICES TO THE FLEET.

The CANES program received approval to enter the production and deployment phase Dec. 14. The Milestone "C" acquisition decision memorandum was approved by Under Secretary of Defense for Acquisition, Technology and Logistics Frank Kendall. The decision commits the Department of Defense to production and authorizes the program to begin limited deployment. The program was approved for limited fielding of 29 CANES units with 23 installations.

The CANES program is managed by the Program Executive Officer for C4I. To acquire CANES, PEO C4I used a game-changing business model that encourages vigorous industry competition that when combined with an open architecture design, reliance on commercial off-the-shelf technology and government-owned data rights decreases total ownership costs for the Navy and delivers operational warfighting agility.

"CANES is more than a system, it is also a new business model for delivering capability to the fleet. It takes five legacy networks and combines them into one network, allowing us to

streamline support, training and operating procedures," said Rear Adm. Jerry Burroughs, program executive officer for C4I.

The development of CANES is in response to fleet demand for a robust tactical network. CANES is made up of two main subprograms: the common computing environment, which consolidates all the hardware, racks, servers and communications media for shipboard applications, and the afloat core services, which is a consolidation of applications in use today.

Capt. D.J. LeGoff, PEO C4I, tactical networks program manager (PMW 160) and program manager for CANES, said CANES standardizes infrastructure and components which decreases the complexity and costs of training and sustainment.

"Applications that ride on CANES are owned by other programs of record with their own resource sponsors. CANES provides the common infrastructure and replaces about 135 legacy systems. The standard baseline makes it easier for Sailors to operate and maintain CANES," LeGoff said. "Hardware refresh is planned and funded for every four years and software refresh every two years and assures keeping pace with technology — it eliminates the headaches of multiple versions of hardware and software and also decreases threats to the network."

CANES technology is scalable, meaning there are minor variations depending on the ship class — which assures the same infrastructure from one ship to another.

"Today, we have many different vari-

ants of networks out there that present significant supportability and information assurance challenges," Burroughs said. "CANES also has significant IA capability built into it that we've never had before, which will allow us to ensure we're delivering secure capability that stays relevant to the warfighter."

"IA in legacy systems was bolted-on or patched in," LeGoff said. "Ten to 15 years ago when we were building systems the risks were not the same as they are now, also new threats have emerged over the years. Information assurance is the foundation that we used to build CANES. It makes protecting CANES easier — as well as the hardware and software refresh."

There is an established training pipeline for the Sailors who will be operating CANES — information systems technicians receive training in a continuum from beginner to journeyman level which includes a 26-week course that includes courses in Microsoft certifications. Then ITs deploy on ships for real fleet experience and return to the classroom in "C" School. A five-week CANES course is in development in San Diego and will be ready for students in February.

Sailors will be able to perform routine IA, but most network elements will be locked down to ensure system integrity and configuration management.

Commander Operational Test and Evaluation Force conducted an operational assessment of CANES in September. While the final report from that assessment won't be available until early next year, initial evaluation contributed to a successful Milestone

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

Rear Adm. Jerry Burroughs
PEO C4I

Ultimately, CANES will be deployed to more than 190 ships, submarines and Maritime Operations Centers by 2020.

C Decision. Following the decision, work began on the San Diego-based destroyer USS Milius (DDG 69) Dec. 17. Installation will take about 18 weeks to strip out the legacy hardware and systems and install CANES.

"But we are not tying up the Milius for 18 weeks; she is undergoing other types of maintenance as part of the ship's availability alterations to ships accomplished by alteration installation teams," Burroughs said.

At the same time, LeGoff and Burroughs said they hope to decrease the time it takes to install CANES on each ship because the cost savings and benefits to the Navy are so great, and they are confident that they can.

"With the lessons learned from installation on Milius, we hope to shrink the 18-week installation estimate down. We fully expect to see some surprises, but we are fully prepared for that," LeGoff said.

Ultimately, CANES will be deployed to more than 190 ships, submarines and Maritime Operations Centers by 2020.

LeGoff said his office is working with



SAN DIEGO (Sept. 11, 2012) The Arleigh Burke-class guided-missile destroyer USS Milius (DDG 69) returns to homeport Naval Base San Diego after an eight-month independent deployment to the western Pacific and U.S. Central Command areas of responsibility. Milius enhanced relationships with foreign coastal states, provided local security to merchantmen and fishermen in international waters, and conducted approach and assistance visits to mariners at sea. The ship also conducted Iraqi infrastructure protection exercises with the U.S. Coast Guard, Kuwaiti Navy and British Royal Navy forces. U.S. Navy photo by Mass Communication Specialist 2nd Class Rosalie Garcia.

Naval Sea Systems Command and the Navy to obtain funding to install CANES on the other 100 or so other ships in the fleet.

"The first set of ships for CANES [deployment] is determined first and foremost by age — those with the oldest and most problematic legacy systems, but this can be limited by the maintenance availability which depends on a lot of factors and is controlled by NAVSEA," LeGoff said.

In May 2012, PEO C4I announced that CANES proved to be 44 percent cheaper than expected compared to the government's initial cost estimate. LeGoff credited the CANES business model for the lower than expected costs. However, the Navy is not locked in to the current limited deployment phase contract, which was awarded in February 2013. LeGoff said the Navy will re-compete the contract for the next round of ships selected for CANES deployment. The open architecture and COTS technology ensure that multiple vendors can submit bids.

"We provide all the system docu-

mentation [to potential bidders] and the Navy owns all the data rights to the system ... and offering a proposal that doesn't meet open standards is the best way to get kicked off the contract," LeGoff said.

The Navy is also taking the lead as the software systems integrator and will maintain the segment of CANES called afloat core services, the services-oriented architecture that forms a key part of the common system. The result will be products that are entirely open-source, LeGoff explained.

CANES encompasses the full gamut of security classification up to sensitive compartmented information and coalition access. It does not include the ship's machinery and real-time combat systems but mostly all a ship's IT systems are included, LeGoff said.

Full rate production for CANES is planned for spring/summer period in 2014. ●

SHARON ANDERSON is the senior editor of CHIPS. She can be reached at chips@navy.mil.

SSC ATLANTIC RECIPIENT OF PRESTIGIOUS USD(AT&L) WORKFORCE DEVELOPMENT GOLD AWARD

By Diane Owens

Space and Naval Warfare Systems Center Atlantic officials were notified Oct. 26 that the center was selected to receive the 2012 Under Secretary of Defense for Acquisition, Technology and Logistics Workforce Development Gold Award for large organizations (more than 500 employees). The award recognizes SSC Atlantic as a Department of Defense acquisition, technology and logistics organization that has made exemplary contributions to career-long development of its acquisition workforce, promoting the goal of a high quality, agile and ethical workforce. The award program also identifies best practices for other USD (AT&L) organizations to follow.

Maintaining and enhancing previous learning and development programs and being proactive in providing employees with additional career-development activities enabled the center to advance from recognition as a silver award recipient in 2011 to achieving gold status in 2012.

The center's total force management competency leads submitted the award application which described the competency aligned organization/integrated product team (CAO/IPT) structure used by SSC Atlantic, and stated that SSC Atlantic's fiscal year 2012 tactical training plan and budget exceeded \$7.3 million and included tuition assistance, graduate programs, process improvement, leadership development programs, development of business processes, and specialized training focused on building capability to deliver new technologies to customers. More than \$1 million of that budget was invested in academics and \$1.5 million was expended (as of the Aug. 1 application date) on labor costs for the acquisition workforce to attend training. More than 500 employees have pursued undergraduate and graduate coursework

Assistant Secretary of Defense (Acquisition) Katrina G. McFarland presents the USD (AT&L) Workforce Development Gold Award to Space and Naval Warfare Systems Center Atlantic Executive Director Christopher Miller Dec. 17, 2012 in the Hall of Heroes at the Pentagon. The award recognizes SSC Atlantic as a DoD organization that has made exemplary contributions to career-long development for its acquisition workforce, promoting the goal of a high quality, agile and ethical workforce.

with an investment exceeding \$6 million since fiscal year 2008, and the number of employees who have earned degrees has increased to a historic high of more than 65 percent of the workforce.

A strategic partnership with Defense Acquisition University (DAU) resulted in more than 17 weeks of onsite courses being offered to personnel, which greatly reduced travel costs since no DAU campus is within commuting distance of Charleston and more than 1,500 members of the AT&L workforce were previously required to travel to obtain classroom training.

Other initiatives to provide learning and development opportunities to employees, supervisors and executives, included new employee onboarding and orientation sessions, the mid-career leadership development program, executive coaching, the council of supervisors, leadership development workshops, telework, employee yes/no surveys, strategic communications, the IPT lead accreditation program, a variety of mentoring programs, new professional programs, and community outreach focused on science, technology, engineering and math careers. The award was presented to SSC Atlantic Executive Director Christopher Miller



at the USD(AT&L) Acquisition awards ceremony Dec. 17 at the Hall of Heroes in the Pentagon.

Commanding Officer for SSC Atlantic Capt. Mark Glover said, "I am proud to command an organization with such a talented workforce that every day makes IT (information technology) count for the warfighter and the nation."

Congratulations on successfully "going for the gold!" ●

DIANE OWENS is the employee newsletter editor for SPAWARSYSCEN Atlantic.

SSC ATLANTIC rapidly delivers and supports solutions that enable information dominance for naval, joint, national and coalition warfighters. The organization is a leading edge Navy engineering center that designs, builds, tests, fields and supports many of the finest frontline advanced command, control, communications, computer, intelligence, surveillance and reconnaissance (C4ISR) systems in use today, and those being planned for the future. SSC Atlantic's headquarters are located in Charleston, S.C., with major detachments in Hampton Roads, Va., New Orleans, La., Washington D.C. and several other Southeastern U.S. locations. SSC Atlantic overseas locations are in Europe, the Middle East and Antarctica.

SPAWAR ENGINEER HONORED with MULTIPLE PRESTIGIOUS AWARDS

By *Patric Petrie*

Ron Broersma, a Space and Naval Warfare (SPAWAR) Systems Center Pacific information technology division chief engineer, received one of the Defense Department's top awards, the DoD High Performance Computing Modernization Program (HPCMP) Hero Award for long-term sustained contributions. Broersma was presented the award Jan. 7 by SSC Pacific Commanding Officer Capt. Joe Beel and Executive Director Carmela Keeney.

Broersma, a 2010 winner of SSC Pacific's prestigious Lauritsen-Bennett Award, and SPAWAR's enterprise network security manager, was chosen for the honor for his overall contribution to the science and technology (S&T) and test and evaluation (T&E) communities for the last five years. In a letter to the award's nominating committee, Broersma was cited by HPCMP's associate director for networking for his outstanding support for the organization through the Defense Research and Engineering Network (DREN) program.

Broersma's technical expertise and contributions to the DREN (where he has served as chief engineer for the past decade) were saluted as "second to none." Broersma and his team successfully implemented a suite of carrier-grade support services, including state-of-the-art video teleconferencing, domain name service, Linux distribution repositories, and utilization statistics for DREN customers. These services were installed in multiple enterprise-class data centers.

The HPCMP supports DoD objectives through research, development, test and evaluation. The HPCMP was initiated in 1992 in response to congressional direction to modernize DoD laboratories' high performance computing capabilities. The HPCMP was assembled out of

SPAWARSYSCEN Pacific Commanding Officer Capt. Joe Beel and Executive Director Carmela Keeney present Ron Broersma with the Department of Defense High Performance Computing Modernization Program Hero Award for sustained contributions to the HPCMP Jan. 7, 2013 at SSC Pacific located in San Diego, Calif.



a collection of small high performance computing departments, each with a rich history of supercomputing experience that had independently evolved within the Army, Air Force and Navy laboratories and test centers.

HPC tools are used to solve complicated and time-consuming problems. Researchers expand their toolkit to solve modern military and security problems using HPC hardware and software. Programs assess technical and management risks, such as performance, time, available resources, cost and schedule.

Through HPC solutions, programs gain knowledge to protect our military through new weapons systems, prepare U.S. aircraft for overseas deployments in Afghanistan and Iraq, and assist long-term weather predictions to plan humanitarian and military operations throughout the world.

In addition to receiving the DoD award, Broersma was also recently honored as one of four recipients of the IPv6 Forum Internet Pioneer award. The IPv6 Forum is a worldwide consortium of leading Internet service vendors, national research and education networks, and international Internet service providers.

The award recognizes significant achievement and hard work from

individuals who excel in their efforts to support the mission of IPv6 deployment across world geographies for a cause greater than their own self interest.

The IPv6 Forum's mission is to promote the rapidly advancing technology of IPv6 by improving market and user awareness, creating a quality and secure next-generation Internet, and allowing worldwide access to knowledge and technology.

Broersma was presented with the HPCMP Hero Award on Jan. 7, 2013, by SSC Pacific's Commanding Officer Capt. Joe Beel and Executive Director Carmela Keeney. ●

PATRIC PETRIE is a lead writer for SPAWARSYSCEN Pacific.

SPACE AND NAVAL WARFARE SYSTEMS CENTER PACIFIC provides the U.S. Navy and military with essential capabilities in the areas of command and control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). SSC Pacific provides the full spectrum of C4ISR capabilities from basic research and prototype development, to extensive test and evaluation services, through systems engineering and integration, to installation and life-cycle support of fielded systems.

Enlisted Information Dominance Warfare Specialist Program

Program changes expand opportunities for enlisted ID warfare qualification

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

The Enlisted Information Dominance Warfare Specialist designation was implemented in 2010 to enhance the Navy's understanding of information dominance to increase warfighting and mission effectiveness. The EIDWS warfare qualification specifically focused on Information Dominance Corps personnel in the aerographer's mate (AG), cryptologic technician (CT), intelligence specialist (IS) and information systems technician (IT) ratings.

Navy Cyber Forces Command, as the executive agent for the EIDWS program, reviewed the program and identified a lack of qualification opportunities for Sailors in the AG, IS, CT and IT ratings assigned to commands not under IDC command administrative control. Navy Cyber Forces determined that as of October 2012, only 50 percent of IDC enlisted personnel were eligible to enroll in the EIDWS program.

To support the Navy "Strategy for Achieving Information Dominance" and enhance the professional development of IDC enlisted personnel, the provisions of NAVADMIN 343/12 (www.public.navy.mil/bupers-npc/reference/messages/Documents/NAVADMINS/NAV2012/NAV12343.txt) expand the program to allow all IDC personnel an opportunity to enroll in any existing certification program. Any IDC Sailor having reasonable access to a command with an established EIDWS program may enroll in that command's program. This additional opportunity for earning enlisted warfare qualifications will enhance the professional development of all IDC Sailors and increase warfighting capabilities and cyber expertise throughout the Navy.

Shipboard personnel attached to com-

mands without a program may enroll and qualify via an approved program within their strike group, amphibious readiness group (ARG) or task force. If not assigned to a strike group, ARG or task force. Shipboard IDC personnel may enroll at any reasonably accessible approved EIDWS program. Primary command personnel qualification standards (PQS) and warfare qualifications, based on command function, must be obtained prior to authorization to enroll in an EIDWS program.

New program validation and approval will continue as needed to support emerging ID mission expansion. Commands currently in the process of EIDWS program development may continue with program certification efforts. Specifically, aircraft carriers, amphibious assault ships and fleet commands interested in creating an EIDWS program are directed to follow the guidance outlined in COMNAVCYBERFOR Instruction 1414.1.

Prior to the release of NAVADMIN 343/12, only 50.4 percent of IDC enlisted personnel, or 12,689 of 25,172, were eligible to enroll. Program expansion increases opportunities for more than 90 percent of IDC personnel in the AG, CT, IS and IT ratings.

"Realizing that it is virtually impossible for us to extend the opportunity

to 100 percent of the Information Dominance Corps, a 90 percent solution is a great number. In keeping with (retired) MCPON West's goal of having 'all Sailors wearing a warfare pin,' our expansion not only drives toward this stated goal but exceeds the efforts of all other enlisted warfare qualification efforts. Every eligible Sailor who pursues this voluntary opportunity will bolster their own professional resume and enhance the warfighting capability of their own commanders. The efforts of Senior Ross and Senior Morrow in leading the cradle-to-grave charge in this effort have been remarkable. The EIDWS remains our Navy's most 'coveted and sought after' warfare pin," said (now retired) FORCM(IDW/AW/SW) Jay Powers, Force Master Chief for Navy Cyber Forces Command.

So far, 121 commands have an approved EIDWS program, with 22 in the process of validation. More than 3,300 Sailors have already qualified. An updated EIDWS instruction will be released containing program revisions and updated requirements. In the meantime, please refer to NAVADMIN 343/12 for guidance. ●

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

For assistance please contact:

NAVCYBERFOR Force Master Chief: FORCM Steve Giordano at (757) 417-6705; DSN: 537-6705 or steven.giordano@navy.mil.

EIDWS program coordinator: CTNCS Russell Ross at (757) 417-7931 ext. 8; DSN: 537-7931 ext. 8 or russell.a.ross1@navy.mil.

Program Coordinator: ITCS STEFAN MORROW at (757) 417-6757 ext. 1; DSN: 537-6757 ext. 1 or stefan.morrow@navy.mil.

Large Number of Center for Information Dominance Chiefs Pinned

By Gary Nichols, CID Public Affairs

Across the fleet, from naval installations to ships at sea to air stations, one of the most treasured and time-honored traditions is the pinning of the golden anchors for the first time on the collars of the Navy's newest chief petty officers.

On Sept. 14 at the atrium of the National Museum of Naval Aviation, 32 new chief petty officers were pinned from the Center for Information Dominance (CID) Unit Corry Station, Navy Information Operations Command (NIOC) Pensacola and Naval Hospital Pensacola.

Throughout the CID domain, there were 206 E-6s who were board-eligible for advancement to chief petty officer. Of these, 59 were selected, resulting in an impressive 29 percent selection rate to chief petty officer.

"Typically the advancement rate for chief petty officers is about 20 percent or lower," CID domain career adviser Eric Tremaine said. "The high numbers for CID reflect the high caliber of personnel we have from across the CID domain."

Thirteen of these new chiefs were based at CID Unit Corry Station, and the remainder were scattered throughout the CID domain, primarily at the other commands: CID Unit Monterey, Fleet Intelligence Training Command at San Diego and Navy Marine Corps Intelligence Training Command at Dam Neck, Va.

"This is proof that the fleet is sending the cream of the crop to CID for instructor duty, and it shows in the high advancement rate for our new chief petty officers," CID Command Master Chief Travis Brummer said. "This is a win-win situation for everybody: our students, our instructors and the Navy."

Naval Education and Training



PENSACOLA, Fla. (Sept. 14, 2012) FY-13 Chief Petty Officers during a pinning ceremony at the National Museum of Naval Aviation on board Naval Air Station Pensacola. Throughout the CID domain, there were 206 E-6s who were board-eligible for advancement to chief petty officer. Of these, 59 were selected, resulting in an impressive 29 percent selection rate to chief petty officer. U.S. Navy photo by Cryptologic Technician Collection 1st Class Joshua Pugh.

Command (NETC) Force Master Chief (AW/SW) April Beldo, who was the guest speaker during the pinning ceremony, had words of encouragement and advice for the newly pinned chief petty officers.

"I am very passionate about being a chief petty officer, and a part of the chief's mess," Beldo said. She related the pride she felt in September 1995 when she received her gold anchors while onboard the USS Abraham Lincoln. "I

remember it like it was just yesterday," she said. "It is still one of the most proud times of my life."

On March 13, 1893, U.S. Navy Regulation Circular No. 1 established the rating of chief petty officer. In the past 119 years the chief's pinning ceremony has become one of the Navy's most time-honored ceremonies. Earning the right to wear the gold anchors is not easy, and the process of becoming a chief petty officer is a long and difficult

road — and is arguably the greatest achievement a Sailor can achieve. The ceremony signifies a new position of leadership and responsibility for the new E-7s. For the newly selected chief petty officers, the pinning ceremony represents the culmination of four weeks of the induction process, a rigorous training schedule involving physical training, and leadership, teamwork, time management, and Navy history and tradition course work.

Information Systems Technician “A” school instructor Chief Information Systems Technician Arian Sanchez said the induction process was more challenging than he expected. “The level of teamwork and the level of camaraderie that I’ve learned through this process is unequalled so far,” Sanchez said. “The biggest difference he said is that with the E-5 and E-6 mindset you tend to look out for yourself and your career, and by extension, you are helping the Navy; as a chief petty officer, you learn to take care of others first and foremost.”

“To the newest members of the mess this is your time; I want you to embrace it, I want you to have fun and I want you to look forward to the days ahead,” Beldo said. “You are now ‘the Chief,’ the backbone of the Navy.”

CID Unit Corry Station Commanding Officer Cmdr. Luciana Sung also congratulated the new chief petty officers.

“Pinning our newest chiefs is always a great honor and we’re all very proud of our chief’s mess for all the mentoring and sponsoring they provided for this season,” Sung said.

CID Unit Corry Station Senior Enlisted Leader Master Chief Cryptologic Technician (Collection) (SW/AW) Jimmy Dawkins said he was proud to be part of the process that helped to develop the Navy’s newest crop of chief petty officers, and offered words of encouragement to the new leaders, who after four weeks of intensive training during the induction process were eager to step into their new role as the Navy’s newest chief petty officers.

“Step up to the challenge,” Dawkins



PENSACOLA, Fla. (Sept. 14, 2012) Center for Information Dominance Commanding Officer Capt. Susan K. Cerovsky congratulates newly pinned chief petty officers at the National Museum of Naval Aviation on board Naval Air Station Pensacola. U.S. Navy photo by Cryptologic Technician Collection 1st Class Joshua Pugh.

The chief petty officer pinning ceremony signifies a new position of leadership and responsibility. For the newly selected chief petty officers, the ceremony represents the culmination of four weeks of the induction process, a rigorous training schedule involving physical training, and leadership, teamwork, time management, and Navy history and tradition course work.

said. “Lead your Sailors, guide them, mentor them, and understand that you have more impact on that Sailor’s life than you could ever fathom.”

At the conclusion of the pinning ceremony, the new chiefs seemed relieved but exhilarated. “It’s the greatest point in my military career,” Chief Cryptologic Technician (Technical) (IDS/SW) Aaron Ricker said. “I’ve never been so excited and so proud.”

“I am very proud of each and every one of you, and look forward to serving with you in the fleet,” Beldo said. CID 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. ●

GARY NICHOLS is the public affairs officer for the Center for Information Dominance.

FOR MORE INFORMATION
Center for Information Dominance News
www.navy.mil/www.navy.mil/local/corry/

Center for Information Dominance
www.netc.navy.mil/centers/ceninfodom

Hull Swap – a Sea Story

SPAWAR personnel install critical shipboard software upgrade

By Sharon Anderson

IN APRIL 2012, THE BIG-DECK AMPHIBIOUS ASSAULT SHIPS USS BONHOMME RICHARD (LHD 6), AND USS ESSEX (LHD 2), STATIONED IN SASEBO, JAPAN, COMPLETED A HULL SWAP DURING WHICH THE CREWS WORKED DILIGENTLY LEARNING THE DIFFERENCES BETWEEN THE NETWORK SYSTEMS AND SOFTWARE APPLICATIONS INSTALLED ON EACH OF THE SHIPS.

THE CHALLENGE

Hull swap, or ship rotation, is part of the Navy's long-range plan to routinely replace older ships assigned to the Navy's Forward Deployed Naval Force with newer or more capable ships. In a hull swap, ships switch places, but crews and families remain in their homeport.

Initially planned for one month in duration, the timeframe for the hull swap between Bonhomme Richard and Essex was reduced to two weeks due to the fleet's tight operating schedule. The compressed schedule allowed the forward deployment of Bonhomme Richard to ensure the ability of Commander U.S. 7th Fleet to fulfill the U.S. government's commitment to the defense of Japan and the maintenance of international peace and security in the Far East in support of the Treaty of Mutual Cooperation and Security.

Critical to the success of the hull swap was the deployment of an automated solution to transition Naval Tactical Command Support System (NTCSS) personnel data between the two ships. Personnel from the Navy's Command and Control Program Office, PMW 150, under the Program Executive Office for Command, Control, Communications, Computers and Intelligence (C4I), led the effort by gathering requirements and planning and coordinating efforts with Space and Naval Warfare Systems Cen-



SAN DIEGO (OCT. 24, 2012) THE AMPHIBIOUS ASSAULT SHIP USS ESSEX (LHD 2) IS MOORED WITH THE ASSIGNED MESSING AND BERTHING BARGE AT NAVAL BASE SAN DIEGO. ESSEX IS AT THE BEGINNING OF AN 18-MONTH PLANNED MAINTENANCE PERIOD. THE U.S. NAVY IS RELIABLE, FLEXIBLE, AND READY TO RESPOND WORLDWIDE ON, ABOVE, AND BELOW THE SEA. JOIN THE CONVERSATION ON SOCIAL MEDIA USING #WARFIGHTING. U.S. NAVY PHOTO BY SENIOR CHIEF MASS COMMUNICATION SPECIALIST JOE KANE.

ters Atlantic and Pacific. The team consisted of 20 employees from PMW 150, SSC Pacific and its detachment in Yokosuka, and SSC Atlantic. Their combined actions resulted in a seamless transition of maintenance, supply and administrative capabilities between the ships and enabled the hull swap to be successfully executed as scheduled.

The SSC Atlantic team's contribution involved designing and engineering the automated solution to transition NTCSS personnel data between the two ships. One of the major differences between the applications installed on the ships was the NTCSS software version used. Essex had the legacy CY04 version of NTCSS, whereas the Bonhomme Richard used the newest release, Patriot, which is two releases ahead of the CY04 version. Working with two different versions created unique challenges for the team, but swapping NTCSS versions on the ships was not an option due to the complexity of the software configurations and underlying hardware platforms and network components unique to each

NTCSS version. In addition, the solution had to be ready for testing, installation and validation by SSC Pacific personnel in the compressed 13-day window — April 9 to 21 — with training also completed for both ships' crews to allow Essex to deploy to San Diego for a much-needed shipyard overhaul and repairs. The only viable option was to develop an automated database routine that could quickly download personnel data from the Essex and upload it to the Bonhomme Richard. Also, the Bonhomme Richard's Patriot R-ADM database had to be downgraded to the CY04 version and loaded on the Essex.

NAVAL TACTICAL COMMAND SUPPORT SYSTEM

NTCSS is a multi-application information system that provides standard information resource management to afloat and shore-based fleet activities. NTCSS was created by the merger of three long-time key programs: the Shipboard Non-Tactical Automated Data Processing Program (SNAP), the Naval Aviation Logistics

Command Management Information System (NALCOMIS) and Maintenance Resource Management System (MRMS).

NTCSS provides a full range of standardized mission support automated data processing hardware and software to support management of logistics information, personnel, material, equipment maintenance, and the funding required to maintain and operate ships, submarines and aircraft in support of the Navy and Marine Corps. Major NTCSS components include personnel data stored in the Relational Administrative Data Management (R-ADM) application, one of the primary NTCSS applications, and in NTCSS ORG, an application containing the ship's organizational structure, for example, code information, such as the department, division and work centers where personnel are assigned. NTCSS also includes Relational Supply (RSupply), Organizational Maintenance Management System New Generation (OMMS-NG) and NALCOMIS.

R-ADM is the authoritative database for afloat activities that use the NTCSS suite; it is designed to capture individual level unit training, personnel qualification standards (PQS) and certifications. R-ADM also tracks training exercises and enables creation, management and maintenance for watch bills.

RSupply is a real-time interface into the Defense Automated Addressing System for status processing (both incoming and outgoing) and requisition submission. RSupply uses a real-time cumulative transaction ledger which provides users with explicit details of the transactions processed thus providing a tool for tracking and researching transactions.

OMMS-NG provides Navy maintenance personnel with quick, convenient access to the maintenance information they need to ensure warship readiness. Such information includes information concerning configuration items, work candidates and ordering parts for equipment.

NALCOMIS is an automated information system that provides aviation maintenance and material management with timely, accurate and complete data on which to base daily decisions. It is a



Space and Naval Warfare Systems Center Pacific Lightning Bolt awardees: AZCS Adolfo Ramirez, Cedric Peery, Glenn Peterson, Otis Glover, Mike Wickstrom and Rocky Sgro.



SSC Pacific Det Yokosuka Lightning Bolt awardees: LSCS Ronald Cruz, ENC Manuel Jamosmos, LSCM Arlene Carter, LSC Lito Fuentes and Staff Sgt. Marklyne Chery.

single, integrated, real-time system that supports workers, supervisors and managers. NALCOMIS features an automated source data entry device for simplifying and improving data collection, while also furnishing a means to satisfy the Naval Aviation Maintenance Program requirements.

The NTCSS Patriot release encompasses improved security, including enhanced protection for personally identifiable information (PII); it eliminates

non-essential data and allows encryption for Social Security numbers, essentially making the migration of data to an earlier NTCSS version much more complex.

From the two different release platforms, the SSC Atlantic team had to identify all the personnel data that needed to be migrated from the Essex, then determine whether the data was encrypted and if it existed on the Bonhomme Richard, and then identify the R-ADM database table structures of the

ships' platforms. After determining these items, using Perl, a high-level, general-purpose, dynamic programming language, personnel performed database analysis, wrote the conversion script and designed and developed the data packages needed for each ship. The team's efforts eliminated countless labor-intensive hours in manual data entry for more than 1,000 crew members and helped ensure that the ships' departure schedules were met.

SSC Pacific Detachment Yokosuka, along with Commander Naval Surface Force, U.S. Pacific Fleet (COMNAVSURPAC) and SSC Atlantic personnel, worked tenaciously running various software scripts to extract databases and complete the Integrated Shipboard Network System (ISNS) Common PC Operating System Environment Program (COMPOSE) and NTCSS users migration for both ships in a timely manner.

The SSC Atlantic team delivered the data packages to the SSC Pacific team April 6 in time for SSC Pacific employees to assist the crews of both ships in transferring data between the NTCSS databases, train the crews on the differences between the two releases and then complete the actual hull swap.

Military personnel from SSC Pacific's NTCSS team in Yokosuka and San Diego, provided training guides and devoted 66 hours of training to the crews to ensure that crew members could successfully operate NTCSS and generate required reports and financial records. Team members worked across multiple geographical locations and time zones to keep the project on track. They maintained continuous communications with shipboard and COMNAVSURPAC personnel in preparation for the data migration and training via regularly scheduled briefs.

FLEET FIRST

The combined cooperation and teamwork of PEO C4I/PMW 150, SSC Pacific NTCSS Fleet Support and the SSC Atlantic In-Service Engineering Agent (ISEA) enabled the task to be successfully planned, managed and completed from start to finish. In recognition of the team's



SSC Atlantic Lightning Bolt awardees, front row, from left: Robert Konu, Jason Womack, Oscar Gonzalez, back row, Mohamed Al-Aghbari, Clare Tucker, Jan McNaught, Patricia Rarick, Michael Artegian. Photo by Heather Rutherford/CHIPS.

outstanding performance, each member was recognized with SPAWAR's prestigious Lightning Bolt Award. The team is now busily making plans for future sea swaps using the lessons learned and successes of this first effort.

SSC Atlantic is the central design agency to PEO C4I's PMW 150 program office, providing NTCSS systems and software engineering, implementation, technical support, help desk services for software-related trouble calls, and installation and training for East Coast NTCSS hardware installations. SSC Atlantic meets the nation's demands for uninterrupted vigilance, fail-safe cybersecurity, adaptive response and engineering excellence by delivering secure, integrated and innovative solutions to naval, joint and national agencies.

PEO C4I acquires, fields and supports C4I systems that extend across Navy, joint and coalition platforms. This includes managing acquisition programs and projects that cover all C4I disciplines: applications, networks, communications, intelligence, surveillance and reconnaissance systems for afloat platforms and shore commands.

SSC Pacific provides West Coast NTCSS software installations, training, help desk services and other technical assistance. SSC Pacific delivers naval,

joint and national knowledge superiority through quality research, development, acquisition, test and evaluation and full life cycle support of effective C4ISR, information operations, enterprise information services and space capabilities. ●

NTCSS TEAM MEMBERS AND SPAWAR LIGHTNING BOLT AWARDEES
PEO C4I PMW 150
 ROCCO SGRO (CONTRACT SUPPORT)
 MICHAEL WICKSTROM (CONTRACT SUPPORT)

SSC ATLANTIC
 JANE MCNAUGHT (TEAM LEAD)
 MOHAMED AL-AGHBARI
 MICHAEL ARTEGIAN
 OSCAR GONZALEZ
 ROBERT KONU
 PATRICIA RARICK
 CLARE TUCKER
 JASON WOMACK

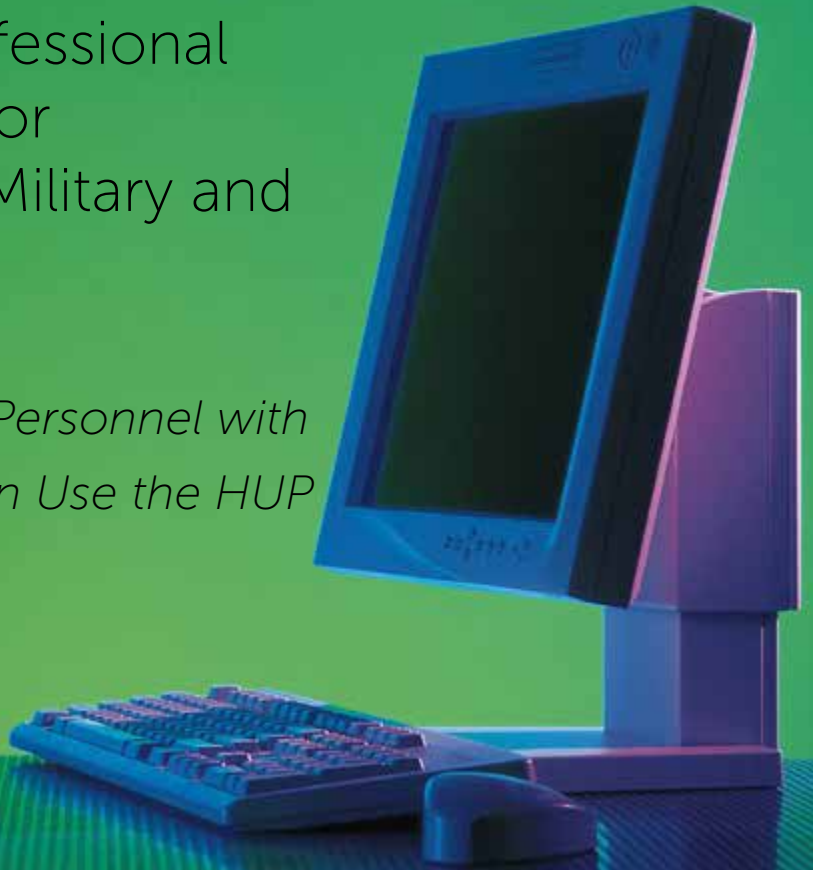
SSC PACIFIC
 GLENN PETERSON (BRANCH HEAD FOR NTCSS IMPLEMENTATION & FLEET SUPPORT)
 OTIS GLOVER
 AZCS ADOLFO RAMIREZ
 CEDRIC PEERY (CONTRACT SUPPORT)
 RICHARD SIMPSON

SSC PACIFIC DETACHMENT YOKOSUKA
 LSCM ARLENE CARTER (TEAM LEAD)
 MARINE CORPS STAFF SGT. MARKLYNE CHERY
 LSCS RONALD CRUZ
 LSC LITO FUENTES
 ENC MANUEL JAMOSMOS

Microsoft Office Professional Plus 2010 Available for Home Use to DON Military and Civilian Personnel

DON Military and Civilian Personnel with Active NMCI Accounts Can Use the HUP for Minimal Fee

By Sharon Anderson



The Department of the Navy, through its contract with Hewlett Packard (HP) for the Navy Marine Corps Intranet, is entitled to Microsoft's Home Use Program (HUP) as a volume license holder with Microsoft.

The HUP allows government civilian and uniformed personnel presently with active NMCI accounts to obtain a licensed copy of the current versions of Microsoft Office, Project or Visio desktop applications to install and use on a home computer if these products are also installed on their NMCI computer, regardless of the version on the user's work computer.

Who is Eligible

Participants must have a valid NMCI email address in order to participate, for example, John.Doe@navy.mil, Jane.Doe@usmc.mil or Jack.Doe@pacom.mil. The HUP is a software assurance benefit extended to the DON by HP under the NMCI contractor's license with Microsoft. If users have a non-NMCI computer or a legacy computer, even though they have connectivity to the NMCI network, they cannot participate in the HUP. Home use or secondary usage rights for their Microsoft products, is contained in their non-NMCI license agreement with Microsoft. Contractors are ineligible to participate.

Products Available

Specifically, the DON's NMCI HUP includes*:

- ➔ Microsoft Office Professional Plus 2010 (Contains: Word 2010, Excel 2010, PowerPoint 2010, Outlook 2010, OneNote 2010, SharePoint Workspace 2010, Publisher 2010, Access 2010 and InfoPath 2010);
- ➔ Language packs for Microsoft Office Professional Plus 2010 (available for \$9.95 each);
- ➔ Microsoft Project Professional 2010; Microsoft Visio Premium 2010; and
- ➔ Microsoft Office 2011 for Macintosh.**

* Applications should only be purchased for home use if used at your work place.

** If you use Office Professional at work and have a Mac at home, you can order and use Mac Office 2011 at home.

There is a minimal charge for the administrative costs of obtaining the software, including media and shipping. Each product costs \$9.95 for processing and handling, plus local sales tax for an electronic download service, payable via a credit card for each product ordered. Media, if requested, is an additional \$13.99.

Terms & Conditions

There is no specific expiration date to the Home Use Program license. However, if you leave the Department of the Navy, or your agency/command discontinues its software assurance coverage or you are no longer a user of the licensed software as part of your employment, your license terminates and you should discontinue use of the software. Your agency/command should notify you if any of these conditions apply.

Only one copy of each product can be obtained per NMCI email address, and you are restricted to only one home computer for hosting the obtained Microsoft product. However, although you cannot purchase more than one license, it does allow for two installations on one PC and one "portable device" (i.e., laptop).

For portable devices, simply download the software (if you don't have media) from the HUP email you received from Microsoft. The email must be accessed via your portable device. You also must use the same product key.

You can upgrade only when a newer version of the software application is offered.

If you change computers at home after purchasing a version of Office (PC or Mac), you can switch to a new office version (PC or Mac) only when Microsoft replaces the Office Professional or Mac Office version offered on HUP with a new version. Under the provisions of Software Assurance, Microsoft will offer its latest versions on HUP. Please check the ordering website for offered product changes.

The HUP is for personal home use only for eligible DON personnel. The HUP is not a substitute or alternative Microsoft purchasing program for government-owned computers. DON personnel are not allowed to share the Home Use Program products with anyone. This includes family members. Loading copies of Home Use Program software on PCs or laptops not being used to augment employees working at home is a violation of the licensing agreement and must cease immediately.

The Department of the Navy Chief

Information Officer (DON CIO) website hosts a list of Frequently Asked Questions (FAQs) about the DON's Home Use Program to help users determine their eligibility with specific information about the terms and conditions of using the HUP. Also provided in the FAQs is a step-by-step instruction for eligible NMCI users to order available Microsoft products from the DON's HUP. DON HUP FAQs are available at: www.doncio.navy.mil/ContentView.aspx?id=849.

Who Can Help?

The point of contact for the HUP is the director of commercial IT strategy for the Department of the Navy Chief Information Officer (DON CIO) and co-chair of the Department of Defense Enterprise Software Initiative program, Mr. Floyd V. Groce. He can be reached at floyd.groce@navy.mil or (703) 695-1917. ●

SHARON ANDERSON is the CHIPS senior editor. She can be reached at chips@navy.mil.

Resources

Microsoft's Home Use Program (HUP)

www.microsoft.com/licensing/software-assurance/home-use-program.aspx

NMCI Homeport

Specific ordering information for NMCI users who want to participate in the Navy's HUP is available from the NMCI Homeport

<https://www.homeport.navy.mil/news/articles/hup-license-info/>

DON CIO Information Technology Policy and Guidance

www.doncio.navy.mil

Navy Expeditionary Combat Command

The eighth annual Army Expeditionary Warrior Experiment Bold Quest began September 17, 2012 at Fort Benning, Ga. AEWE addresses live, prototype experimentation requirements with a primary focus on the Soldier and small unit, examining emerging capabilities and concepts for the current and future force across all warfighting functions. AEWE-BQ12 set a new precedent by inviting Joint Staff to take part in this year's exercise, in turn, welcoming Commander, Navy Expeditionary Combat Command to participate as an observer. CHIPS caught up with COMNECC subject matter experts in early December who responded in writing to questions about COMNECC participation in BQ12.



Q: Can you discuss your role as observer?

A: COMNECC was approached by the Joint Staff earlier this year about participating in the Bold Quest series of experimentation. Although major portions of the experiment revolve around combat identification, there are significant pieces that are service driven. BQ 12-2, marked the first-ever integration of this joint/coalition assessment process with the Army Expeditionary Warrior Experiment (AEWE). As such, the BQ coalition of U.S. and allied participants were afforded a unique, front row view of key initiatives fundamental to the *Army's Squad: Foundation of the Decisive Force* concept; they gained insights into the human dimension and leader development elements of the squad.

The heavy emphasis of small unit experimentation was appealing to NECC and had a direct relationship to similar Navy small units such as Navy EOD (explosive ordnance disposal) platoons, boat crews, intelligence detachments, construction detachments and civil Affairs teams.

We saw this exercise as an opportunity to gain insight into multiple processes. First, it was an opportunity to observe the planning and execution involved with an experiment of this size and nature. If NECC has plans to conduct a similar experiment, then this exercise was the opportunity to capture best practices for experimentation. Second, this venue introduced a multitude of small unit concepts and technologies that are not emphasized elsewhere in the Navy's training strategy. There were concepts related to improving situational awareness and decision making combined with virtual technologies designed to immerse users in a realistic scenario that replicates the deployed environment.

The goal of the virtual immersion is to provide users with repeatable scenarios that will inform future decision-making for individuals when confronted with similar scenarios in the joint operating environment. Most virtual trainers used by the Navy are designed for ships and aircraft. For NECC, our virtual training requirements are more aligned with the Army and Marine Corps with an added dose of maritime flavor. COMNECC's attendance

at Fort Benning was designed to gain insight into other service's training concepts and technologies and to examine how these may work to prepare Sailors for similar tasks in a maritime environment.

Q: Among the training modules presented at Bold Quest, which do you think will be most useful to the Navy?

A: The most promising observation was a concept called ASAT — Advance Situational Awareness Trainer. ASAT is a combat situational awareness training approach developed by Orbis Operations, LLC and modeled after the Marine Corps's Combat Hunter program. The goal of ASAT is to provide students with the physical and mental ability to recognize threats in a combat environment with a focus on urban terrain.

ASAT employs a combination of pattern recognition, experiential learning, law enforcement techniques, military tactics, and other approaches to improve sense making and tactical decision-making. The instructor delivery techniques were a major factor in knowledge transfer during the classroom iteration. Although instruction included complex topics based on philosophy (logic), sociology and psychology, the delivery method was tailored to the training audience (Army's Squad) and appeared to be effective. This capability could appeal to expeditionary forces if the baseline was re-centered on the maritime environment.

Also, this capability aligns with the Navy's effort in *Maritime Infrastructure Protection and Confronting Irregular Challenges* by emphasizing the human dimension of training. A version of ASAT tailored to NECC's diverse maritime and ground forces (Coastal Riverine Force/CRF, Explosive Ordnance Disposal/EOD, Naval Construction Force/NCF, Navy Expeditionary Intelligence Command/NEIC, Maritime Civil Affairs and Security Training Command/MCASTC, and Navy Expeditionary Logistics Support Group/NAVELSG), integrated with other live and virtual training efforts would significantly enhance the combat readiness of our forces.

Q: Do you know when the Navy will have the opportunity to use the virtual training demonstrated at the AEWE Bold Quest event?

A: The Navy and COMNECC continue to pursue simulation and synthetic training in order to deliver better and more effective integrated training. During the exercise, some of the virtual training was used as a demonstration, while other efforts are funded service programs of record. The first step in any procurement process is to make sure that the problem is identified and clearly articulated.

COMNECC has drafted a synthetic training strategy that outlines efforts to integrate live, virtual and constructive training initiatives for expeditionary forces. This draft strategy has highlighted the need to further develop a simulation master plan that drives future requirement and resourcing decisions for emerging training technologies and concepts like the ones demonstrated at Fort Benning. Once these processes are in place, COMNECC can better decide on our use of current and future training technologies and the mechanisms required to sustain the chain of live, virtual and constructive training efforts.

Q: How does the Navy conduct training now and can you explain how virtual training may replace or enhance the training that the Navy currently uses?

A: COMNECC Commander, Navy Expeditionary Combat Command is aligned with other Type Commands (TYCOMs) and delivers training based on the Fleet Training Continuum and the Fleet Response Plan. Based on the Fleet Response Training Plan, live, virtual and constructive training is conducted throughout each phase as separate or integrated functions. The end state of the FRTP is readied and prepared forces as emphasized in the recently issued U.S. Fleet Forces Command Vision Guidance (October, 2012).

COMNECC's current approach to training demands the integration of a mix of requirements to include: expeditionary core skills training; required operational capability training; general military training; theater specific training, to include language and culture training; and mission essential training. Additionally, expeditionary forces are more likely to confront irregular mission sets; therefore, [they] are prepared beyond the basic Navy crew standards for deployment.

In order to meet these competing requirements, training is conducted at the individual and unit level throughout the FRTP. Individual training is normally evaluated at the lower command level, while unit or collective training is evaluated at higher levels to include TYCOM (type commander) certification during the integrated phase of the FRTP.

Training in a live environment offers the highest degree of human interaction and experience. This factor is important when training scenarios are designed around counterinsurgency, security force assistance, maritime security and other irregular mission sets that require more use of the human dimension of warfighting and decision making at lower levels. NECC's current

FRTP does include several simulated and constructive training technologies, but we would like to see an increase in training systems related to support of irregular mission sets and expeditionary force requirements.

Although simulated training cannot replace live training, it does provide many advantages for both individual and collective training. First, it offers the ability to conduct multiple iterations of tactical scenarios for individual and small unit training. This provides the training audience the ability to learn through 'new' experiences and develops a database of practical knowledge that can be recalled in time of conflict.

Second, simulated and immersive training offers a cost-effective means to introduce environmental characteristics into the training environment such as civilians on the battlefield, multi-dimensional terrain displays, sights, sounds and smells that are more expensive to replicate in a live environment. There is still much work to be done in these areas, but we foresee simulated and immersive training as the standard for major portions of military training in the next 20 years. The key is finding the right mix and ensuring that they are properly synchronized within the entire training spectrum.

Q: I understand that 2012 is the first year that NECC was invited to attend Bold Quest. Are there plans for the Navy to be more hands-on at the next Bold Quest?

A: Fleet Forces Command has been a participant in past BQ events focused on combat ID and is currently involved with the 2013 planning. NECC has made plans to be an active participant in the BQ-13 events. Next year's participation will be small in scope and will highlight COMNECC's capabilities to provide operational support through digitally aided close air support (DACAS) technology. This event was timely and was easily integrated into the planning cycle.

Based on lessons learned from observations at Fort Benning, COMNECC will need to properly position resources to adequately pursue similar virtual training efforts demonstrated by the Army. This includes all of the administrative and logistical considerations for experimentation such as: experimental force, analysis team, ranges and training areas, and contract administration. Our goal is continued participation in the Bold Quest series and to ramp up our participation level each year. More emphasis on simulation at the tactical and operational levels is needed for expeditionary forces and NECC is working to align simulation resources comparable to other TYCOMs. Bold Quest offers an excellent venue for continued experimentation in this effort. ●

BOLD QUEST AEWE
WWW.BENNING.ARMY.MIL/MCOE/CDID/AEWE/

NAVY EXPEDITIONARY COMBAT COMMAND
WWW.NECC.NAVY.MIL

USS Enterprise (CVN 65) – “We Are Legend”

By Sharon Anderson

Not every ship can make such a boast but there is no doubt the USS Enterprise (CVN 65) has earned the right in its 51 years of service. Enterprise, the world's first nuclear-powered aircraft carrier, served in every major conflict since the Cuban Missile Crisis in 1962: six deployments in support of the Vietnam War and through the Cold War and Gulf wars.

Enterprise commemorates a name that has been a continuing symbol of the great struggle to preserve American liberty, justice and freedom since the first days of the American Revolutionary War. It is the eighth ship in the fleet to carry the illustrious name that is defined by boldness, power and innovation.

The first Enterprise originally belonged to the British and cruised Lake Champlain to supply posts in Canada. After the capture of Fort Ticonderoga by the Americans May 10, 1775, it became apparent to Benedict Arnold that he would not have control of Lake Champlain until its capture. On May 18, he surprised and stormed the British garrison at St. John's on the Richelieu in Canada and took possession of the 70-ton sloop. Arnold named it Enterprise.

The seventh Enterprise (CV 6) was the first of the Enterprise ships to receive the nickname of “Big E” — other nicknames included the “Lucky E” — the “Grey Ghost” — and the “Gallop-ing Ghost.” CV-6 became the sixth aircraft carrier to join the U.S. Navy fleet upon its commissioning Oct. 3, 1936. After its heroic World War II service, the first Big E was decommissioned Feb. 17, 1947 — as the most decorated ship in U.S. naval history.

ENTERPRISE VIII (CVN 65)

In 1954, Congress authorized the construction of the world's first nuclear-powered aircraft carrier, USS Enterprise

(CVN 65). The giant ship would be powered by eight nuclear reactors, two for each of its four propeller shafts. This was an enormous undertaking because never before had two nuclear reactors ever been harnessed together. When the engineers first started planning the ship's propulsion system, they were uncertain how it would work, or even if it would work according to their theories. After years of planning and exhaustive work by thousands of engineers, designers, welders, and more, she was commissioned Nov. 25, 1961.

In October 1962, Enterprise and other ships in the U.S. 2nd Fleet were dispatched to set up a naval blockade around Cuba when it was discovered that the Soviet Union had built nuclear missile sites on the island. The aim of this “quarantine,” as President John F. Kennedy called it, was to prevent the Soviets from bringing in more military supplies. The President demanded the immediate removal of the missiles already there and destruction of the missile bases. The first Soviet ship was stopped Oct. 25, and Oct. 28, Soviet leader Nikita Khrushchev agreed to dismantle the nuclear sites, concluding the Cuban Missile Crisis — and averting nuclear war.

On Sept. 11, 2001, Enterprise was headed to Naval Station Norfolk after a long deployment when its commanding officer ordered the ship to turn around and head toward Southwest Asia, where it later launched some of the first attacks in direct support of Operation Enduring Freedom. The ship's captain at the time is now the vice chairman of the Joint Chiefs of Staff, Adm. James A. Winnefeld.

Another defining moment in the ship's history occurred in 1969 on the morning of Jan. 14 when an explosion erupted due to an overheated rocket attached to a parked F-4 Phantom. The

initial explosion caused other armed aircraft to ignite spreading fires and additional explosions across the flight deck. The fires were brought quickly under control, in comparison to previous carrier flight deck fires, and were finally extinguished four hours later.

Forty-three years later, while underway in the Atlantic Ocean, Jan. 14, 2012, Sailors and Marines assigned to USS Enterprise paused to remember the catastrophic fire probably for the last time. Former crew members recalled that day both as Enterprise's worst tragedy and its finest hour as the crew fought bravely to save the ship. Twenty-seven Sailors perished and 314 were injured, and despite the valiant efforts of the crew, Enterprise was heavily damaged during the fire. Repairs were completed in April 1969 in Pearl Harbor, Hawaii, and then Enterprise proceeded as scheduled on deployment to Vietnam and the Tonkin Gulf. The fire not only changed damage control and firefighting for the Enterprise, it improved techniques and training across the fleet. Many lessons learned from that tragedy are still used by the Navy today.

Enterprise has also had its share of Hollywood glamour. The hugely popular 1986 movie “Top Gun” was filmed aboard the Enterprise featuring daring young naval aviators that captured the imagination of young adults across America who wanted to emulate the skill and bravado of the F-14 Tomcat fighter pilots in the action-drama. When production concluded the movie producers donated a pair of black fuzzy dice which are still on display in Primary Flight Control or “Pri-Fly” 26 years later.

During its memorable history, Enterprise chalked up some amazing statistics: 25 deployments, 10 major operations and 400,000 arrested landings. On Enterprise's final deployment, which lasted eight months, it transited through



ATLANTIC OCEAN (Nov. 3, 2012) The aircraft carrier USS Enterprise (CVN 65) underway in the Atlantic Ocean after completing a 7-and-a-half month deployment to support operations in the Mediterranean and Arabian seas. Enterprise is completing its final deployment to the U.S. 5th and 6th Fleet areas of responsibility in support of maritime security operations and theater security cooperation efforts. U.S. Navy photo by Lt. Ryan de Vera.

the Strait of Hormuz 10 times to protect freedom of the seas.

But ultimately, it's not the number of deployments, Hollywood movie or impressive statistics that make up a ship's legacy — it's the crew — its heart and soul. The Navy estimates that 100,000 Sailors have served on the Enterprise and many former crew members joined the current crew during inactivation week — a weeklong celebration of Enterprise history which culminated in an inactivation ceremony Dec. 1 on board Naval Station Norfolk. During inactivation week veterans and friends of the "Big E" were given the opportunity to tour the ship. About 8,000 visitors toured Enterprise that week, while the inactivation ceremony drew about 12,000 attendees.

LEGENDARY CREW AND SHIP

CHIPS staff joined about 1,000 other enthusiastic well-wishers Nov. 29 for a tour of the Enterprise. Among those we met was a man who said he had been fascinated with the Enterprise since he was a small boy. He and his young son tackled the 15-hour drive from Kenosha, Wisconsin, to Norfolk for the tour and were lucky enough to score tickets for the inactivation ceremony. We met retired, teary-eyed shipyard workers, pilots, crew members, schoolchildren — and the curious — all fascinated by

the historic ship and exceedingly moved to be aboard Enterprise for the final farewell.

A carrier has approximately 18 levels, including eight above the ship's enormous hangar bay and 10 decks below. The "island" or superstructure above the flight deck contains the bridge, where the commanding officer monitors flights and oversees operations, and the flag bridge, where the admiral and staff can watch operations and conduct task force planning. Our group eagerly clambered up and down the ship's ladders leading to most of the 18 levels on Enterprise.

Topside, the 4.5 acres of flight deck looked particularly desolate without Enterprise's usual complement of 60 to 70 aircraft, including F/A-18E and F Super Hornets, E-2C Hawkeyes, EA-6B Prowlers, SH-60F Seahawk helicopters, C-2 Greyhounds (carrier onboard delivery aircraft) and Marine Corps F/A-18C Hornets. Enterprise's air wing, Carrier Air Wing One, with about 1,300 personnel, had flown off the Enterprise days before its return to Norfolk Nov. 4.

Our tour guide, Aviation Boatswain's Mate (Aircraft Handling) 3rd Class Benji Long, was joined by Airmen Sean Condon and Eric Murphy to escort our group of 15. We began on the bridge where we met Quartermaster 2nd Class Thomas Sanborn, who along with sev-

eral other Sailors, was standing watch. Sanborn explained that he was manning the ship's signal flags on the lookout for a man overboard, computing tidal data, conducting weather observation, and generally vigilant for any type of emergency. He showed us the Enterprise's position on a nautical chart and pointed to several areas of interest in the waters off Norfolk Naval Station. He explained that while newer ships in the fleet use an electronic navigation system, Enterprise relied on paper navigation charts and compass to plot course. "It didn't slow us down though," Sanborn said. "We were still the fastest ship in the Navy."

While other nuclear-powered carriers have four nuclear reactors, Enterprise's eight allowed it to sail more than 35 miles an hour in the open seas.

Next stop, Pri-Fly, a level up from the bridge, where we saw the famous fuzzy



Aviation Boatswain's Mate (Aircraft Handling) 3rd Class Benji Long and Airmen Sean Condon and Eric Murphy aboard USS Enterprise Nov. 29.

dice and were briefed by ABH2 Jenna Weddel. The small room towers seven stories above Enterprise's flight deck. The panoramic view of deck operations below provides Sailors with a bird's eye view of flight ops. Monitoring an average of 90 aircraft take-offs and arrested landings on a daily basis while the ship is deployed, often with less than a minute (sometimes seconds) between launch and recovery operations, the Pri-Fly crew must continuously survey all flight and deck operations to help keep personnel safe in one of the world's most dangerous working environments. The "Air Boss" and "Mini Boss" are in charge of all Pri-Fly operations, which cover all aircraft activity within a five-mile radius of the ship.

Using a number of advanced radar systems and constant communication with the pilots, aircraft from up to 50 miles away from the ship are monitored by personnel located in the CATCC, or carrier air traffic control center. Even with advanced radar systems, landing 30-ton jets can still be difficult. Problems that may occur include: low fuel, engine or landing gear problems, and any number of emergency landing situations, Long said.

More ladders to navigate, and on to flight deck control, which is the central location for all operations that involve any flight deck maneuver. From foreign object debris walk downs, refueling jets, to launching and recovering aircraft, the crew in flight deck control coordinates operations by means of a "ouija board" — a scaled down version of the flight deck sized to 1/16 inch to one foot, mounted on a table and populated with miniature aircraft.

The atmosphere in flight deck control was definitely laid back, with no aircraft on board to worry about; aircraft handlers had time to describe flight operations for those touring the ship. The camaraderie of the air crew was obvious and no wonder they work 15 to 16-hour days while deployed relying on each other to ensure the safety of personnel and multimillion-dollar aircraft. Several off-duty Sailors had brought their active toddlers on board for a visit. At one point, an inquisitive baby grabbed a plane from the ouija board while his mom remarked that she moved those planes around all day. Long said, "We are like family here; even during our time off we like to hang out with each other."

Sailors in flight deck control must keep aircraft handlers informed of flight deck movements. The handler displays the aircraft's movement and location on the ouija board, and it is the handler's job to confirm



NORFOLK (Nov. 30, 2012) A U.S. Navy Sailor, assigned to the aircraft carrier USS Enterprise (CVN 65), gives a presentation on the operations of the ship's flight deck control center to a tour group during the ship's inactivation week tours Nov. 30. He is seated in front of the "ouija board" — a scaled down version of the flight deck. Enterprise was commissioned in 1961 and is scheduled to celebrate her inactivation, Dec. 1, after 51 years of service. U.S. Navy Photo by Mass Communication Specialist 2nd Class Alex R. Forster.

all aircraft are in the appropriate location during flight operations. The handler's main task is to make sure the flight deck has enough room for jets to maneuver, not only for launch and recovery missions, but refueling as well.

"We can get a call from [air crew] on deck, someone could just want to open the wings on a plane but he has to call down here [flight deck control] for permission first," Long said.

The hangar bay covers 3.5 acres, and four elevators move aircraft between the hangar bay and flight deck. There are four steam catapults to launch aircraft.

Long's berthing compartment was nearby so we headed there next, where he graciously showed us his rack (bunk), storage locker and a communal shower. Spaces were cramped but our group gamely took turns inspecting everything that Long and his cohorts were willing to show us. One Sailor passing in the opposite direction marveled, "He's showing them the bathrooms?" Clearly, our tour guides were proud to present every inch of the Enterprise for inspection.

From there we saw the general mess for the crew, Chiefs' Mess and Wardroom, each stocked with an appetizing variety of fresh salads and fruit, as well as fried chicken, mashed potatoes and gravy. We didn't tour these, but Enterprise also has a general store, two gyms, two barber shops, laundromat, print shop, chapel, library, television station and studio, coffee shop, and a daily newspaper distributed when the ship

was underway.

Next we moved to damage control, sick bay and the ship's forecandle (pronounced fo'ksul). The forecandle is the forward part of the main deck and is home to the ship's ground tackle, all the equipment used in anchoring. Ground tackle is one of the most vital parts of a ship's equipment since its safety can depend upon the proper use of this gear. We examined the anchor windlass, equipped with capstan head, massive anchor chains and the chain locker. Interestingly, the forecandle, because of its large open space, is also used to hold ceremonies.

In sick bay, corpsmen provided a snapshot of the Enterprise's medical capabilities and reported that most crew injuries were broken bones and bumped heads resulting from rushing up and down ladders or failing to duck under low bulkheads. Still, the ship's doctor and corpsmen can handle virtually any medical emergency while more complicated cases may require airlift to a hospital when the ship is deployed.

In damage control, personnel use equipment and techniques to prevent or minimize damage caused by battle, fire, collision, grounding and explosion. Personnel are also trained in defensive measures used to mitigate the effects of weapons of mass destruction, such as chemical, biological and radiological warfare.

INACTIVATION PHASE

The Enterprise will remain at Naval Station Norfolk for approximately six months to

off-load equipment and to make the ship ready for tow to Huntington Ingalls Industries-Newport News Shipyard for inactivation. The inactivation phase will last about four years in which hydraulic systems will be drained and expendable materials, tools, spare parts and furnishings will be removed.

Additionally, tanks containing oil and other fluids will be drained and cleaned, any hazardous material will be removed, and the ship's electrical and lighting systems will be de-energized.

Concurrent with inactivation, the ship will be defueled using the same proven techniques that have been used successfully to refuel and defuel more than 350 naval nuclear-powered warships. The ship will also be prepared to be towed to Puget Sound Naval Shipyard and Intermediate Maintenance Facility in 2017 for dismantling and recycling.

Most of the crew will be reassigned to other commands shortly after inactivation. A smaller group will stay with the ship serving as watch standers until the reactors are completely defueled. Some will remain during the tow to Puget Sound Naval Shipyard.

During the tour, we chatted with the Enterprise's pleasant and highly professional crew — in many ways — the best part of the tour. Most were anxious to hear of their next assignment. Long said he hoped to be headed for a career change and acceptance into "A" School for Hospital Corpsman. A few were looking forward to shore duty while most we talked with were going to other carriers and back to sea.

Crew members were cheerfully anticipating the holidays in port. Airman Eric Murphy said he has been enjoying his wife's cooking since the ship's return; it was what he missed most while deployed. Airman Sean Condon said he was just glad to hang out with his friends — most of whom are Enterprise shipmates.

In a video played at the inactivation ceremony, Secretary of the Navy Ray Mabus announced that the name Enterprise will live on as he officially passed the name to CVN 80, the third Ford class carrier and the ninth ship in the U.S. Navy to bear the name. Nostalgic Enterprise veterans old and new were delighted to hear the news. ●

SHARON ANDERSON is the senior editor of CHIPS. She can be reached at chips@navy.mil.

FOR MORE INFORMATION
www.enterprise.navy.mil



NORFOLK (Dec. 1, 2012) Veterans, family, and friends participate in the inactivation ceremony for the aircraft carrier USS Enterprise (CVN 65). Enterprise was commissioned Nov. 25, 1961 as the first nuclear-powered aircraft carrier. The inactivation ceremony marks the end of her 51 years of service. U.S. Navy photo by Mass Communication Specialist Seaman Joshua E. Walters.

USS ENTERPRISE (CVN 65) FACTS AND STATS

KEEL LAID: Feb. 4, 1958
LAUNCHED: Sept. 24, 1960
COMMISSIONED: Nov. 25, 1961
MAIDEN VOYAGE: Jan. 12, 1962
INACTIVATION: Dec. 1, 2012

SHIP'S COMPANY: 3,100
AIR WING: 1,300
EMBARKED STAFFS: 200
AIR WING: CVW-1 (Carrier Air Wing ONE)
Staffs Include: Carrier Strike Group Twelve and Destroyer Squadron Two

ARMAMENT: Multiple NATO Sea Sparrow, Phalanx CIWS, and Rolling Airframe Missile (RAM) mounts

ENTERPRISE'S FINAL DEPLOYMENT

- ➔ 239 DAYS DEPLOYED (270 OF 308 DAYS IN 2012 UNDERWAY)
- ➔ 80,968 MILES STEAMED
- ➔ 39 RESTRICTED WATER TRANSITS
- ➔ 10 STRAIT OF HORMUZ TRANSITS
- ➔ 2 BAB EL-MANDEB TRANSITS
- ➔ 2 SUEZ CANAL TRANSITS
- ➔ 1 STRAIT OF MESSINA TRANSIT
- ➔ 38 REPLENISHMENTS AT SEA
- ➔ 7 PORT VISITS
- ➔ 15 PRE-ACTION AIM CALIBRATION (PAC) FIRE ON THE CLOSE-IN WEAPON SYSTEM (CIWS) EXPENDING 6,750 ROUNDS.

The Enterprise Medical Department had **25,150 patient encounters**, filled more than **10,000 prescriptions**, performed **1,189 radiology exams**, **5,494 laboratory tests**, conducted **77 emergent and same-day surgical procedures** and managed more than **59 medical evacuations** from **seven different ships at sea**.

The supply team handled more than **700,000 pounds of mail**, prepared more than **3 million meals**, baked more than **300,000 cookies**, processed more than **500,000 pounds of laundry**, gave more than **25,000 haircuts** and **expedited 6,000 high-priority parts valued at \$250 million to keep Enterprise's jets flying**.

Norfolk Naval Station's Solar Electric System Project

Navy builds largest solar array on East Coast

By Heather Rutherford

Personnel attached to Norfolk Naval Station and residents living near the base are accustomed to seeing cutting-edge technology in the form of ships and aircraft, and other high-tech platforms, on this, the world's largest naval base, nearly every day. In keeping with the Navy's pioneering spirit, in December 2012, the base unveiled a new 10-acre solar array system to help pay its utility bill.

The solar farm contains 8,624 solar panels installed in a rack system, each bolted onto steel stilts installed in a soggy field called Monkey Bottom just outside the naval station's gate and visible from the Chesapeake Bay and Hampton Roads Bridge-Tunnel.

Eighteen-thousand linear feet of above-ground conduit is installed in the array field with 15,000 linear feet of PVC conduit installed below ground; 230,000 linear feet of wire is pulled in the array field to support the operation of the solar panels. The system produces up to 2.1 megawatts of electricity, according to Naval Facilities Engineering Command Mid-Atlantic, who is responsible for the project.

According to Tom Kreidel, spokesman for NAVFAC Mid-Atlantic, the solar array is the largest solar project at any Navy base on the East Coast.

The project is important because Secretary of the Navy Ray Mabus set an energy policy that will improve the Navy's

energy security, increase its energy independence and help lead the nation toward a clean energy economy. The Department of the Navy established five ambitious energy goals (http://www.navy.mil/features/Navy_EnergySecurity.pdf) intended to move the Navy and Marine Corps away from a reliance on petroleum and dramatically increase the use of alternative energy.

One of the goals is to increase alternative energy ashore. By 2020, the department will produce at least 50 percent of shore-based energy requirements from alternative sources and 50 percent of DON installations will be net-zero — meaning they will produce enough energy to be energy-independent.

The solar project will help the Norfolk Naval Station meet the secretary's goals for greater energy efficiency.

The project was awarded in June 2009, and the solar array is expected to be fully operational by the end of 2012.

Solar panels use the sun's rays to produce electricity. Sunlight, in the form of photons, shines down on the panels. The panels convert the photons into electrons as direct current. Then the photons flow to a DC/AC

Closer look at Naval Facilities Engineering Command Mid-Atlantic's solar farm project onboard Naval Station Norfolk.



power converter, also known as an inverter, where they are converted into alternating current power.

"As far as how it works with our energy program, the power from the panels goes back into the grid that feeds the base. So it doesn't go to any one particular place on base. The energy we produce with the solar panels is energy that we don't have to buy from the local electric company," said Michelle Perry, NAVFAC's project manager for the solar panel system.

The cost of the project was \$21 million. ●

FOR MORE INFORMATION

NAVFAC Mid-Atlantic

https://portal.navy.mil/portal/page/portal/navfac/navfac_ww_pp/navfac_NAVFACMIDLANT_pp

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

Naval Facilities Engineering Command Mid-Atlantic recently completed a photovoltaic project at Naval Station Norfolk. The project features more than 8,000 solar panels that will generate more than 2 megawatts of electricity at the world's largest naval base. U.S. Navy photos by John Land/NAVFAC.



ONR-Funded Microgrid Powers "World Green City"

Concept ideal for small rural village and island communities

By Eric Beidel, Office of Naval Research

THE OFFICE OF NAVAL RESEARCH (ONR), A LEADER IN THE EXPLORATION OF RENEWABLE

POWER, played a major role in the development of a new "World Green City" at its headquarters in Arlington, Va., on Dec. 12, as a prototype community powered by alternative energy sources.

Keeping in line with Chief of Naval Operations Adm. Jonathan Greenert's recently announced 2013-2017 Navigation Plan — which calls for improving operational energy efficiency by investing in new technologies — the World Green City boasts the latest in renewable power, including a direct-current (DC) microgrid funded by ONR's Sea Warfare and Weapons Department (<http://www.onr.navy.mil/Science-Technology/Departments/Code-33.aspx>).

Dr. Richard T. Carlin, head of the department, spoke to international leaders and scientists during the opening ceremony of the World Green City and Eco-Product Exhibition 2012.

"The World Green City provides an opportunity to evaluate and understand the implementation of renewable energy technologies in a real-world microgrid," Carlin said. "Such microgrids make possible sustainable, decentralized power systems that are applicable to many communities, especially remote communities, as well as forward-deployed naval operational bases. Our partnership with Chiang Mai Rajabhat University will benefit communities in Thailand and ultimately communities across the Asia Pacific region."

The idea for the microgrid began two years ago when Dr. Wattanapong Rakwichian, executive director of the Asian Development Institute for Community Economy and Technology (adiCET) at Chiang Mai Rajabhat University, discussed his vision for a "green" campus with ONR officials at a workshop on alternative and renewable energy funded by ONR.

Located on the new Saluang-Keelek campus of Chiang Mai Rajabhat University in Northern Thailand, the World Green City now includes about 20 buildings over 200

acres operating on renewable power from solar cells.

"With support from ONR, we have created a model community that applies smart technologies and renewable energies into the green living style," said Dr. "Watt," as he is affectionately called. "As a result, we hope that our World Green City will serve as a model for developing the rest of the smart communities in Thailand and other parts of Asia."

The DC system takes power from an array of solar cells and delivers it to houses, businesses, classrooms and offices on the campus without having to convert to alternating current (AC). This saves money and eliminates the need for DC-to-AC power conversion equipment, and the associated losses of the conversion process.

The research also features innovations in the development of smart microgrids, which manage power production, storage and distribution. Research in this area could lead to smaller, portable DC power plants that can be set up quickly for use during emergencies, without the need for fossil fuels. Such systems could find use in various naval applications.

"It's ideal for a small rural village and also island communities," said Capt. Paul Marshall, interim associate director for Power and Energy for ONR Global (<http://www.onr.navy.mil/Science-technology/onr-global.aspx>) and project officer from the ONR Reserve component. "If you have a community living on an island disconnected from the main power grid, they need to be able to produce their own power, which can be managed by having a microgrid on the island. In a way, it's analogous to a ship at sea. Some of these technologies being researched could someday be used in naval applications."

Ken Foster, consul general of the U.S. Department of State's Consulate General in Chiang Mai (http://chiangmai.usconsulate.gov/about_the_consulate.html), praised the collaboration between ONR and the local university during his remarks at the opening ceremony for the World Green City.

"As the U.S. Department of State celebrates 180 years of friendship between the United States and Thailand, we are pleased to witness another partnership success story between the U.S. Office of Naval Research and Chiang Mai Rajabhat University," Foster said. "We congratulate these partners for establishing real-world renewable energy research in northern Thailand, and connecting environmental innovators across sectors and across the globe."

The forum began with an opening speech from Thailand's Vice Minister of the Ministry of Energy, and a ribbon cutting for the World Green City. In addition to the opening ceremony, ONR representatives are attending, presenting and moderating at the third annual Workshop on Alternative and Renewable Energy for Sustainability and the World Alternative Energy Forum while in Thailand. ●

OFFICE OF NAVAL RESEARCH

ONR provides technological advantage to the Navy and Marine Corps through investments in science and technology (S&T) research. ONR's investments have enabled many firsts, including the launch of the first U.S. intelligence satellite; the development of SEALAB I/II; the validation of the Global Positioning System concept and launch of the first GPS satellite; the first global atmospheric prediction model; Overseas Contingency Operation support through various quick-response programs; the Electromagnetic Railgun; Free Electron Laser; energy S&T; and underwater autonomous systems.

● *Ranked No. 1 Best Place to Work in the Navy, by the Partnership For Public Service*

E-mail: onrcsc@onr.navy.mil

Web: www.onr.navy.mil

Facebook: www.facebook.com/officeofnavalresearch



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 NAFL employees; Intelligence Community (IC) covered organizations to include all DoD Intel System member organizations and employees, but not the CIA, nor other IC employees, unless they are assigned to and working with DoD organizations; DoD contractors authorized in accordance with the FAR; and authorized Foreign Military Sales.

For more information on the ESI or to obtain product information, visit the ESI website at www.esi.mil/.

Software Categories for ESI

IT Asset Management

Belarc

BELMANAGE ASSET MANAGEMENT: Provides software, maintenance and services.

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

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

ORDERING EXPIRES: 30 Dec 16

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

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

BMC

REMEDY ASSET MANAGEMENT: Provides software, maintenance and services.

CONTRACTOR: BMC Software Inc. (W91QUZ-07-A-0006)

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

ORDERING EXPIRES: 23 Mar 15

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

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

DLT

BDNA ASSET MANAGEMENT: Provides asset management software and services.

CONTRACTOR: DLT Solutions Inc. (W91QUZ-07-A-0002)

AUTHORIZED USERS: This BPA has been designated as a GSA SmartBUY and is open for ordering by all Department of Defense (DoD) components, authorized contractors and all federal agencies.

ORDERING EXPIRES: 01 Apr 13

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

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

Flexera

FLEXERA PRODUCTS: Flexera is a provider of strategic solutions for application usage management. Flexera software helps application producers and their customers strategi-

cally manage application usage to achieve continuous compliance, optimized usage and maximized value.

CONTRACTORS:

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

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

ORDERING EXPIRES: 21 Oct 15

WEB LINKS: **Flexera DLT Solutions**

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

Flexera Immix Group

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

Database Management Tools

Microsoft Products

MICROSOFT DATABASE PRODUCTS: See information under Office Systems on page 76.

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

ORDERING EXPIRES:

DLT: 31 Mar 17

immixTechnology: 02 Mar 16

Mythics: 16 Mar 13

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

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

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

SPECIAL NOTE TO NAVY USERS: See the information provided on page 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 Apr 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 Mar 13 (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 74.

RWD Technologies

RWD TECHNOLOGIES: Provides a broad range of integrated software products to improve the productivity and effectiveness of end users in complex operating environments. RWD's Info Pak products allow you to easily create, distribute and maintain professional training documents and online help for any computer application. RWD Info Pak products include Publisher, Administrator, Simulator and OmniHelp. Training and other services are also available.

CONTRACTOR: RWD Technologies (N00104-06-A-ZF37); (404) 845-3624

ORDERING EXPIRES: 14 Apr 15

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

SAP

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

CONTRACTORS:

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

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

Carahsoft Technology Corp. (N00104-08-A-ZF43); Small Business; (703) 871-8583

Oakland Consulting Group (N00104-08-A-ZF44); Small Business; (301) 577-4111

ORDERING EXPIRES: 14 Sep 13

WEB LINKS:

SAP Public Services, Inc.

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

Advantaged Solutions, Inc.

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

Carahsoft Technology Corp.

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

Oakland Consulting Group

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

Information Assurance Tools

Websense (WFT)

WEBSense: Provides software and maintenance for Web filtering products.

CONTRACTOR:

Patriot Technologies (W91QUZ-06-A-0005)

AUTHORIZED USERS: This BPA is open for ordering by all DoD components and authorized users.

ORDERING EXPIRES: 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

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

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

Softmart

www.esi.mil/contentview.aspx?id=117&type=2

SHI

www.esi.mil/contentview.aspx?id=123&type=2

Minitab

MINITAB: A DoD-wide blanket purchase agreement was established non-competitively with Minitab, Inc. to provide software licenses, media, training, technical services, and maintenance for products including Minitab Statistical Software, Quality Companion, and Quality

Trainer. It is the responsibility of the ordering officer to ensure compliance with all fiscal laws prior to issuing an order under a BPA, and to ensure that the vendor selected represents the best value for the requirement being ordered (see FAR 8.404).

CONTRACTOR:

Minitab, Inc. (N00104-08-AZF30); (800) 448-3555

AUTHORIZED USERS: This BPA is open for ordering by all Department of Defense (DoD) authorized components, U.S. Coast Guard, NATO, Intelligence Community and authorized DoD contractors.

ORDERING EXPIRES: 07 May 13

WEB LINK:

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

PowerSteering

POWERSTEERING: Provides software licenses (subscription and perpetual), media, training, technical services, maintenance, hosting and support for PowerSteering products: software as a service solutions to apply the proven discipline of project and portfolio management in IT, Lean Six Sigma, Project Management Office or any other project-intensive area and to improve strategy alignment, resource management, executive visibility and team productivity. It is the responsibility of the ordering officer to ensure compliance with all fiscal laws prior to issuing an order under a BPA, and to ensure that the vendor selected represents the best value for the requirement being ordered (see FAR 8.404).

CONTRACTOR:

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

AUTHORIZED USERS: All DoD components, U.S. Coast Guard, NATO, Intelligence Community, and authorized DoD contractors.

ORDERING EXPIRES: 14 Aug 13

WEB LINK:

www.esi.mil/contentview.aspx?id=145&type=2

Office Systems

Adobe Digital Media Product

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

It is the responsibility of the ordering officer to ensure compliance with all fiscal laws prior to issuing an order under a BPA, and to ensure that the vendor selected represents the best value for the requirement being ordered (see FAR 8.404).

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

CONTRACTORS:

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

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

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

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

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

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

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

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

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

ORDERING EXPIRES: 30 Jun 16

WEB LINKS:

Carahsoft Technology Inc.

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

CDW-G

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

Dell

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

Emergent, LLC

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

GovConnection

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

Insight

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

SHI International Corp.

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

Softchoice

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

Softmart

www.esi.mil/contentview.aspx?id=309&type=2

Adobe Server Products

ADOBE SERVER PRODUCTS: Provides software licenses (new and upgrade), maintenance, training and support for numerous Adobe server products, including LiveCycle Forms;

LiveCycle Reader Extensions; Acrobat Connect; Flex; ColdFusion Enterprise; Flash Media Server and other Adobe server products.

CONTRACTOR:

Carahsoft Technology Corp. (N00104-09-A-ZF31); (703) 871-8556

ORDERING EXPIRES: 14 Jan 14

WEB LINK:

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

Autodesk

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

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

ORDERING EXPIRES: 20 Nov 14

Web Link: www.esi.mil/contentview.aspx?id=266&type=2

Microsoft Products

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

CONTRACTORS:

CDW Government, LLC (N00104-02-A-ZE85); (312) 705-1889 or (703) 621-8211

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

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

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

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

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

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

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

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

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

ORDERING EXPIRES: 31 Mar 13

WEB LINKS:

CDW Government, LLC

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

Dell

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

EnPointe Gov., Inc.

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

GovConnection

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

GTSI

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

Hewlett-Packard

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

Insight Public Sector, Inc.

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

SHI

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

Softchoice

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

Softmart

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

Red Hat/Netscape/Firefox

Through negotiations with August Schell Enterprises, DISA has established a DoD-wide enterprise site license whereby DISA can provide ongoing support and maintenance for the Red Hat Security Solution server products that are at the core of the Department of Defense's Public Key Infrastructure (PKI). The Red Hat Security Solution includes the following products: Red Hat Certificate System and dependencies; Red Hat Directory Server; Enterprise Web Server (previously Netscape Enterprise Server); and Red Hat Fortitude Server (replacing Enterprise Server).

August Schell also provides a download site that, in addition to the Red Hat products, also allows for downloading DISA-approved versions of the following browser products: Firefox Browser; Netscape Browser; Netscape Communicator; and Personal Security Manager.

The Red Hat products and services provided through the download site are for exclusive use in the following licensed community: (1) All components of the U.S. Department of 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

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

WEB LINK: www.disa.mil

Red Hat

RED HAT LINUX: Provides operating system software license subscriptions and services to include installation and consulting support, client-directed engineering and software customization. Red Hat Enterprise Linux is the premier operating system for open source computing. It is sold by annual subscription, runs on seven system architectures and is certified by top enterprise software and hardware vendors.

CONTRACTORS:

Carahsoft Technology Corp. (HC1028-09-A-2004)

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

Carahsoft: 09 Feb 14

DLT Solutions, Inc.: 17 Feb 14

WEB LINKS:

Carahsoft Technology Corp.

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

DLT Solutions, Inc.

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

Research & Advisory

Gartner Inc.

GARTNER INC.: Research and Advisory Services BPAs provide unlimited access to telephone inquiry support, access to research via websites and analyst support for the number of users registered. In addition, the services provide independent advice on tactical and strategic IT decisions. Advisory services provide expert advice on a broad range of technical topics and specifically focus on industry and market trends. The BPA Ordering Period commences 12/01/2006 and is effective for the term of the GSA FSS Schedule. The BPA will be reviewed annually and is contingent upon the Contractor maintaining or renewing GSA Schedules GS-35F-5014H.

CONTRACTOR:

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

ORDERING EXPIRES: 31 Mar 13

WEB LINK:

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

Forrester Research

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

CONTRACTOR:

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

Ordering Expires: 10 Aug 2013

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

Department of the Navy Agreements

Oracle (Deal-O)

Database Enterprise License

for the Navy

On Oct. 1, 2004 and May 6, 2005, the Navy established the Oracle Database Enterprise License, effective through Nov. 1, 2013. The enterprise license provides Navy shore-based and afloat users, to include active duty, Reserve and civilian billets, as well as contractors who access Navy systems, the right to use Oracle databases for the purpose of supporting Navy internal operations. Navy users in joint commands or supporting joint functions should contact Dan McMullan, NAVICP Mechanicsburg contracting officer, at (717) 605-5659 or email daniel.mcmullan@navy.mil, for further review of the requirements and coverage.

This license is managed by the Space and Naval Warfare Systems Center (SPAWAR-SYSCEN) 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

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.peoeis.portal.navy.mil/pmm110/default.aspx>. Since this is a dynamic environment, other

policies may be added with little notice. Information about ordering products via DON ELAs can also be found at this site.

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

WEB LINKS:

DON CIO

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

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

www.esi.mil

DoD ITAM Reports on Software Asset Management Resources

The Department of Defense (DoD) IT Asset Management (ITAM) team has noted progress on several fronts for DoD employees who are responsible for Software Asset Management (SAM). For example:

- ITAM is collaborating with a TagVault work group on defining secure asset management. TagVault.org is the registration authority for ISO/IEC 19770-2 software identification tags. Mitre—a collaborator on Information Security Community standardization activities and initiatives for making security measurable—has joined the TagVault board and is working as part of the TagVault work group defining Common Platform Enumerator (CPE) requirements. CPE is a standardized approach for identifying and describing an enterprise's computing assets, including: applications, operating systems, and hardware devices.
- The DoD is encouraging use of the ISO 19770-2 standard that establishes specifications for tagging software to optimize its identification and management.



ESI News

ESI Newsletter - Summer 2012

NEW BPA PROVIDES ACCESS TO FORRESTER RESEARCH AND ADVISORY SERVICES

On August 10, 2012, the Department of the Navy awarded a new Blanket Purchase Agreement (BPA) to Forrester Research — an independent technology and market research company. Forrester provides proprietary research, business data, custom consulting, and other services to help leaders in the technology market address their specific challenges. The new DoD ESI BPA with Forrester is available to all DoD components including the Intel community—and offers additional discounts beyond GSA pricing. More details including ordering information and the complete document can be found at www.esi.mil/.contentview.aspx?id=313&type=1.

- Microsoft has announced its support for the ISO-IEC 19770-2 software asset tag standard. It has already embedded -2 tags in some of its products and is committed to incorporating them into the planning cycle for future product releases.
- DoD has submitted a change request to the DoD IT standards registry (DISR) to add the ISO-IEC 19770-2 standard as an emerging technology with a plan to mandate it for all commercial software vendors in the future.
- GSA has re-established the Federal Software Asset Management (SAM) work group. The DoD IT Asset Manager is working with the GSA to help in defining the way forward for SAM.

New BPAs Deliver up to 33% Discount for Adobe Software

On July 1, 2012, the Department of the Navy IT Umbrella Program and the Naval Supply Systems Command, Weapon Systems Support, Mechanicsburg, Pennsylvania established multiple Enterprise Software Agreements (ESAs) for Adobe Digital Media (formerly Adobe Desktop)

software products on behalf of the DoD ESI Project (www.esi.mil). These ESAs expire 6/30/2016, after two one-year-option ordering periods.

The ESAs were established as Blanket Purchase Agreements (BPAs) against General Services Administration (GSA) Federal Supply Schedules, and include software licenses, upgrade licenses, maintenance, media, and documentation. Some of the Adobe Digital Media products offered through these BPAs include the Adobe Acrobat family, Adobe Creative Suite family, Adobe eLearning Suite, and Adobe Captivate, as well as other software programs. The BPAs offer discounts up to 33 percent off GSA TLP prices and are open for ordering by all DoD components, the Intelligence Community, the U.S. Coast Guard and authorized contractors. Prices are reviewed annually and spot discounting is encouraged.

The BPAs and ordering instructions can be found on the DoD ESI website at www.esi.mil/agreements.aspx?id=301.

In accordance with DFARS 208.74, software buyers must check the DoD ESI for inventory or an ESA before using another method to purchase any software products.

USS ENTERPRISE

The aircraft carrier USS Enterprise (CVN 65) arrives at Naval Station Norfolk Nov. 4, 2012. Enterprise's return to Norfolk will be the 25th and final homecoming of her 51 years of distinguished service. The Enterprise was inactivated Dec. 1, 2012.

U.S. Navy photo by Mass Communication Specialist 1st Class Rafael Martie.

