

Sharing Information - Technology - Experience

CHIPS

January - March 2010

NAVY'S NEW STRATEGY AND ORGANIZATION FOR INFORMATION DOMINANCE

OPNAV N0194

GETTING FROM NMCI TO NGEN

Report from PEO EIS PMAV 310

U.S. JOINT FORCES COMMAND PROVIDES GLOBAL FORCE MANAGEMENT

USJFCOM J214 Air Force BRIG GEN Robert Yates



Radio Frequency and Electromagnetic Spectrum

**Department of the Navy
Chief Information Officer**
Mr. Robert J. Carey

Space & Naval Warfare Systems Command
Commander Rear Admiral Michael C. Bachmann

Space & Naval Warfare Systems Center Atlantic
Commanding Officer Captain Bruce Urbon

Senior Editor
Sharon Anderson

Assistant Editor
Nancy Reasor

Layout and Design
Sharon Anderson

Web Support
Tony Virata
DON IT Umbrella Program

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

Contributors
Eric Carr, DON CIO Graphics
Lynda Pierce, DON CIO Communications

CHIPS is sponsored by the Department of the Navy Chief Information Officer (DON CIO) and the DON IT Umbrella Program Office, Space and Naval Warfare Systems Center Pacific.

CHIPS is published quarterly by the Space and Naval Warfare Systems Center Atlantic. USPS 757-910 Periodical postage paid at Norfolk, VA and at an additional mailing office. POSTMASTER: Send changes to CHIPS, SSC Atlantic, 9456 Fourth Ave., Norfolk, VA 23511-2130.

Submit article ideas to CHIPS at chips@navy.mil. We reserve the right to make editorial changes. All articles printed in CHIPS become the sole property of the publisher. Reprint authorization will be granted at the publisher's discretion.

Requests for distribution changes or for other assistance should be directed to Editor, CHIPS, SSC Atlantic, 9456 Fourth Ave., Norfolk, VA 23511-2130, or call (757) 443-1775; DSN 646. E-mail: chips@navy.mil; Web: www.chips.navy.mil.

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

Don't miss a single issue of CHIPS! To request extra copies or send address changes, contact CHIPS editors at chips@navy.mil or phone (757) 443-1775, DSN 646.



COVER

The vivid colors of the electromagnetic spectrum. In this issue, members of the Department of the Navy electromagnetic spectrum community provide a look at the many applications of spectrum and the ways that the DON ensures that naval forces have global access for spectrum-dependent communications and combat systems. Articles begin on page 6.



The Department of the Navy Chief Information Officer's Spectrum Team: Tom Kidd (middle) is the director of Strategic Spectrum Policy for the DON. Mark Rossow (left) is senior adviser to the director on Department of Defense, federal and national regulatory spectrum issues. Steve Ward (right) is senior adviser to the director on bilateral and international treaty interests.



Statement of Ownership, Management and Circulation

The U.S. Postal Service requires all publications to publish a statement of ownership, management and circulation.

Date	1 July 2009
Title of Publication	CHIPS
Title of Publisher	U.S. Navy
USPS Publication Number	ISSN 1047-9988
Editor	Sharon Anderson
Frequency of Issue	Quarterly
Owner	U.S. Navy
Total No. of Copies Printed	31,540
No. Copies Distributed	31,540
No. Copies Not Distributed	0
Total Copies Distributed and Not Distributed	31,540
Issue Date for Circulation	July-September 2009
Location of Office of Publication	SPAWARSYSCEN Atlantic CHIPS Magazine 9456 Fourth Ave Norfolk, VA 23511-2130

Navigation Guide



FEATURES

6 The Electromagnetic Spectrum

Articles begin on page 6

16 Navy's New Strategy and Organization for Information Dominance

Information emerges as a core warfighting capability equivalent to seapower and airpower

20 Getting from NMCI to NGEN

Early Transition Activities will ensure seamless follow-on of the Next Generation Network

22 U.S. Joint Forces Command Provides Global Force Management

Air Force Brig. Gen. Robert Yates discusses the new surge of 30,000 troops to Afghanistan

IN EVERY ISSUE

4 Editor's Notebook

5 Message from the DON CIO

12 Full Spectrum

33 Web 2.0

35 Hold Your Breaches!

37 Going Mobile

42 The Lazy Person's Guide

45 Enterprise Software Agreements



From the DON CIO

6 Greener Spectrum

By Tom Kidd

8 Climate Monitoring

By Tom Kidd

9 Using the DON Enterprise Architecture to Support Critical Decision Making Processes

By Victor Ecarma

10 Enabling Future Naval Capabilities NAVSEA Headquarters' Perspective

By Mr. D. Mark Johnson and Mr. J. Don Pierce

14 The U.S. Navy's New Electromagnetic Pulse (EMP) Program

By Blaise Corbett and James Partak

25 Radio 2050

By Tom Kidd

38 Identity Management Operations to Improve Cybersecurity

By Sonya Smith

International Spectrum

44 Iraqi Government Begins Management of the High Frequency Radio Band

By Multi-National Force-Iraq Public Affairs

New Technologies

26 Advances in Magnetometer Technology

By Tom LaPuzza

30 Coalition Warrior Interoperability Demonstration 2010

By Sharon Anderson

C4ISR

28 SPAWAR Releases Naval IT, C4ISR, Space Systems, and Enterprise Support: Today and Tomorrow – *New technical vision for the C4ISR, Business IT and Space Community*

Around the Fleet

34 Remote Testing Using ADEPT

New test equipment saves money and time in maintenance and repair

By Joel H. Timm

Navy Training

36 Navy's Chief Training Officer Addresses Defense Contractors and DoD Reps

By Joy Samsel

Navy Medicine

40 NSIPS Enhancements Help Navy's Aspiring Healthcare Professionals Receive Faster, More Accurate Financial Benefits

By Deborah Gonzales

New DON Principal Deputy CIO Selected



Barbara Hoffman has been selected by the Department of the Navy Chief Information Officer, Rob Carey, to serve as the DON Principal Deputy Chief Information Officer. Her appointment was based on her years of exceptional leadership within the DON CIO. Hoffman has served previously as Acting DON Principal Deputy CIO and Director of Operations.

As DON Principal Deputy CIO, Hoffman is the principal adviser to the CIO and is responsible for managing and leading the DON CIO staff; developing information management/information technology strategies for achieving enterprise integration across the department; leading change efforts; and ensuring effective communication among the CIO, the Navy and Marine Corps staffs, as well as all other constituent customers and stakeholders. As Principal Deputy CIO, Hoffman also assumes the role of DON Senior Information Assurance Officer.

Editor's Notebook

In this issue, we look at the many facets of managing the electromagnetic spectrum, more commonly known as the radio frequency band, with articles from the DON CIO, NAVSEA and the Multi-National Force-Iraq.

The array of spectrum topics demonstrates the complexities and wide scope of spectrum needs, from personal devices, to Defense Department systems and communications, to the radio frequencies allocated across the international community.

The use of the electromagnetic spectrum is something that we take for granted. I don't know about you, but take away my cell phone, garage door opener, satellite radio, or other entertainment and convenience devices, and I'm pretty grumpy. A more serious concern is how critical the use of the electromagnetic spectrum is to the defense, security and economic well-being of the United States.

Use of the electromagnetic spectrum has implications in our other feature articles as well, including the CNO-directed reorganization of the N2 and N6 directorates into the newly stood up Deputy Chief of Naval Operations for Information Dominance (N2/N6); the DON's strategy for transition from the Navy Marine Corps Intranet to the Next Generation Enterprise Network; and the president's directive for a surge of 30,000 troops to Afghanistan to increase security and combat the insurgency.

This extraordinary logistics campaign is discussed by Air Force Brig. Gen. Robert Yates, USJFCOM's director for Operations, Plans, Logistics and Engineering (J3/4). USJFCOM, in its primary force provider role, is helping combatant and operational commanders plan and synchronize the deployment of forces to carry out the president's strategy.

Try to imagine the spectrum resources that will be required for the communications and operational needs of 30,000 additional troops in Afghanistan. It's a sobering thought for the new year.

Welcome new subscribers!
Sharon Anderson



HELMAND PROVINCE, Afghanistan – Marines and Sailors with 1st Battalion, 6th Marine Regiment disembark a C-17 cargo plane at Camp Bastion, Dec. 15, 2009, in support of Operation Enduring Freedom. For many of the junior Marines and Sailors of 1/6, this is their first deployment, and in many cases, their first time outside of the United States. For others, the deployment marks a return to Afghanistan after serving there in 2008.

The Marines and Sailors grabbed their gear and loaded into white buses turned brown from dust and set out to Camp Leatherneck where they filed into ballroom-size tents and picked out places to bed down in their new home.

Later, the Marines get on phones to hear the voices of friends, wives and children. Card and board games are played between training and work, as the Marines and Sailors seek out a routine that can be maintained throughout the course of their deployment.

Photo and story courtesy of American Forces Press Service. (Go to www.defense.gov/ for more Defense Department news.)



ATTACK COURSE – A U.S. Marine fire team advances toward an enemy position after receiving simulated enemy contact during a training exercise on Camp Dwyer, Afghanistan, Jan. 2, 2010. The Marines ran an attack course focused on the positive identification of targets and precision fires to reduce the risk of civilian casualties during future operations. The fire team is assigned to Bravo Company, 1st Battalion, 6th Marine Regiment. *U.S. Marine Corps photo by Lance Cpl. James W. Clark.*

Past CHIPS editions have addressed and focused on well-known information technology (IT) areas such as knowledge management and computer network defense. However, this edition highlights a lesser-known area that often isn't directly associated with IT even though it is vital to nearly all Navy and Marine Corps information based capabilities — the management of the electromagnetic spectrum. Frequencies in the electromagnetic spectrum, what many people recognize as radio frequencies, provide the invisible medium that enables all wireless capabilities. These capabilities range from use of our BlackBerrys, to our garage and car door openers, to our ability to send aviation-based jamming signals.

"Spectrum" is, quite simply: Electromagnetic energy our technology uses to sense, interfere or communicate wirelessly. While radio frequencies provide the preponderance of naval spectrum use, Navy and Marine Corps spectrum use is pervasive and also includes microwave, infrared and visible light frequencies.

The use of spectrum to enable wireless capabilities throughout the world is and has been escalating at a feverish pace. Commercial demand for spectrum continues to grow as does the Navy's and Marine Corps' demand. Spectrum is critical to our nation's economic strength, as well as our national defense, and the same is true for many nations of the world. In areas of the world that have high population densities, spectrum congestion is occurring. As a result, ensuring access to spectrum for the global requirements of our naval services has become challenging in many geographical areas including areas within the United States.

Recognizing that spectrum access and use is vital to the Navy and the Marine Corps, the Department of the Navy is heavily and continuously engaged in the diverse task of "spectrum management." The electromagnetic spectrum is governed by one immovable force, the law of physics, and as such, it is a limited resource for the entire world to use.

Spectrum management includes international and national strategic efforts, dynamic and complex operational efforts, and technically challenging spectrum supportability efforts. And all of these tasks involve the coordinated actions of the DON's leadership, its operational forces, and the naval acquisition com-



munity. Whether planning contingency communications two hours in advance, or negotiating spectrum treaty language that will affect our forces for coming decades, department Navy and Marine Corps spectrum personnel are assuring our Sailors and Marines have access to this vital resource when and where they need it.

To more effectively use this finite resource, the DON is investing in the development of advanced technology. Software defined radios, dynamic spectrum access and cognitive radio systems are just some of the emerging spectrum technologies

that promise greater spectrum efficiency, fewer operational constraints and advanced capabilities for global deployment. But technology alone will not satisfy the world's requirements for spectrum. As spectrum use has increased among industry, the public and defense community, so must the coordination

and sharing of this important resource. The DON will meet this challenge, as it has with all IT challenges it has faced, to ensure its naval services are fully capable anytime — anywhere.

To this end, this issue of CHIPS explores different aspects of our employment of systems that use components of the electromagnetic spectrum. The information presented won't make anyone an expert on all spectrum-related matters. However, it does address a number of topics that affect requirements and challenges for spectrum use by the Navy and Marine Corps.

SPECTRUM IS CRITICAL TO OUR NATION'S ECONOMIC STRENGTH AS WELL AS OUR NATIONAL DEFENSE

Finally, I am proud to establish **The John J. Lussier Electromagnetic Spectrum Leader-**

ship Award. Named for our Principal Deputy Chief Information Officer who lost his courageous battle with cancer in June 2009, the award will be presented to an individual that demonstrates superior achievement in naval electromagnetic spectrum management and use. John Lussier was a true champion for strategic investment in electromagnetic spectrum. His legacy lives on in every Marine, Sailor and civilian dedicating their career to assuring the department's spectrum access today, tomorrow and into the future.

For further information about the award, send questions to DONSpectrumTeam@navy.mil.

— Robert J. Carey



DEPARTMENT OF THE NAVY - CHIEF INFORMATION OFFICER

www.doncio.navy.mil



Greener Spectrum

by Tom Kidd

While the range between 540 – 610 in terahertz (THz) is (literally) the “green” portion of the electromagnetic spectrum, that isn’t what we are going to discuss here. This article introduces the concept of the electromagnetic spectrum as a critical resource in the study of climate change. The Department of the Navy electromagnetic spectrum community supports many different radio and telecommunication technologies including equipment for weather and climate change monitoring, prediction, detection and mitigation in the event of hurricanes, typhoons, thunderstorms, earthquakes, tsunamis, man-made disasters, and more.

During his visit to the International Telecommunication Union (ITU) headquarters in June 2007, the United Nations Secretary-General, Mr. Ban Ki-moon, remarked that the “International Telecommunication Union is one of the most important stakeholders in terms of climate change.” He also described climate change as the “moral challenge of our generation.”

The United States was one of 120 countries to develop a new digital broadcasting plan at the 2006 ITU Regional Radiocommunication Conference. The plan envisages significant reduction (by almost 10 times) in transmitter power and a reduction in the number of transmitters (due to the possibility of transmitting several television and sound programs on one channel) in the 120 participating countries. Such high-level policies may not be considered in the front lines of climate change, but taking into account that there are roughly 100,000 transmitters in these 120 countries with power capacity of up to 100-150 kilowatts each, and most of them operating 24 hours a day, the energy savings will be significant!

Department of the Navy members of the U.S. delegation to the ITU assure the department’s technological advances are considered in international treaties on radio regulations. The DON spectrum team has been a key member of the ITU study group that developed the “Land Mobile Handbook (including Wireless Access) - Volume 4: Intelligent Transport Systems.” This handbook describes the use of radio technologies for minimizing transportation distances and costs that will also have a positive effect on the environment. It also pushes cutting-edge technology by introducing the use of vehicles as environmental monitoring tools to measure air temperature, humidity and precipitation by sending data through wireless links for weather forecasting and climate control.

Meeting every four years, the World Radiocommunication Conferences (WRC) analyze spectrum requirements. They also allocate spectrum for radiocommunication systems and radio-based applications employed for environmental and climate monitoring. Decisions made by the WRC provide support for the development and operation of systems involved in weather and disaster prediction, detection and relief. This includes weather satellites that track the progress of hurricanes and typhoons;

weather radars for tracking tornadoes, thunderstorms, the effluent from volcanoes and

major forest fires; and radio-based meteorological aid systems that collect and process weather data. International radio regulations facilitate the successful operations of diverse radiocommunication systems (satellite and terrestrial) used for disseminating information concerning natural and man-made disasters.

The WRC and Radiocommunication Assembly 2007 adopted a number of resolutions on studies related to remote sensing, which is a vital component in the science of climate change. They included a recommendation on radiocommunication systems and radio-based applications operating in the Earth Exploration Satellite, and meteorological aids and meteorological satellite services, which provide most of the data for the Global Observing System and Global Climate Observing System.

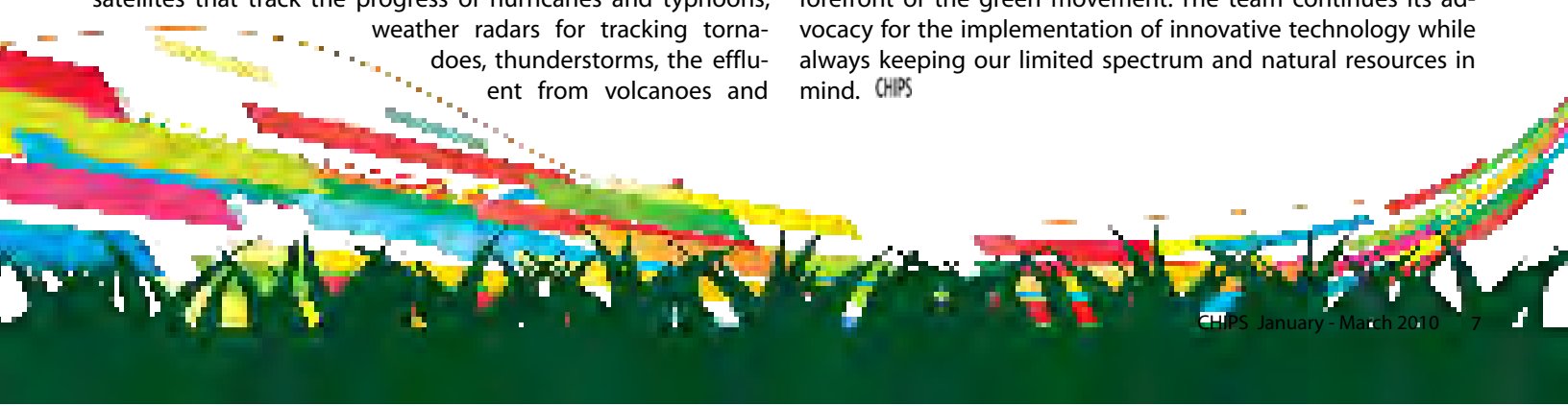
Also in 2007, the ITU, in cooperation with the World Meteorological Organization, produced a handbook on the “Use of Radio Spectrum for Meteorology: Weather, Water and Climate Monitoring and Prediction.” It provides information on the development and proper use of radiocommunication systems and radio-based technologies for environmental observation, climate control, weather forecasting, and natural and man-made disaster prediction, detection and mitigation.

DON members of the U.S. delegation to WRC 2007 were instrumental in the adoption of a resolution requesting the establishment of a database of available frequencies for use in emergency situations. This resolution also urges administrations to provide relevant up-to-date information concerning their national frequency allocations and spectrum management practices for emergency and disaster relief radiocommunication operations.

Radiocommunication Assembly 2007 also approved resolutions instructing all ITU radiocommunication sector study groups to carry out studies on the use of radiocommunication in disaster prediction, detection, response, mitigation and relief. In many cases, when disaster strikes, the “wired” telecommunication infrastructure is significantly or completely destroyed, and only radiocommunication services can be employed for disaster relief operations.

The study groups have developed recommendations, reports and handbooks related to the use of radiocommunication for the mitigation of the negative effects of climate change and natural and man-made disasters. Mitigation of the negative effects of climate change is another important area of the ITU Radiocommunication sector activities.

In April 2009, the DON Chief Information Officer, along with the Assistant Secretary of the Navy for Research, Development and Acquisition and the Assistant Secretary of the Navy for Installations and Environment, signed the “Department of the Navy Strategy for Green IT Electronic Stewardship and Energy Savings.” Although the relationship of “green IT” and spectrum may be new to some, the DON spectrum team has been at the forefront of the green movement. The team continues its advocacy for the implementation of innovative technology while always keeping our limited spectrum and natural resources in mind. CHIPS



Climate Monitoring

The Department of the Navy Chief Information Officer (DON CIO) represented the DON at the first International Telecommunication Union (ITU) and World Meteorological Organization (WMO) joint seminar in September 2009. It was organized as an open forum for discussion of the ITU and WMO roles in the use of radio spectrum, space orbits and radio-based meteorological tools and systems for monitoring, mitigation and adaptation to climate change.

Between 1980 and 2005, more than 7,000 natural disasters worldwide took the lives of approximately 2 million people and produced economic losses estimated at more than 1.2 trillion in U.S. dollars. Ninety percent of these natural disasters, 72 percent of the casualties, and 75 percent of the economic losses were caused by weather, climate and water-related hazards, such as droughts, floods, severe storms and tropical cyclones. For this reason, climate change monitoring and disaster prediction mechanisms are increasingly vital for our personal safety and economic well-being.

Radio-based applications, such as remote sensors, are the main source of information about the Earth's atmosphere and surface. For 135 years, there has been an excellent partnership between the WMO and ITU. The WMO focuses its efforts on meeting the needs for environmental information and the corresponding radio frequency spectrum resources. The ITU, as international steward of the spectrum, allocates the necessary radio frequencies to allow the interference-free operation of radio-based applications and radiocommunication systems (terrestrial and space) used for climate monitoring and prediction, weather forecasting, and disaster early warning and detection.

The primary goal of the ITU/WMO seminar was to provide a forum to exchange information about meteorological and radio-frequency spectrum management services and authorities on the use and development of radio-based space and terrestrial systems and applications employed for weather, water and climate monitoring, and the relevant radio frequency spectrum management activities.

The main issues discussed were:

- The role of information communication technologies in general, and radio-based technologies in particular, in monitoring climate change;
- WMO and ITU roles in development, use and effective operation of systems and applications for monitoring the environment; prediction and detection of natural disasters; and mitigation of the negative effects of disasters initiated by climate change;
- Status and development of radio-based systems and applications for weather, water and climate monitoring and prediction;
- Operation of meteorological systems and quality of meteorological measurements; and



The Earth Exploration Satellite (discussed on the previous page) is used for the establishment of radiocommunication service between Earth stations and one or more space stations, which may include links between space stations, in which information relating to the characteristics of the Earth and its natural phenomena is obtained from active or passive sensors on Earth satellites. Similar information is collected from airborne or Earth-based platforms, such information may be distributed to Earth stations within the system concerned, and platform interrogation may be included.

– European Union

- Activities of other national and international organizations in climate monitoring and disaster prediction, and detection and mitigation of the negative effects of disasters. CHIPS

The text for Greener Spectrum and Climate Monitoring was compiled from information published on the ITU's Web Site at www.itu.int/ by Mr. Tom Kidd, DON director of strategic spectrum policy and delegate to the United Nations ITU World Radiocommunication Conference in 2007. Send questions to DONSpectrumTeam@navy.mil, or go to the DON CIO Web site: www.doncio.navy.mil.

Using the DON Enterprise Architecture to Support Critical Decision Making Processes

By Victor Ecarma

The DON Enterprise Architecture helps decision makers make informed decisions about investments in new technology and, at the same time, capitalize upon vast existing technology assets. In addition, the DON EA is focused on maintaining alignment between the department's goals and objectives, and its information management/information technology (IM/IT) investments.

Since both technology and business needs change over time, the DON EA must be flexible enough to respond to these changes, yet do so in a controlled manner and with minimal adverse impact.

The DON EA's success is dependent upon its relevance and value to DON decision makers and program managers. As the "Chief Architect" of the department, the DON Chief Information Officer (CIO) is leading the effort to design and develop a single integrated DON EA that includes Navy and Marine Corps architectures and federates with external partners' and organizations' architectures.

The DON EA will describe policy requirements, processes, information flows, solutions, data descriptions, technical infrastructure and standards. It will support developing weapons, intelligence and business systems, and enterprise IT infrastructure and core services. Currently, DON EA compliance is incorpo-

and Navy Echelon II Command Information Officers and Marine Corps C4 for programs categorized as ACAT III and below.

DON EA Compliance as part of the DON IM/IT Investment Review Process

DON IM/IT investment reviews are required for all programs, systems and initiatives within the Business Mission Area (BMA) and the Enterprise Information Environment Mission Area (EIEMA). DON IM/IT investment reviews are required before obligating any development/modernization funding and as part of annual reviews. The reviews must be completed by May 15 of each year.

DON EA compliance must be demonstrated as part of the DON IM/IT investment review package. Program managers must show compliance using the DECAT before submitting the annual review package for their IT investment. In addition, all required waivers must be submitted and approved before submitting the annual review package. Program managers' assertions of compliance with the DON EA will be reviewed as part of the normal IM/IT investment annual review process.

Currently, the DON CIO is the pre-certification authority for Tiers 1 through 3 defense business systems. Pending legislation may mandate that military department chief management of-

DON EA'S SUCCESS IS DEPENDENT UPON ITS RELEVANCE AND VALUE TO DON DECISION MAKERS AND PROGRAM MANAGERS

rated into two existing processes: the Clinger-Cohen Act (CCA) confirmation process and the IM/IT investment review process. Additionally, the requirement for assessing compliance, with the DON EA as part of these processes, has been incorporated into the department's annual IT budget execution policy.

Clinger-Cohen Act Confirmation

Clinger-Cohen Act confirmation is required for all information technology, including National Security Systems, before any acquisition milestone, contract award, or full-rate production or full deployment decision. As of Oct. 1, 2009, DON EA compliance must be demonstrated as part of all CCA confirmations.

Program managers must show compliance using the DON EA Compliance Assessment Tool (DECAT) before submitting the CCA package for review. In addition, all required waivers must be submitted and approved before the CCA package is submitted. Program managers' assertions of compliance with the DON EA will be reviewed as part of the normal CCA sign-off process.

The final DON CCA approval authorities are the DON CIO for programs categorized as Acquisition Category (ACAT) I and II,

and Navy Echelon II Command Information Officers and Marine Corps C4 for programs categorized as ACAT III and below. The Defense Business Systems Management Committee is the final Office of the Secretary of Defense (OSD) approval authority.

The DON CIO is the approval authority for all other BMA and EIEMA Tier 3 investments, and the DON Deputy CIO (Navy or Marine Corps) is the approval authority for Tier 4 and non-tier reviews.

DECAT and other DON EA information, including training, may be accessed at <http://www.intelink.gov/go/98617>. All DON EA information is "For Official Use Only" and access to the site requires an account to Intelink, the U.S. government's collaborative Web site. CHIPS

Victor Ecarma provides support to the DON CIO enterprise architecture and emerging technology team.

Enabling Future Naval Capabilities

NAVSEA Headquarters' Perspective

By Mr. D. Mark Johnson and Mr. J. Don Pierce

Naval Sea Systems Command is comprised of command staff, headquarters directorates, affiliated program executive offices (PEOs) and numerous field activities. NAVSEA is accountable to the Chief of Naval Operations to deliver, modernize and maintain a 313-ship Navy that meets our national security requirements. NAVSEA has the further responsibility of establishing and enforcing technical authority in combat system design and operation. NAVSEA's technical standards ensure systems are engineered effectively, and that they operate safely and reliably.

NAVSEA is the "technical authority" for the following electromagnetic spectrum-related issues that affect ships and submarines: electromagnetic interference (EMI) control; electromagnetic compatibility (EMC); electromagnetic pulse (EMP); and radiation hazards (RADHAZ). As a technical warrant holder, NAVSEA's Force E3/Spectrum Office controls EMI, the spectrum and EMP impact on the effectiveness of warfare systems, to maintain warfighting readiness for all ships, submarines and systems.

The electromagnetic environment (EME), in which naval systems must operate, is created by a multitude of sources. Primary contributors are ships, forces, other friendly transmissions, enemy transmissions, spurious emissions from equipment, the ship's metallic hull, natural and environmental noise, and possibly EMP resulting from a nuclear burst. The dominant contributor(s) to the EME depend on the platform's (or system's) location and operating circumstances. Many elements of the EME are vital to system performance; others are potential sources of EMI. Electromagnetic signals vital to one system's performance may prove fatal to another system's performance. An increased awareness of the EME will enhance identification and reduction of platform/system EMI.

Defense Department policy requires all electrical and electronic systems, subsystems and equipment, including ordnance containing electrically initiated devices, to be mutually compatible in their intended EME without causing or suffering unacceptable mission degradation due to electromagnetic environmental effects (E3).

Accordingly, appropriate E3 requirements must be imposed to ensure a desired level of compatibility with collocated equipment (intra-system) within the applicable external EME that may include intersystem, radio frequency, lightning, EMP and precipitation static. E3 requirements must also address safety of personnel, ordnance and fuel.

In addition, national, international and DoD policies and procedures for the management and use of the electromagnetic spectrum direct program managers developing spectrum-dependent systems or equipment to consider spectrum supportability requirements and E3 control early in the development process, and throughout the acquisition life cycle.

NAVSEA's Force E3/Spectrum Office's goal is to partner with each system, ship or submarine program to provide the best products to the warfighter. This is accomplished by getting plugged-in at the earliest stages of program development. NAVSEA subject matter experts help guide individual programs through the E3/spectrum certification (SC) process, requirements identification and controls implementation, and through the Technical Warrant Pyramid (Figure 1).

NAVSEA Headquarters leads the tri-SYSCOM organization consisting of Space and Naval Warfare Systems Command (SPAWAR), NAVSEA and Naval Air Systems Command (NAVAIR) for EMI control, EMP and spectrum certification matters.



NAVSEA

NAVAL SEA SYSTEMS COMMAND

Figure 1 shows the top-down organization of the Force Level EMC Program. At the headquarters level, front line systems engineers interface with the various PEOs (PEO Ships, PEO Carriers, etc.). At the field activity level, NAVSEA designates engineering agents (EAs) for specific functional areas. These EAs form teams of subject matter experts to assist in the investigation and resolution of EMI problems ashore and afloat. These activities champion and execute E3/spectrum management (SM) in the design, development, procurement and integration of equipment and platforms, as well as naval shore sites.

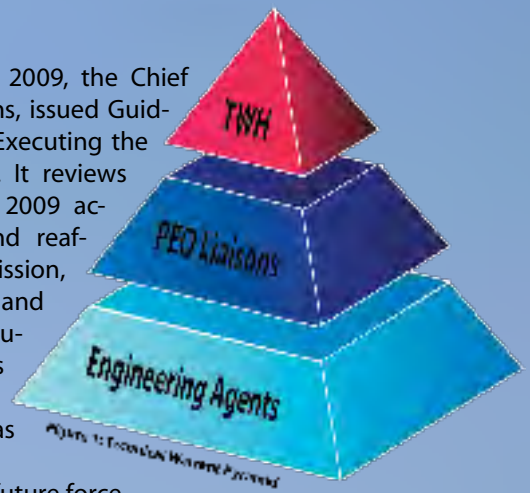
The Technical Warrant Pyramid illustrates the depth of knowledge and expertise that exists within the Force Level EMC Program. This team maximizes operational performance and safety with respect to E3 and spectrum management in ships and submarines, their combat systems and shore installations.

The key to enable future naval capabilities is well-engineered warfare systems. This is accomplished through a disciplined up-front systems engineering effort, which includes the review of acquisition documents (initial capability documents, capability development documents, capability production documents, or capstone requirements documents).

To ensure EMC for new systems introduced into the fleet, NAVSEA reviews ship change documents and ensures that systems attain spectrum certification. NAVSEA ensures the performance and readiness of current naval systems and that platforms are ready to fight by executing shipboard EMC and RADHAZ certification, the Submarine Pre-Deployment EMC Survey, and providing direct fleet and program manager support.

The NAVSEA team exercises technical authority by holding formal technical warrant holder reviews, thereby enforcing electromagnetic environmental effects/spectrum certification acquisition policies and providing E3/SC technical subject matter expert guidance.

In September 2009, the Chief of Naval Operations, issued Guidance for 2010 for Executing the Maritime Strategy. It reviews the Navy's major 2009 accomplishments and reaffirms the vision, mission, guiding principles and focus areas articulated in last year's guidance. The Navy's focus areas remain:



- Build the future force.
- Maintain our warfighting readiness.
- Develop and support our Sailors and Navy civilians.

The CNO Guidance 2010 places emphasis on the following five objectives:

- Continue to be the dominant, ready naval force across all maritime missions.
- Build a Navy with appropriate force structure and strategic laydown.
- Achieve decision superiority.
- Align the requirements, resources and acquisition processes.
- Evolve and establish international relationships.

The CNO Guidance is a basis for NAVSEA's Force E3/Spectrum Office's goals to ensure we build the future force through an up-front engineering process and maintain our warfighting readiness through ship maintenance and developing our Sailors and Navy civilians. CHIPS

Mr. D. Mark Johnson is the OPNAV program spectrum supportability, electromagnetic environmental effects and electromagnetic pulse coordinator.

Mr. J. Don Pierce, is the director of the NAVSEA Force Level E3/Spectrum Office.





Full Spectrum

Assessing Spectrum Supportability

By Tom Kidd

The electromagnetic spectrum is a critical enabler of the Department of the Navy's ability to communicate and operate in a global environment. Now more than ever before, deployed Sailors and Marines depend on the electromagnetic spectrum because it enables nearly all Navy and Marine Corps capabilities, including strategic command and control; tactical communications (airborne and ground); intelligence, surveillance and reconnaissance; and radar, navigation and weapons systems.

Spectrum is also important to world commerce because it enables a vast array of wireless capabilities, including e-mail, mobile telephone, and other capabilities that are now essential to modern-day business and life. While spectrum is a finite natural resource, it is readily available in most rural areas of the world.

However, spectrum is congested in major metropolitan areas which include many coastal regions of the world. As a result, spectrum can be challenging to acquire in some geographical areas of the world and easily acquired for use in others.

The ability of Navy and Marine Corps forces to support diverse missions is critically dependent on the availability of spectrum. This availability is determined by a number of varying factors, including a host nation's allocation and control of spectrum within its borders, congestion, and operational requirements of spectrum-dependent equipment and systems.

Due to diverse and unique governance within many sovereign nations, spectrum-dependent systems and equipment procured for U.S. military use should be planned and designed for multiband operation or provide significant tuning flexibility to maximize global use.

Spectrum supportability is an assessment of whether the electromagnetic spectrum necessary to support the operation of spectrum-dependent equipment or systems will be available when required. While assessing the spectrum supportability for equipment does not constitute the right to operate the equipment, it can identify whether equipment can be supported with spectrum.

Spectrum supportability is composed of a number of processes. Obtaining permission to operate spectrum-dependent equipment may involve a lengthy, multi-step process that should be started as early as possible. It begins with a Spectrum Supportability Assessment (SSA) and includes considerable coordination and scrutiny. The box above contains guidance for ensuring spectrum supportability.

Department of Defense Instruction (DoDI) 4650.01, "Policy and Procedures for Management and Use of the Electromagnetic Spectrum," requires all DoD components to conduct spec-

In addition to the Spectrum Supportability Assessment, spectrum supportability may include the completion of:

- DD Form 1494 – Application for Equipment Frequency Allocation
- U.S. Equipment Certification
- Electromagnetic Environmental Effects (E3) Assessment
- Host Nation Coordination/Approval (HNC/HNA)
- Frequency request/assignment
- Spectrum Supportability Assessment

trum supportability risk assessments as early as possible in the procurement of spectrum-dependent systems or equipment.

The purpose of the risk assessment is "to affect design and procurement decisions" because the early identification of regulatory, technical and operational spectrum supportability risks minimizes the possibility that the spectrum-dependent equipment cannot be employed to support Navy and Marine Corps requirements. Identified risks should be reviewed during acquisition milestones for programs of record and throughout a system's life cycle.

Within the DON, the responsibility for conducting a Spectrum Supportability Assessment resides with the organization procuring or acquiring the spectrum-dependent system or equipment. The composition and level of complexity for conducting a SSA is dependent upon a number of factors including the type of spectrum-dependent equipment and the intended operational area.

While it is necessary to assess the supportability of all spectrum equipment intended for procurement, some equipment requires only completion of the SSA. This would generally include equipment that complies with the "non-licensed" requirements identified in the National Telecommunications and Information Administration's (NTIA) "Manual of Regulations and Procedures for Federal Radio Frequency Management" and for equipment that will not be used outside of the United States and its possessions (US&P).

Equipment of this type often includes wireless peripheral devices such as a wireless mouse or keyboard, wireless routers and Family Radio Service. Any spectrum-dependent equipment intended for use outside of the US&P, regardless of conformance with NTIA non-licensed requirements, is subject to DD Form 1494 – Application for Equipment Frequency Allocation requirements and applicable host nation requirements.

DD Form 1494 – Application for Equipment Frequency Allocation

The DD Form 1494 – Application for Equipment Frequency Allocation is used to record the technical characteristics of spectrum-dependent equipment and apply for host nation coordination and host nation allocation. The technical information documented on the form includes transmitter power, bandwidth and receiver sensitivity. It also includes other data that is essential for the employment of the equipment, HNC/HNA requirements, and frequency requests and assignments.

Host Nation Coordination/Host Nation Approval

In peacetime, international spectrum governance requires military forces to obtain host nation permission to operate spectrum-dependent systems and equipment within a sovereign nation. International governance is honored and enforced by the U.S. departments of State, Defense and Navy. In wartime, international spectrum governance is not honored between warring countries; however, the sovereign spectrum rights of bordering countries must be respected by military forces executing their assigned missions.

Accordingly, HNA is solicited by U.S. naval forces to use spectrum-dependent systems and equipment in bordering countries' airspace and/or on bordering countries' soil. HNA must be obtained before the operation of spectrum-dependent systems and equipment within a sovereign nation. The combatant commander is responsible for coordinating requests with sovereign nations within his or her area of responsibility. Because the combatant commander has no authority over a sovereign nation, the HNC/HNA process can be lengthy.

U.S. Equipment Certification

Equipment certification is a U.S. HNC/HNA process. The NTIA coordinates and reviews equipment certification requests with the agencies of the federal government. U.S. equipment certification ensures that the radio frequencies required for the operation of the equipment can be made available within the United States. It also ensures that equipment that cannot be supported with a radio frequency is not purchased.

Electromagnetic Environmental Effects

The joint definition of electromagnetic environmental effects (E3) is: "the impact of the electromagnetic environment upon the operational capability of military forces, equipment, systems, and platforms. It encompasses all electromagnetic disciplines, including electromagnetic compatibility and electromagnetic interference; electromagnetic vulnerability; electromagnetic pulse; electronic protection; hazards of electromagnetic radiation to personnel, ordnance and volatile materials; and [the] natural phenomena effects of lightning and precipitation static."

Before the acquisition of spectrum-dependent equipment, possible impacts of electromagnetic compatibility (EMC) and electromagnetic interference (EMI) should be considered to ensure the equipment can be employed in its intended operational environment.

The Department of the Navy has established spectrum policy that aligns with international, national and DoD spectrum governance to attain access for all spectrum requirements of the Navy and Marine Corps.

- Secretary of the Navy (SECNAV) Instruction 2400.1, "Electromagnetic Spectrum Policy and Management," provides DON spectrum policy and delegates spectrum responsibilities within the department (available at www.doncio.navy.mil).
- SECNAVINST 5000.2D, "Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System," identifies DON specific requirements associated with the acquisition of spectrum-dependent equipment (available at <http://doni.daps.dla.mil>).
- OPNAVINST 2400.20F, "Electromagnetic Environmental Effects (E3) and Spectrum Supportability Policy and Procedures," provides service-level policy for the Navy while Marine Corps Order 2400.2A, "Marine Corps Management and Use of the Electromagnetic Spectrum," provides Marine Corps spectrum policy (available at <http://www.marines.mil/news/publications> – search on "electromagnetic spectrum").

In accordance with DoD Directive 3222.3, "DoD Electromagnetic Environmental Effects (E3) Program," "Identification of requirements for E3 control shall be initiated early during the concept refinement and technology development phases, fully defined prior to Milestone C, and verified throughout the acquisition process."

Frequency Request and Assignment

A frequency assignment provides authorization for operation of a spectrum-dependent system or equipment under specific requirements and generally applies to a specific geographical area. Frequency assignments must be requested before the operation of systems and equipment and authorized by a proper authority for a given geographical area.

Within the US&P, frequency assignments for use by federal agencies, including the DON, are authorized by the NTIA. Navy and Marine Corps requests for frequency assignments are coordinated with the NTIA under the authority of the DON Chief Information Officer. Outside the US&P, regional combatant commanders authorize and assign frequencies within their area of responsibility; a sovereign host nation is the ultimate authority for use of radio frequencies within its boundaries.

Ensuring spectrum supportability for Navy and Marine Corps equipment and systems is often a complex task in light of global requirements. But despite the enormity of the challenge, the DON maintains a fully capable team of experts to assist and process applicable spectrum supportability requirements. CHIPS

Tom Kidd is the director of strategic spectrum policy for the Department of the Navy. For more information e-mail DONSpectrumTeam@navy.mil.

The U.S. Navy's New Electromagnetic Pulse (EMP) Program

Resurrecting the Capability in a New World

By Blaise Corbett and James Partak

Dormant for more than a decade, the U.S. Navy's Electro magnetic Pulse (EMP) Program is being revived through the Naval Sea Systems Command (NAVSEA) Office of the Director for Force Electromagnetic (EM) Effects and Spectrum Management. The program's immediate goals include establishing cog nizance about current standards for system acquisition as re lated to EMP survivability; assisting with developing standards and methodology to test and assess future systems; assessing the current posture of mission critical systems with regard to EMP survivability; and coordinating with other Department of Defense (DoD) services and entities to share EMP resources and information.

High-Altitude Electromagnetic Pulse

Electromagnetic pulse is a ra diated electromagnetic field, typically generated and as sociated with a nuclear detonation. A nuclear device detonated at an altitude in ex cess of 40 miles generates High Altitude Elec tromagnetic Pulse (HEMP), which is the focus

of the U.S. Navy program. This high altitude nuclear explosion creates high energy photons known as gamma rays. The pho tons collide with molecules in the upper atmosphere creating free electrons called Compton electrons, which then interact with the Earth's geomagnetic field lines to create a HEMP.

HEMP can be characterized as a radio frequency emission with broad frequency content, high electrical field levels up to 100 kilovolts per meter, and high instantaneous power den sity levels that can exceed 20 megawatts per meter squared.

HEMP is composed of three components commonly re ferred to as E1, E2 and E3.

E1, often referred to as the prompt component, is charac terized by short pulse duration and a fast rise time. The actual EMP experienced is a function of the weapon yield and design, burst height, latitude of the burst, and relative observer location from the burst point.

E2 is often compared to lightning in terms of dura tion and frequency con tent (frequencies con tained in the signal), while E3 has the longest duration, lowest frequency content, and low est field levels.



As such, E1 poses the greatest danger to individual electronic systems, while E3 poses the greatest threat to networked infrastructure, such as long line power and telephone networks. The focus of the military is primarily on electronic system impacts due to E1.

With the collapse of the Soviet Union and no perceived threat, the military's investments in EMP assessment capabilities were significantly reduced.

CBRN Survivability Oversight

The late 20th century saw the emergence of tactical and strategic nuclear capabilities by developing nations whose political agendas and policies are diametrically opposed to the interests of the United States.

In September 2008, the DoD formally established a senior level Chemical, Biological, Radiological, Nuclear (CBRN) Survivability Oversight Group (CSOG) through the mechanism of the CBRN Survivability Policy, Department of Defense Instruction (DoDI) 3150.09.

The CSOG charter established its mission to ensure that equipment survivability in a nuclear weapons effects environment, including EMP, is addressed specifically by requirements during the acquisition process. Further, the CSOG was charged to establish the process for evaluating legacy system vulnerabilities deployed by the services and to prepare a yearly report to Congress about the progress toward achieving hardening of each service's mission critical systems.

The CBRN Survivability Policy: (1) defines a CBRN mission critical system; (2) calls for the establishment of processes to identify and review a mission critical system in the context of the Joint Capabilities Integration and Development System (JCIDS); (3) establishes processes for ensuring system survivability in a CBRN environment; and (4) identifies lines of responsibility for policy implementation.

EMP Program Mission

The new U.S. Navy EMP Program mission is multifaceted but ultimately comes down to providing senior Navy leadership the information to assess fleet posture with regard to EMP. Currently four core elements comprise the new program: testing and assessment, guidance, surveys and standards.

The U.S. Navy EMP Program supports the functions of the NAVSEA electromagnetic environmental effects (E3) technical warrant holder by providing guidance to Navy acquisition programs relative to military standards, requirements and design practices.

It is vital that the U.S. Navy EMP Program engage program managers early in the acquisition process to provide guidance and education about the effect these requirements have on their respective programs. The EMP Program is standing by to assist program managers with such tasks as developing and/or reviewing capability design documents and system specifications.

The Road Ahead

The road ahead for any new program is fraught with challenges. The most significant challenge for the new U.S. Navy EMP Program is cognizance. Due to the long absence of a robust EMP Program, few people in the U.S. Navy or across the greater DoD community have an intimate knowledge of EMP causes and effects. The prevailing thought appears to be that the probability of occurrence is low, so the issue is not important and can be easily dismissed.

However, the risk of failing to implement a mitigation strategy for EMP is at the highest level, and the consequences of failing to take precautions now can be catastrophic. CHIPS

Blaise Corbett has been with the Navy since 2002 and has been directly involved in the EMP assessment of naval systems since 2004. Corbett is currently the group leader for the Naval Surface Warfare Center Dahlgren Division EMP assessment group.

James Partak, an engineer originally from Naval Surface Warfare Center White Oak, has more than 39 years of experience in the area of nuclear effects to electronic systems. Now retired from the Navy, Jim supports the EMP assessment group through EG&G, a division of the URS Corp.

Applicable Policy

- DoDI 3150.09. Chemical, Biological, Radiological, and Nuclear (CBRN) Survivability Policy (Change 1). Aug. 17, 2009.
- MIL-STD-1310G. Standard Practice for Shipboard Bonding, Grounding, and Other Techniques for Electromagnetic Compatibility and Safety. June 28, 1996.
- MIL-PRF-24758A. Performance Specification – Conduit Systems, Flexible, Weatherproof. Sept. 24, 2004.
- OPNAVINST 3401.3A. Nuclear Survivability of Navy and Marine Corps Systems. Jan. 5, 1989.
- OPNAVINST 9070.1. Survivability Policy for Surface Ships of the U.S. Navy. Sept. 23, 1988.

Navy's New Strategy and Organization for Information Dominance

Information emerges as a core warfighting capability equivalent to seapower and airpower

By Jack N. Summe

We are experiencing a period of rapid change in the information realm; new technologies are emerging daily, obsolescence happens within weeks of fielding, global populations grow quickly accustomed to the impact of these new technologies, and our adversaries are using these technologies as a weapon against us.

The challenge is clear:

✓Information technology is driving dramatic change and leading to an explosion in the volume of information, thereby creating both opportunities and challenges.

✓The National Intelligence Council reported: "The growing importance of information technologies ... will make information itself a primary target in future conflicts."

✓The Defense Department detected 360 million attempts to penetrate its networks last year; \$100 million has been spent in the past six months repairing the damage.

✓Current and potential adversaries are applying information technologies and operations to counter our military strengths and preferred mode of warfare.

✓The U.S. military depends on assured access to the global commons — the oceans, space and cyberspace — to project influence and power.

✓Strategic competitors are investing in information capabilities to deny or offset that access.

✓The Navy's Cooperative Strategy for 21st Century Seapower is dependent upon unfettered access to and dominance of that emergent nexus between maritime, space and information domains.

Further, U.S. dominance in the information arena is clearly at risk. Both the president and Secretary of Defense have highlighted this concern.

On May 29, 2009, President Obama said, "Our technological advantage is a key to America's military dominance ...

But our defense and military networks are under constant attack ... it's now clear that this cyber threat is one of the most serious economic and national security challenges we face as a nation."

In January 2009, Defense Secretary Robert Gates said, "The U.S. cannot take its current dominance for granted and needs to invest in the programs, platforms and personnel that will ensure that dominance's persistence."

Recently, the Chief of Naval Operations postured the Navy to play a strategic role in addressing this challenge. There is a clear understanding across the Navy staff that we are at the threshold of a new era; an era where information must no longer serve as just an enabler, but transition to a core warfighting capability of the U.S. Navy. In fact, our service today has the unique opportunity to revolutionize its operational and warfighting capabilities, similar to when the Navy introduced dreadnoughts, aircraft carriers and nuclear power into the fleet.

Alignment to seize this opportunity began with a simple direction to the Di-

Combining the Office of the Director of Naval Intelligence (N2) and the Office of the Deputy Chief of Naval Operations (DCNO) for Communication Networks (N6), as well as other information-related elements from the N3 and N8 staffs, to achieve warfighting dominance and game-changing information capabilities, the new construct for the Deputy Chief of Naval Operations for Information Dominance N2/N6 emerged as an integrated organization as represented in Figure 1.



Figure 1.

rector of Naval Intelligence that culminated a period of consideration and reflection by the current Chief of Naval Operations (CNO), Adm. Gary Roughead.

On June 26, 2009, the CNO sent a memorandum to the Director of Naval Intelligence with guidance to undertake and lead the eventual reorganization of the OPNAV staff, combining the Office of the Director of Naval Intelligence (N2) and the Office of the Deputy Chief of Naval Operations (DCNO) for Communication Networks (N6), as well as other information-related elements from the N3 and N8 staffs.

The intent of this reorganization was simply stated: "The nature of our operations today demand a whole-warfighting approach to how we plan, resource and assess our operational and combat capabilities. The Office of the Chief of Naval Operations

this. We have to organize ourselves, we have to train ourselves, and we have to make sure that we're making the right investments so that we can remain the dominant information force, not just in the United States, but I would say globally."

After four months of detailed planning, coordination, execution and implementation, the OPNAV staff and the Navy have fully reorganized to meet the intent of the CNO as we move into an information-centric operating environment.

In this emerging environment, I simply define information dominance as having the right information at the right time and at the right place to enable leaders to use the right capability to quickly identify, counter or defeat the threat of the future.

Although the N2/N6 staff is working hard to develop and seek approval of definitions for "Information Dominance" and "Decision Superiority," in the implementing NAVADMIN 316/09

The Navy's Cooperative Strategy for 21st Century Seapower is dependent upon unfettered access to and dominance of that emergent nexus between maritime, space and information domains.

(OPNAV) must be organized to achieve the integration and innovation necessary for warfighting dominance across the full spectrum of operations at sea, under the sea, in the air, in the littorals, and in the cyberspace and information domains.

"You [N2] are the flag lead for the reorganization of the OPNAV staff ... This effort and corresponding process will meet a compressed timeline, execute a clear implementation plan, and be collaborative to work through the complex issues you will encounter."

This directive kicked off a compressed period of analysis and detailed planning that delivered a strategy for accomplishing the CNO's intent while executing an energetic reorganization of the OPNAV staff. The result portends significant implications for how Navy approaches the way it will organize to fight and help win our nation's future conflicts.

The CNO's directive was underscored in a follow-on joint memorandum from Vice Adm. David "Jack" Dorsett, N2, and Vice Adm. Harry Harris, then the N6, to the combined N2 and N6 staffs: "This is a historic opportunity to reshape the Navy for warfighting dominance in the information age."

The CNO amplified the significance of this reorganization during an October 2009 address delivered at the influential Center for Strategic and International Studies. There he discussed the significant moves within the Navy "to better man, train and equip the United States Navy for the fight that we're in and for the challenges that we're likely to face in the future."

In a September 2009 podcast to the Navy, the CNO also stated: "We're doing some things here in Washington on my staff that brings intelligence, command, control, communications, computers and information together in a way that [will enable us] to make better decisions ...

"And so by making these changes, by recognizing the importance that information plays in our lives, in our operations and in the success of the Navy's mission, now is the right time to do

message of Oct. 29, 2009, regarding the reorganization, the intent of the CNO was clear, and the significance of the reorganization was promulgated across the U.S. Navy: "The stand up of N2/N6 represents a landmark transition in the evolution of naval warfare, designed to elevate information as a main battery of our warfighting capabilities, and firmly establish the U.S. Navy's prominence in intelligence, cyberwarfare, and information management."

Toward this end, the strategic objectives of N2/N6, as defined in NAVADMIN 316/09, are to:

- ✓Elevate information to a core Navy warfighting capability.
- ✓Functionally integrate intelligence, information warfare, information/network management, oceanography, and geospatial information for information age operations.
- ✓Deliver assured command and control and information access to operational forces.
- ✓Boldly introduce game-changing concepts, strategies and capabilities.
- ✓Coordinate resource investment to deliver information-centric capabilities and competitive advantages.
- ✓Aggressively accelerate experimentation and innovation with information capabilities.
- ✓Deliver deep multi-intelligence penetration and understanding of potential adversaries, melded with deep multi-domain understanding of the operating environment.
- ✓Deliver remotely piloted, unattended and autonomous capabilities adaptively networked to extend reach, penetration and persistence in denied areas.

Effective Nov. 2, 2009, N2/N6 became the newest directorate within the OPNAV staff, and Vice Adm. Jack Dorsett was confirmed as the first DCNO for Information Dominance.

Although the implications of this reorganization are significant, other elements of the Navy were also reorganized to meet the vision of the CNO.



Figure 2.

✓The Navy established and stood up Fleet Cyber Command/U.S. 10th Fleet as the Navy's operational element for cyber and information-related activity and as the U.S. Navy Component Command to DoD's new sub-unified command, U.S. Cyber Command (USCYBERCOM). The establishment of FLT-CYBERCOM was effective Oct. 1, 2009, with a directive to be fully operational by Oct. 1, 2010.

✓Establishment of the Navy Information Dominance Corps (IDC) — simply defined as the combination of all the information-related specialties of the Navy under N2/N6 to better synchronize the training, knowledge and skills of these critical career fields.

✓The transition of Director, Navy Staff-Quadrennial Defense Review (DNS QDR) to Director, Naval Warfare Integration (N00X). In this construct N00X serves as a permanent directorate assigned to assess the alignment between Navy warfare strategy and investments, and to provide the CNO recommendations on how best to improve Navy's ability to deliver the capability, capacity and strategy needed to meet national and combatant commander needs.

✓Movement of the information-related elements of N3 (N39, information and cyber operations) and N8 (unmanned systems programs and resources) into the N2/N6 organization.

With regard to the reorganization of N2 and N6, one might assume that a reorganization of this scope and scale would simply take the easy road of establishing an Assistant DCNO (ADCNO) for Communications and an ADCNO for Intelligence, effectively maintaining the integrity and responsibilities of the previous staff directorates.

However, it was understood early on that to achieve warfighting dominance and game-changing information capabilities, the new construct had to effectively meld the two organizations into one. The planning team worked hard to develop an integrated organization as represented in Figure 1.

As can be seen, this is not a simple combining of two directorates under one senior flag officer.

Generally, the corporate side of the organization provides the manpower, intelligence and compliance structure for the operation of the entire organization, while the business side of the organization is effectively involved in creating the vision and strategic roadmap for information dominance while developing, integrating and managing the programs and future capabilities that will meet the mandate for the organization as set forth by the CNO.

Further, the reorganization has specific implications for all members of the newly formed Information Dominance Corps. As previously stated, the IDC is a management construct for those Navy military

The Information Dominance Corps (IDC) is a management construct for those Navy military and civilian specialties that work in information-related career fields. The vision of the IDC is to establish a focused corps integrated from across Navy's information-intensive fields — comprised of more than 44,000 Navy professionals.

and civilian specialties that work in information-related career fields.

The vision of the IDC is to establish a focused corps integrated from across Navy's information-intensive fields — comprised of more than 44,000 Navy professionals. Individual communities and specialties will maintain their unique history and culture, but a new structure, illustrated in Figure 2, ensures synergy and collaboration.

During the summer of 2009, the Secretary of Defense directed the commander of U.S. Strategic Command to stand up a new sub-unified command focused on the integration of defense cyberspace operations. In response to that guidance, the CNO directed the establishment of FLT-CYBERCOM/10th Fleet as the Naval Component Command for USCYBERCOM.

As such, FLT-CYBERCOM has the responsibility to:

- Serve as the central operational authority for networks, intelligence, cryptology/signals intelligence (SIGINT), information operations, cyber, electronic warfare, and space in support of forces afloat and ashore;

- Operate a secure, interoperable naval network; coordinate Navy's operational requirements for intelligence, information operations, networks, cryptology/SIGINT, and space capabilities; and,

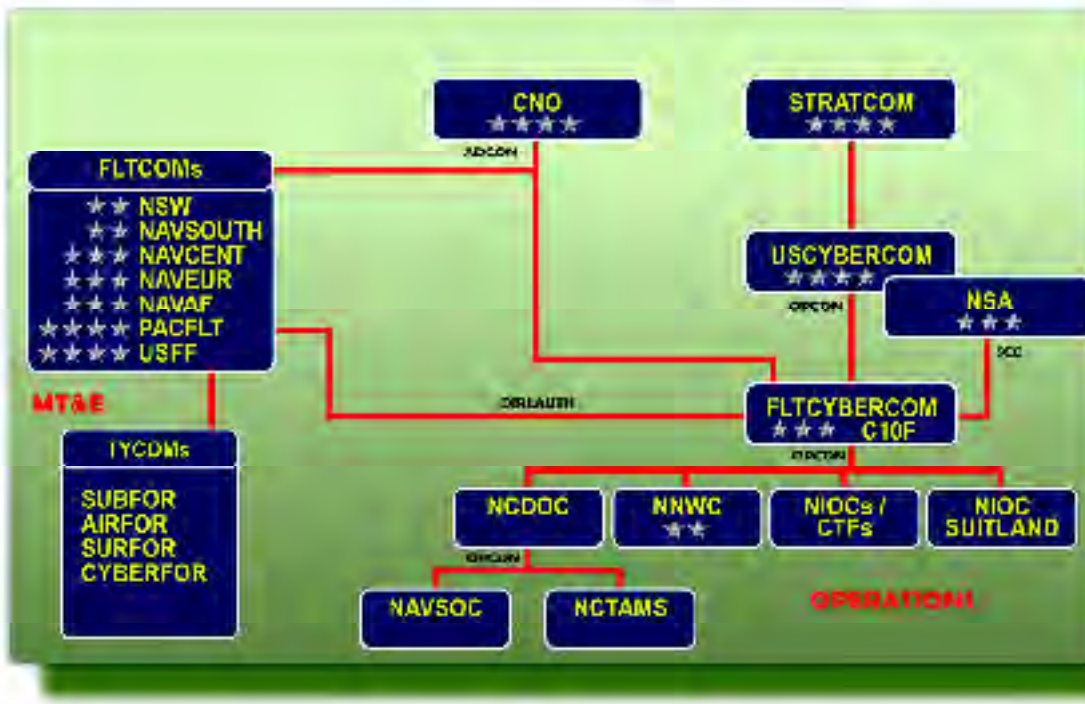


Figure 3.

Fleet Cyber Command/ U.S. 10th Fleet, the Navy Component Command for U.S. Cyber Command, is the central operational authority for networks, intelligence, cryptology/signals intelligence (SIGINT), information operations, cyber, electronic warfare, and space in support of forces afloat and ashore. The projected command and control relationships for FLTCYBERCOM/U.S. 10th Fleet are shown here.

The U.S. Navy is undertaking a significant transformation to better position itself for the future operating environment. The goal of the N2/N6 reorganization is to achieve unprecedented agility and innovation in development and integration of information capabilities, to achieve Information Dominance over our current and future adversaries, and to provide decision superiority for our commanders, operational forces and coalition partners, at the time and place necessary for success in any future environment.

- Provide operational support to Navy commanders worldwide in the areas of cyber, information and computer network operations, electronic warfare and space.

The projected command and control relationships for FLTCYBERCOM are indicated above in Figure 3.

Undoubtedly, the U.S. Navy is undertaking a significant transformation to better position itself for the future operating environment. The goal of this effort is to achieve unprecedented agility and innovation in development and integration of information capabilities, to achieve Information Dominance over our current and future adversaries, and to provide decision superiority for our commanders, operational forces and coalition partners, at the time and place necessary for success in any future environment.

Accordingly, the N2/N6 has established

some initial guiding principles as we begin this strategic endeavor. First principles include:

- Every platform is a sensor;
- Every sensor is networked;
- Every collector and sensor will be dynamically tasked and managed; and
- Every shooter must be capable of using target data derived from any sensor.

This is a very large undertaking, leveraging the knowledge and capabilities of a newly integrated and multidisciplinary staff. One month into the transition, it is already possible to foresee the impact of this new organization on the future of the Navy.

The energy and support dedicated to this effort presage significant changes for

the way the Navy organizes to fight and win future conflicts across all spectrums of engagement and warfare.

I feel confident that this new, groundbreaking reorganization of the Navy staff, combined with the establishment of FLTCYBERCOM/10th Fleet and the Information Dominance Corps, will serve as the best solution to leverage and manage new information technologies within a construct that provides strategic decision superiority to Navy commanders working to ensure the defense and security of our great nation. CHIPS

Jack N. Summe is a senior advisor for strategic engagement for OPNAV N2/N6 and a Defense Intelligence Senior Level (DISL) employee. DISLs are recognized leaders and authorities in a specialized field or functional area. For more information about the U.S. Navy, go to the Navy news site at www.navy.mil.

Getting from NMCI to NGEN

Early Transition Activities will ensure the seamless follow-on of the Next Generation Enterprise Network

By Capt. Tim Holland

The year 2010 marks the end and the beginning of an era in naval information technology. After 10 years of the Navy Marine Corps Intranet, the largest intranet in the world and the single largest defense IT program, the Department of the Navy has started its evolution toward the Next Generation Enterprise Network, the follow-on to NMCI. In fact, NGEN is preparing for the transition through a series of initiatives called Early Transition Activities. These ETAs are paving the way for the DON's vision of the Naval Networking Environment in 2016.

In 2009, the DON began to develop ETAs to prepare for a successful migration of services from a contractor-owned, contractor-operated model to one that gives the government increased command and control (C2). The ETAs are made up of several initiatives that will establish processes and tools used to lay the groundwork for a seamless transition between NMCI and NGEN. The ETAs will mitigate the risk for government and industry as the IT platform's operational model shifts to becoming government-owned.

The NGEN Program Office, or PMW 210, is part of the program portfolio of the Naval Program Executive Office for Enterprise Information Systems (PEO EIS). In August 2009, PEO EIS received approval for all ETA acquisition decisions and programmatic documents. PMW 210 is also authorized to manage the ETAs as risk reduction/risk mitigation efforts. As a result of this approval, the NGEN Program Office and PEO EIS regularly provide status updates on the ETAs to the Assistant Secretary of the Navy for Research, Development and Acquisition (ASN RDA), as well as conducting summits with NGEN stakeholders to keep them informed.

The ETAs are substantial in size and scope. Their scope encompasses people, processes and tool enhancements for the Navy and Marine Corps. Descriptions of the funded ETAs as of press time follow.

ITSM Process Development

To achieve operational control across a large IT enterprise comprised of multiple service providers, the government



Early Transition Activities will prepare the network for a successful migration of services from NMCI through the Continuity of Services Contract (CoSC) period to the implementation of NGEN.

must enhance insights in IT Service Management. ITSM is a discipline for managing information technology systems centered on the customer's perspective. NGEN will leverage the Information Technology Infrastructure Library (ITIL V3), a framework of industry best practices for ITSM. Some inherent benefits for organizations that have chosen to adopt ITIL for service management include lower costs and improved services.

To develop the ITIL competency, the NGEN Program Office, in conjunction with Naval Network Warfare Command (NETWARCOM), will use a phased approach to deploy customized and integrated ITSM processes based on the ITIL V3 framework. The NGEN Program Office and NETWARCOM have begun the initial process development work for knowledge management; service asset and configuration management; information security management; incident management; event management; and portfolio management.

The NGEN Program Office will lead NGEN stakeholders through process design efforts to cultivate standardized processes, procedures, roles, performance management plans and tools to support future NGEN services.

This ETA will also develop standardized service management procedures that will ensure government oversight, IT conformance, standardization and integration of ITSM processes across all segments of the NGEN environment. To effectively

manage the network, the ETA will lay the groundwork for the creation of training specifications for NGEN and contractor network management resources.

Enterprise Tools Strategy

Like the ITSM Process ETA, the Enterprise Tools ETA is part of the proposed NGEN ITSM/ITIL framework and is responsible for the strategy and implementation/integration of technical solutions. Since NGEN is moving toward a consolidated management environment to reduce costs and increase the level of services it provides to customers, ITSM tools for automation, monitoring and management are a mandatory piece to the enterprise puzzle.

This ETA will analyze current tools, perform industry research, develop design requirements and interfaces, and recommend vendor tool integration specifications deemed by the government as necessary to support and enforce enterprise standards for its ITSM processes. This ETA will reduce NGEN tool acquisition risk by analyzing government and commercial off-the-shelf tools, and recommend tools that tightly integrate all ITSM processes, while simultaneously reducing customized tools and overall costs.

The Enterprise Tools ETA strategy is also expected to increase the efficiency of ITSM processes and facilitate collaboration among multiple stakeholders. By integrating state-of-the-art processes and standard workflow tasks, NGEN will also

standardize enterprise management activities. Ultimately, the successful transition from NMCI to NGEN will incorporate ITIL V3 training for personnel as a necessary part of the implementation process. Support will be furnished by qualified ITIL V3 staff.

Global NetOps C2 Workforce Establishment

Achieving NetOps effects in the NGEN environment implies an ability to conduct seamless, synchronized and integrated visibility, management, and command and control of assets and/or resources within NGEN management domains. The focus of this ETA is to provide capability to achieve the NetOps essential tasks and their desired effects in relation to shared situational awareness, unified C2, network assurance, enterprise management, content management, assured system and network availability, assured information delivery and assured information protection. To achieve these effects, the NetOps ETA will develop the personnel, processes and tools to support NGEN NetOps requirements and capabilities, including:

- Visibility into the health and status of NGEN operations and alignment of operational and contractual authorities;
- Alignment of resources with military organizations and missions;
- Focus on network defense activities;
- Support the full range of continuity of operations activities;
- Ability to associate performance issues with a specific NGEN segment; and
- Development of tool requirements and processes to exercise C2 over NGEN resources.

Comprehensive Facilities Inventory

To properly inform the NGEN request for information/request for proposal (RFI/RFP) activities, the DON will create a comprehensive asset database of NMCI's core infrastructure. The Comprehensive Facilities Inventory ETA will capture the information necessary to establish an Enterprise Infrastructure Asset baseline of the current NMCI infrastructure. This will facilitate transition from the vendor-controlled environment to the government-controlled NGEN environment. To establish this baseline, the government will assess the current state of asset configuration information and develop a strategy for collecting and analyzing the data.

CTR Workforce Reconstitution

Currently, DON contract technical representatives (CTR) perform service-related functions, such as ordering, invoicing and contract execution for users on the NMCI contract, as a collateral duty. The CTR Workforce Reconstitution ETA will perform the work analysis and manpower development documentation needed to align the CTR workforce with NGEN acquisition and mission strategies. The ETA will define NGEN CTR roles and responsibilities, as well as training requirements, to meet NGEN performance expectations. By leveraging a unified and coordinated approach to a reconstituted CTR workforce, the DON will improve its ability to realize reduced costs through blended training, as well as ensure a seamless CTR transition from NMCI to NGEN.

DISN Core Extension

This ETA will bring wide area network (WAN) connectivity from the Defense Information Systems Network (DISN) to five

major DON nodes in the Atlantic and Pacific areas of responsibility. One of the issues with the current DISN subscription service structure is that it does not provide enough sites with sufficient bandwidth. Enhanced connectivity provided by this ETA will improve performance and maximize bandwidth usage by utilizing a higher maximum transition unit and through rate shaping, or filtered bandwidth. This should resolve DISN subscription services issues with the Defense Information Systems Agency (DISA), the Department of Defense's primary communications system.

By achieving efficiencies in the DISN's subscription services and minimizing NGEN's circuit costs, the ETA will improve quality of service for warfighters and reduce costs for the DON.

Marine Corps Upgrade WAN and Enterprise Services

The Wide Area Network and Enterprise Services ETA consists of various IT assets that will directly replace and refresh existing Marine Corps Enterprise Network (MCEN) infrastructure items for approximately 30,000 users.

Marine Corps Installation East Pilot

The Marine Corps Installation East Pilot will be conducted at Headquarters Marine Corps Installations East, Marine Corps Base Camp Lejeune, N.C. Transition activities will include assumption of operational control of the base area network, local area network, migration of end-users to Marine Corps Worldwide Active Directory, various management and sustainment processes, and transition of user workstations for approximately 1,200 users. This ETA will serve as the model for the entire Marine Corps NGEN transition strategy.

How We Get There

Each ETA has its own program life cycle and is managed within an integrated product team (IPT) in the NGEN Program Office. Some of the ETAs, such as the Comprehensive Facilities Inventory, are nearing completion in their life cycles whereas other ETAs, such as the ITSM/ITIL Processes and Tools, will continue until NGEN reaches its full operating capability.

PMW 210 continues to meet with stakeholders as it staffs and executes the ETAs in coordination with PEO EIS and ASN RDA oversight. The NGEN Program Office is also reviewing ETA deliverables with the IPTs responsible for each activity and aligning activities with the services that will be provided under the new NGEN operating model.

This is truly an exciting time to be a part of naval IT. As we transition from a model that made great strides in unifying our department under one IT platform, we continue the work that was begun 10 years ago in maximizing efficiencies and reducing legacy systems. As one of the program offices of PEO EIS, NGEN embraces its motto, "Enabling the Enterprise."

I am very proud of the work being conducted by the IPTs and the early progress made by the ETAs to successfully transition to NGEN and to achieve the DON's vision for the Naval Networking Environment ~ 2016. **CHIPS**

Capt. Timothy Holland is the PMW 210 program manager. He is a graduate of the U. S. Naval Academy with a bachelor's degree in engineering and a Master of Science degree from the Naval Postgraduate School.

U.S. Joint Forces Command Provides Global Force Management

Increased troop levels means better security for the Afghan people and an extraordinary logistics campaign for U.S. troop deployment

By Sharon Anderson

On Dec. 1, 2009, President Obama directed an additional surge of 30,000 troops to southern and eastern Afghanistan to reverse the negative security trends in these areas. The first of the troops are expected to arrive within days of the president's announcement and most of the remainder by mid-summer.

U.S. Joint Forces Command, in its primary force provider role, is helping combatant and operational commanders plan and synchronize the deployment of forces to carry out the president's strategy.

Air Force Brig. Gen. Robert Yates, director for Operations, Plans, Logistics and Engineering (J3/4) for USJFCOM, spoke about USJFCOM's role in the Global Force Management (GFM) process, the approach used to deploy the troops and supporting elements to Afghanistan, in mid-December.

"We are getting final details on some of the requirements; we know most of them," Yates said.

Once a combatant commander's request is validated by the Joint Staff, it is forwarded to master planners in the Joint Deployment Center which opened in October 2009. The JDC staff has significantly assisted in analyzing and recommending which forces will best fill commanders' needs, according to Yates.

Although, it may appear to look like the typical office filled with computers and desks, the JDC is ergonomically engineered to facilitate collaboration. Instead of cubicles and halls with closed doors, the center is an open space with state-of-the-art communications. Teams can be quickly formed or clustered to tackle a specific requirement.

The JDC staff is about 275 strong with representation from all the services which makes planning much easier, said Yates. The JDC staff is comprised of active duty and Reserve service members representing all four services, DoD civilians, many of whom are retired military members, and contract personnel. The force sourcing effort, however, goes far beyond the JDC staff.

The force sourcing effort is led by JFCOM personnel from the JDC, but involves other JFCOM directorates, JFCOM service components from the Army, Navy, Air Force and Marine Corps, and each of the services at the leadership level.

The force sourcing institution is organized into Joint Working Groups (JWGs) arranged by subspecialty and spread through the command, components and services accordingly. For instance, sourcing of medical requirements is primarily handled through personnel from the JFCOM Surgeon's Office (J02M) who liaise with service medical providers. Communications requirements are sourced with the assistance of JFCOM's Command, Control, Communications and Computer Directorate, commonly known as the J6, and JFCOM's Intelligence Directorate (J2) helps to facilitate the sourcing of intelligence requirements.

The core of expertise resides in the JDC, but the actual sourcing effort includes hundreds, if not thousands, of experts nationwide.

"If we are discussing the requirement for an engineering unit or a Marine battalion, we don't have to call outside this room,

the representatives for the services are right here and can tell us what is available," Yates said.

The JDC serves as a command center for both the Navy and Joint Forces Command separated by a movable wall that can be easily removed for joint planning. For example, in a domestic crisis, commanders can quickly regroup to get the information they need regarding the status of forces and how they can be deployed to respond to the emergency.

Yates compared his staff's current challenge to the one it faced in the 2007 surge of troops to Iraq. He said that challenge was one of J3/4's biggest successes as a joint force provider. While there are lessons learned to apply in the current surge, there are big differences in the requirements.

"They're unique situations with unique requirements," Yates said. "The type of force that we use for an Afghanistan counter-insurgency and training effort is going to be a little bit different than what was needed for the Iraqi surge. Each theater is unique in terms of force requirements, strategy, terrain, logistics and security."

Included in the deploying force structure are about 4,100 support personnel in the areas of logistics, engineering, operational planners, and specialized providers, for example, explosive ordnance disposal (EOD) and security teams.

Just over half of the forces have been identified and informed of their upcoming deployments, according to Yates. The responsibility for coordinating the rotations falls to USJFCOM.

Defense Department officials announced in early December that 1,500 Marines from Camp Lejeune, N.C., will deploy later in the month, and 6,200 Marines of Regimental Combat Team 2 at Camp Lejeune were alerted for deployment early in the spring.

The 1st Marine Expeditionary Force at Camp Pendleton, Calif., also will deploy 800 Marines in the spring, along with an influx of 3,400 soldiers from the 1st Brigade Combat Team from the Army's 10th Mountain Division at Fort Drum, N.Y., department officials said.

USJFCOM's goal is to anticipate requirements and have the necessary personnel identified and accounted for 18 months in advance of commanders' needs, but officials often must adapt quickly to changing demands on the ground.

The general explained the process for how combatant commanders request troops or resources to fulfill mission requirements.

"Because Afghanistan is in the U.S. Central Command area of responsibility, I'll use CENTCOM as an example. When Gen. [Stanley] McChrystal (commander of the International Security Assistance Force in Afghanistan) sends a request for troops, his requirement goes to Gen. [David] Petraeus, CENTCOM commander, then to the Chairman of the Joint Chiefs of Staff for validation. JFCOM's role is to analyze the requirement and provide courses of action in the form of recommendations for the Joint Staff," Yates said.

Sometimes combatant commanders get exactly what they request, other times the forces they want are not available, and JFCOM can craft a solution that will provide the same effect.

“If a requirement comes in for an Army or Marine battalion, we ask the services what is available including National Guard units. If there isn’t one available, we can work with the COCOM to try to further refine the requirement, maybe a security force would answer the requirement, and we can provide that,” Yates said.

Unit requirements are filled in one of four ways. The primary sourcing method is through a “standard” sourcing solution, meaning it most closely answers the request of the combatant commander. For example, if the request is for engineering capabilities to support an Army Brigade Combat Team, the standard solution would be an Army Engineering Battalion.

Should a standard solution be unavailable, JFCOM next looks to a “joint” solution whereby a unit from another service that possesses the same core capabilities is used to satisfy the request. In the example above, an Air Force RED HORSE engineering unit or a Navy Seabee battalion could be used as a joint solution.

If no standard or joint solution is available, but the request can be filled by retraining a unit to another core capability, an “in-lieu-of” (ILO) sourcing solution can be used. For example, if the request is for a transportation unit that moves cargo in trucks, a field artillery unit can be trained for the mission and temporarily assigned to it. ILO solutions normally keep units intact while performing a mission outside their core capability.

Some requests cannot be satisfied through standard, joint or ILO solutions. This typically happens when a capability is

requested by a combatant commander, but not held in the inventory. In this case, JFCOM may assemble an ad hoc unit by gathering personnel with the requisite skills and forming a new, temporary unit. These personnel can, and do, come from all the services based on skill set and are assembled into a temporary unit complete with an appropriate command structure. Any necessary training is accomplished to ensure the new unit is fully capable of accomplishing the mission without undue risk.

The efforts in Iraq and Afghanistan might appear to heavily depend on Army and Marine Corps ground forces, and they are, but there are significant contributions from the Navy and Air Force as well, Yates said.

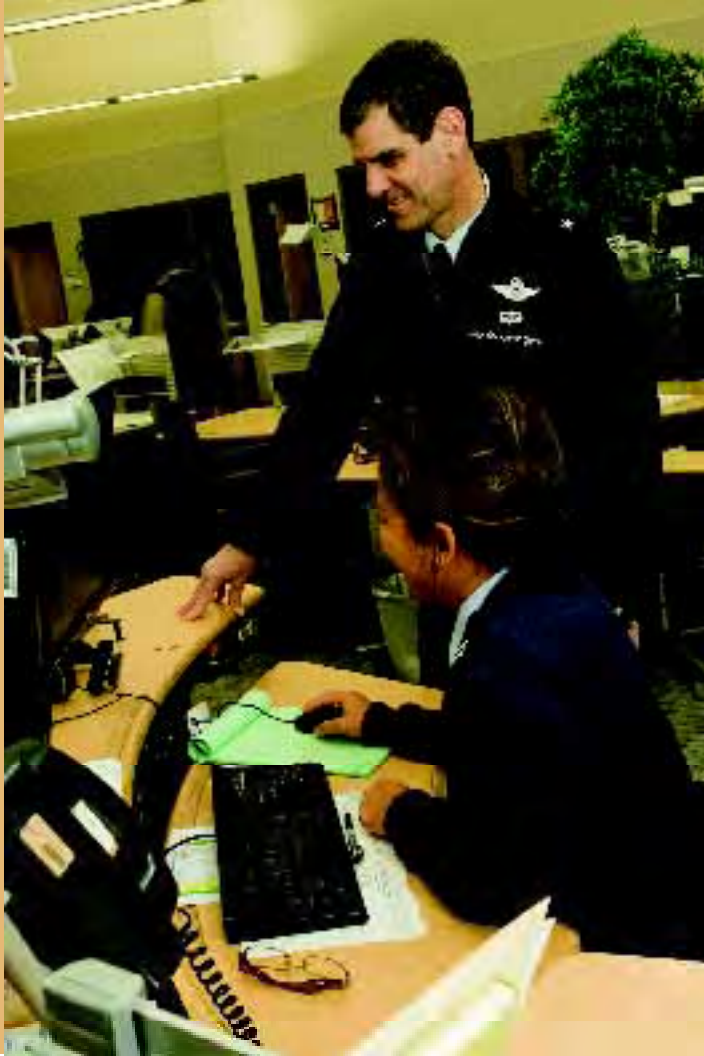
There is substantial air capability from bases inside Iraq and Afghanistan, as well as from aircraft carriers afloat in neighboring seas. All four services contribute in skill sets such as intelligence, EOD, military police and engineering. Air Force and Navy medical personnel and units provide medical evacuation capability, as well as trauma care on the ground. Air Force RED HORSE units and Navy Seabee battalions perform a myriad of construction tasks from building roads, to digging wells, to raising buildings.

Logistics teams from every service maintain the flow of food, water, consumables and fuel to units widely dispersed throughout the theater. Intelligence specialists are in high demand, and every service provides these valuable personnel to units and staffs on the ground. Operations Iraqi Freedom and Enduring Freedom are very much team efforts requiring significant contributions from every branch of the U.S. military.

While Marine Corps and Army units typically deploy with a

U.S. Joint Forces Command Joint Deployment Center, which opened in October 2009, is ergonomically engineered to facilitate collaboration. Instead of cubicles and halls with closed doors, the center is an open space with advanced communications. In an emergency, teams can be quickly formed to tackle a specific requirement. The facility covers 49,000 square feet and has a state-of-the-art data, communications and audio-visual collaborative network supported by more than 110 miles of cable. A centralized server and secured hard drives eliminate the need for desktop personal computers, optimizing work space and network security. The JDC contains a conference center, operational areas and a crisis response center.





Air Force Brig. Gen. Robert Yates, director for Operations, Plans, Logistics and Engineering (J3/4) for USJFCOM, and Air Force Capt. Mei ling Taylor, Joint Force Provider Orders Writer in USJFCOM's Joint Deployment Center. The JDC, located on the Norfolk Naval Base, plays a pivotal role in the Global Force Management process, the method used to respond to combatant commander requirements.

Below, Army Col. Eric Weidemann, former J3/4 Chief of Staff. He is prepping for a tour in Afghanistan.

Photos by Air Force Staff Sgt. Vanessa M. Valentine, U.S. Joint Forces Command photographer.



supporting infrastructure for communications and operations, and with provisions for food and shelter, it is reasonable to anticipate that much of the deploying supporting element will tackle the logistical challenges of providing for the additional troops, according to Yates.

"We take it day-by-day. In a typical day, there is activity at every level of the enterprise. While sourcing is a serial process, following a sequence of combatant commander requests, Chairman validation, Joint Force Provider sourcing, Joint Staff recommendation, and Secretary of Defense approval, these functions operate in parallel at any given time. On a normal day in the JDC validated requests are being received, others are being parsed out to the JWG leads for potential solutions, others are being pitched to the Joint Staff, and still others are being presented to SecDef for approval.

"There is a great deal of liaison work throughout the process. JDC action officers (AO) often discuss the specific details of validated requirements with their counterparts from the geographic combatant commanders. They also negotiate with their JFCOM service component counterparts over potential solutions. Issues that can not be resolved at the AO level are presented during general and flag officer (GO/FO) secure video teleconferences in an effort to reconcile solutions when requirements outnumber capabilities," Yates said.

While there is no one priority at the top of his list, Yates said that his staff understands the enormity of their task to get Gen. McChrystal the flexibility he needs to put troops where needed. Many of the 30,000 U.S. forces will be employed to combat the

Taliban, while others will assist NATO troops in training new Afghan soldiers and police.

The 2010 goal for trained and equipped Afghan soldiers is 134,000 and about 110,000 for the Afghan police, said Joint Staff Chairman Adm. Mike Mullen at a Pentagon news conference Dec. 10, 2009.

Afghanistan's international partners showed their enduring commitment by pledging about 7,000 additional troops. Some 43 nations will contribute to a security effort that will be nearly 150,000 strong — at the invitation of the Afghans — and with the sanction of the United Nations, reported the Defense Department.

"The ability to contribute to the uplift of U.S. forces to Afghanistan as ordered by the president is a great honor. While most of us here would prefer to be among those deployed and contributing daily to the coalition effort in Afghanistan, we understand the importance of doing our job well to the ultimate achievement of success," Yates said.

"We know the new strategy and increased force levels will result in achievement of our national objectives in Afghanistan; because of this our contribution to that success as force providers is very rewarding and a point of pride for the men and women of the Joint Forces Command J3/4 involved in the sourcing effort." CHIPS

Sharon Anderson is the CHIPS senior editor. For more information about the Joint Deployment Center, go to www.jfcom.mil.

RADIO 2050

by Tom Kidd

It can be embarrassing to attempt to predict technology beyond its current development horizon. This is especially challenging when the technology has begun to accelerate exponentially. To predict the future of radio into the second half of the 21st century, we will need to look back at its development from a 19th century oddity, to a 20th century necessity, and into the early years of the 21st century.

The expansion of Maxwell's electromagnetic theory of light by Heinrich Hertz in 1886 starts our timeline.

Radio's first 50 years saw the technology move out of the laboratory and into society. By the mid-1930s, radio, television and radar had become the cutting-edge technology of the day. However, another technology was also in development that would not only eclipse radio as the icon of the future, but would forever change the way radio technology is employed in society. This development, the computer, changed the fundamental building blocks of radio hardware. And it is that marriage of computer to radio that is having the greatest impact on radio's second century.

It has been said of technology that "form follows function." But when the function is formless an interesting opportunity for integration occurs.

In the later years of the 20th century, the function of producing radio waves moved out of the physical dimension of tubes and transistors to become a function of software and microchips.

Today's wireless technology is a chipset capability and no longer a proprietary device. While we will always have legacy technology, somewhere someone is still making buggy whips, the future of radio is to disappear into an integrated interconnected fabric of the world around us.

Within the next decade, radio technology will enable the wireless exchange of information among systems ranging from household appliances to automobiles. The per unit cost of wireless nodes will continue to drop while their capabilities will continue to increase. Lower cost devices will lead to their integration in diverse and unexpected ways.

As we head into the middle of the 21st century we won't be surprised to find that more of our devices are interconnected than are not. Taking a studied look around the

typical office or home, we find countless items that will interact with each other in much the same way that we interact with them today.

Where today, a human looks for wear and tear in home or office equipment; in 2050, a device will not only know its level of wear but will communicate with other affected items to manage its deficiencies.

Perhaps our transportation systems will communicate with other systems or devices to optimize our experiences or minimize their impact on our environment.

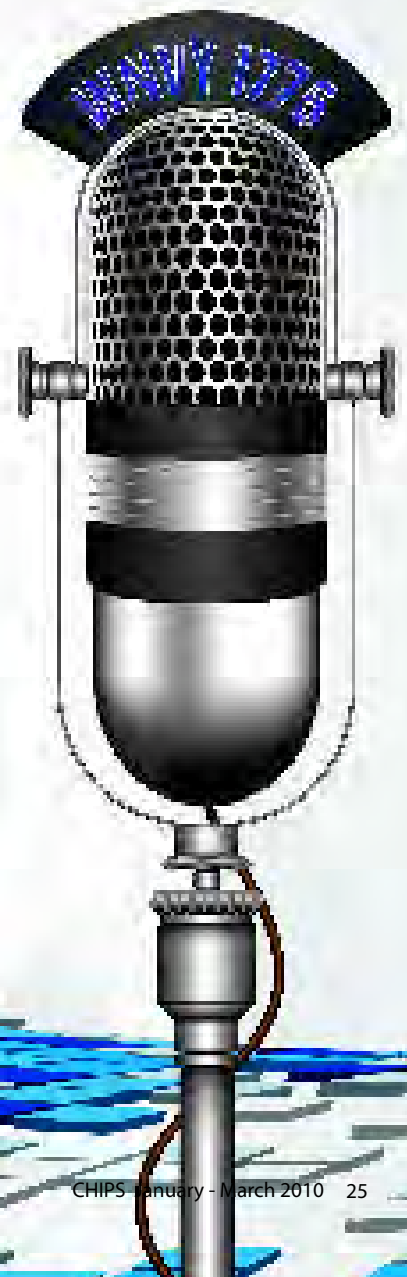
And the knowledge we collect may interact with the collective knowledge of our friends, family, co-workers, and their devices to anticipate capabilities we may not know we need until they are presented for our use.

While total interconnectivity throughout our environment is unlikely, the ratio of interconnection to disconnection will be much higher than it is today. All this interconnection will be done wirelessly. Physical connections will be seen as cumbersome and antiquated.

But the radio, as a unique device, will have all but disappeared into the products themselves.

By January 2050, the typical consumer will assume a device is capable of wireless interconnectivity and will be surprised when it isn't. CHIPS

Tom Kidd is the director of strategic spectrum policy for the Department of the Navy.



Advances in Magnetometer Technology

U.S. Marines will no longer have to worry about what is hidden behind the next rock – they will know

By Tom LaPuzza

A six-year collaboration by Space and Naval Warfare Systems Center Pacific (SSC Pacific) scientists and engineers, with colleagues in Sweden and Sicily, has put new force protection technology into the hands of U.S. Marines, who will be taking it to the battlefield sometime this year.

Drs. Adi Bulsara and Visarath In, serving as principal investigators, and several other SSC Pacific personnel, have been working with physicists and engineers from the University of Catania in Italy and the Swedish Defense Research Agency (FOI) in Stockholm, to harness the substantial potential of nonlinear dynamics for military and civilian applications.

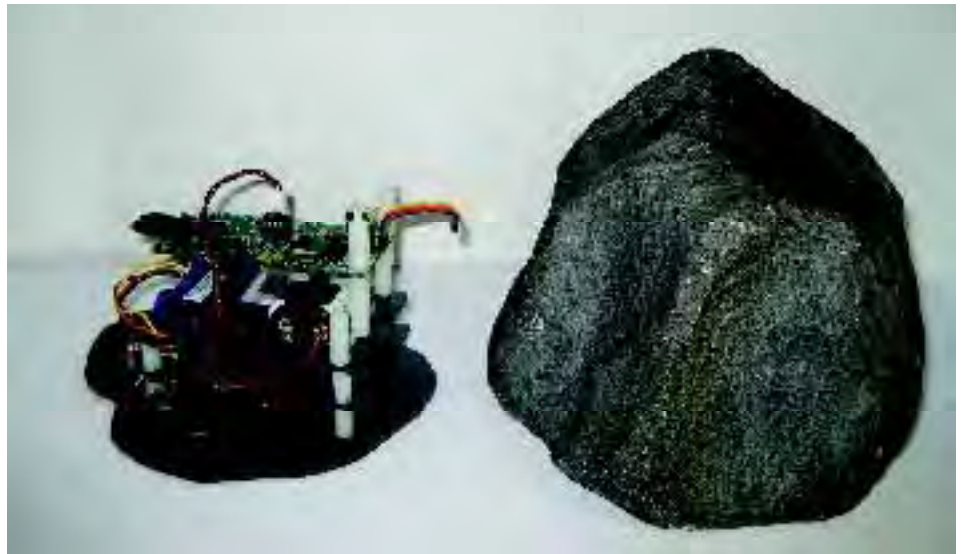
These applications include battlefield sensors disguised as rocks that can communicate with each other and pass vital information to military planners via satellite links. Similar sensors can be placed on the seafloor and detect swimmers and divers passing in the water column a few meters away.

An add-on to the U.S. Marines' Tactical Remote Sensor System (TRSS) will allow a reconnaissance patrol to image armed individuals even through a wall, and can also be deployed in remote areas as an unattended ground sensor for persistent surveillance. Other sensors, the size of clothing buttons, can also be distributed randomly around a building to alert security personnel to the presence of intruders.

Technology Development

The basic idea of using the principles of nonlinear dynamics in developing a magnetometer with a simpler readout based on the idea of spike timing, which underpins the neural code, came during a 2003 discussion between Dr. Bulsara, his colleagues in Stockholm, and professor Luca Gammaitoni of the University di Perugia in Italy.

"We were chatting and jotting some thoughts on a chalkboard, when it hit us that the physics would allow us to develop a magnetometer that could sense minute changes in a magnetic field caused by



The magnetometer to be placed on the U.S. Marines' Tactical Remote Sensor System and the "rock" under which it would be hidden to gather information without being noticeable to those passing by.

objects made of ferrous metal, leading to a wide range of applications," Dr. Bulsara said.

"Of course, the basic fluxgate magnetometer had been around since World War II; however, the idea of modifying the readout to mimic the process whereby neurons are believed to code and process information in the nervous system was different. We realized quite rapidly that if certain physics constraints were met, then the idea afforded simplicity and elegance which are always desirable in new concepts. We persuaded FOI to do a quick experiment to test the idea (it worked), and [we] wrote a long article about it in *Physical Review A* in 2003," Dr. Bulsara said.

"Over the next six years, we rigorously proved the physics and began developing various pieces of hardware. It's a reflection on the dynamics of the group that one of the products of that early discussion and subsequent development, the single core magnetometer, is ready to go into the field within only six years from the initial ideas as an additional sensor of the TRSS that gives the Marines some remarkable capabilities, including the ability to 'see' moving ferrous material (e.g., rifles) through walls."

After Visarath In and Joe Neff arrived at

the lab, research accelerated and theoretical work aimed at better understanding the physics of coupled nonlinear oscillators rapidly evolved into the "coupled-core magnetometer" which involves coupling an odd number of wound ferromagnetic cores cyclically to one another in a ring oscillator configuration. A magnetometer based on the unique physics of this configuration is far more sensitive than the single core magnetometer.

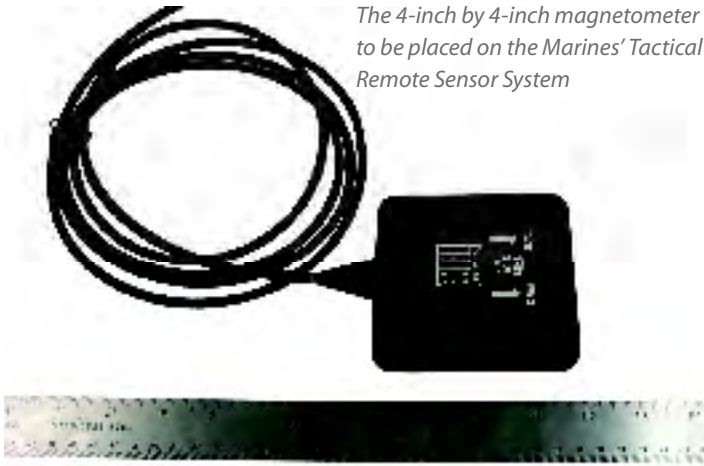
The coupled-core magnetometer is being refined, with a number of practical issues remaining to be addressed. However, it will likely render the single core magnetometer obsolete in a couple of years. The SSC Pacific group and their international collaborators are exploring other sensors and devices that employ the unique features of the coupled oscillator configuration.

TRSS

TRSS, developed mostly by other organizations, is a handheld device weighing only a few pounds, but it carries acoustic, infrared, seismic and magnetic sensors.

The SSC Pacific contribution is a magnetometer about 4 inches by 4 inches (shown on the next page) that will replace

The 4-inch by 4-inch magnetometer to be placed on the Marines' Tactical Remote Sensor System



the magnetic sensor with a much more powerful one. It can detect extremely small changes in the ambient magnetic field, such that through a plaster and wood wall a handgun can be detected at a range of approximately 8 meters.

The technology requires that the object be moving. If a handgun were to be taken off a table, or an individual walked out of a room carrying a weapon, the device would detect it. Similar technology has been developed for placing magnetometers in objects that look like rocks. They could be placed, for example, in plain sight at a sentry location through which pedestrians pass. A Marine with a personal digital assistant could be positioned some distance away monitoring those passing through. An individual passing by with hidden ferrous metal objects (weapons) could be stopped for interrogation and search.

Similarly, a network of such magnetometers disguised as rocks could be placed strategically along paths through mountain passes to alert security forces to the passing of heavily armed individuals.

"We could send a Tomahawk (missile) through a mountain pass dropping sensors at predetermined time separations," Dr. Bulsara said. "They are designed always to land right-side up."

The sensors can, if necessary, carry GPS receivers to provide critical position data, and radio frequency communications to "talk" to other sensors in the area or to transmit collected information to a satellite. In another application, a "rock" containing a magnetometer could be programmed to transmit a command to a nearby camera to shoot still photos or videos of a passing individual armed with ferrous metal, thus providing security personnel with images of subjects of interest.

Critical to the successful operation of the technology was the realization that rather than using changes in power, a time-domain description that underpins the neural code could be used.

"We're talking at a basic level about the firing of neurons, wherein a membrane voltage crosses a threshold and generates a spike, which means a neuron has fired," Dr. Bulsara said. "As an example, if we're monitoring an individual and someone sticks him with a pin, then the sensory neurons fire more rapidly leading to a change in the statistics of the interspike intervals. Changes in measurable quantities like the mean firing rate can be correlated with the stimulus that led to these changes. The so-called neural code is widely believed to be based on the timing between spikes."

"Sensors based on this operating principle require simplified readout circuitry: a clock and a counter for keeping a running arithmetic mean of the interspike intervals suffice." (In this case, the intervals between the crossings of the upper and lower core magnetization thresholds by the internal magnetization parameter.)

This allowed the group to eliminate time-honored signal processing techniques, such as Fast Fourier Transforms (FFT), and merely calculate time differences so the readout became event-based. The standard time unit employed is one-tenth of a second.

The core of the current single core magnetometer is an exotic material about as thick as a human hair, with very favorable magnetic properties. The hardware is hand assembled on-site at SSC Pacific at a cost of about \$400 per unit, compared to a price tag of \$6,000 or so for commercially available magnetometers that are used in geophysics or other military surveillance applications.

"Make it small, make it light, make it cheap"

The refinement of the technology required removing original designs from shielding against the Earth's magnetic core and then determining sources of interference, reducing false alarms and optimizing the thresholds to ensure the signal wasn't missed by being buried in noise. Then there was the need to make it small, make it light, make it cheap.

In a planned competition among eight magnetometers, the SSC Pacific model was first in all categories except maintenance, since the developers' basic approach was: "It costs \$100, if it breaks, throw it away, and we'll send you a new one."

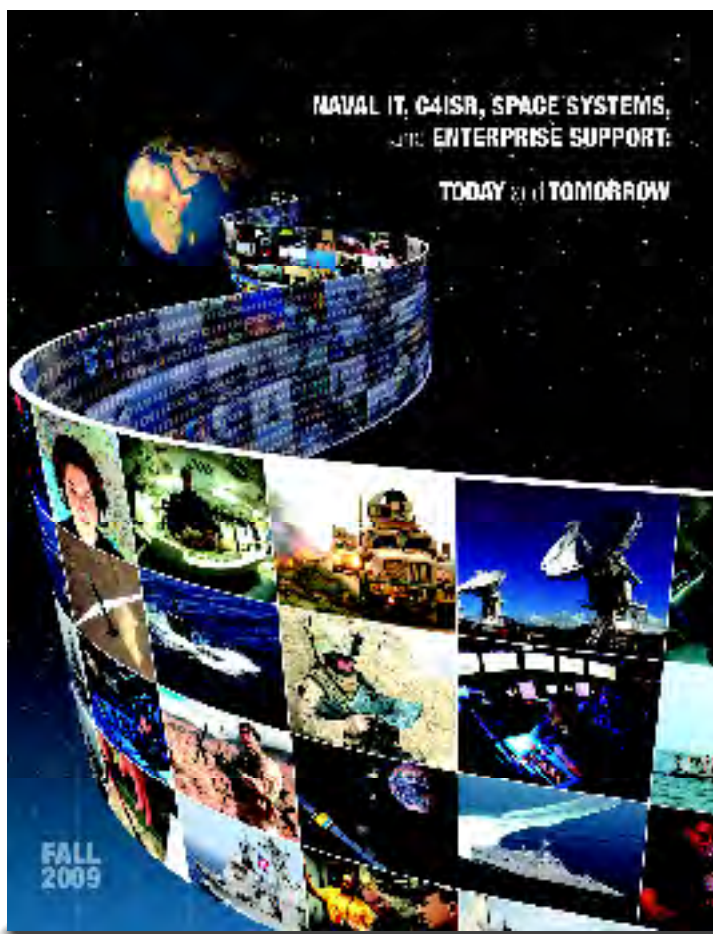
With the competition settled, the SSC Pacific group was funded by the Office of Naval Research for three years to build hardware for the Marines to put into the field.

Planned improvements underway include completion of the coupled-core magnetometer and development of ultra-low power electronics, since its power requirements are significant.

"We have demonstrated the coupled-core magnetometer successfully in a sea test," Dr. Bulsara said. "Once we get the power requirement to a manageable level, our current single core model could be obsolete. In the meantime, the single core magnetometer has a measured in-the-field (i.e., unshielded) resolution of 0.5 to 1nT (nano tesla – unit of magnetic flux density), making it possibly the best room-temperature magnetometer available today."

SSC Pacific personnel involved in the effort are Drs. Joe Neff, Brian Meadows and Visarath In; and Andy Kho, Chris Obra and Greg Anderson. Their collaborators are professors Bruno Ando and Salvatore Baglio of the University of Catania, Italy; Drs. John Robinson, Peter Krylstedt, Peter Sigray and Bjorn Lundqvist of the Swedish Defense Research Agency in Stockholm; and Dr. Antonio Palacios of San Diego State University. CHIPS

Tom LaPuzza is with the public affairs office of SSC Pacific. For more information about SSC Pacific, go to the SPAWAR Web site at www.spawar.navy.mil.



SPAWAR Releases Naval IT, C4ISR, Space Systems, and Enterprise Support: Today and Tomorrow

New technical vision for the C4ISR, Business IT and Space Community

The Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR), Business Information Technology (IT) and Space Community published their first technical vision that articulates their product line and future plan as a community

Collaboration is Key

The technical vision, "Naval IT, C4ISR, Space Systems, and Enterprise Support: Today and Tomorrow," is sponsored by Space and Naval Warfare Systems (SPAWAR) Commander Rear Adm. Michael Bachmann, in collaboration with resource sponsors in the Office of the Chief of Naval Operations, and with contributions from the U.S. Marine Corps Staffs, Naval Network Warfare Command (NETWARCOM), and others.

The new technical vision highlights the information-centric contributions of naval C4ISR, business IT and Space Community professionals, and it articulates how C4I products and services employed in-theater are currently playing major roles in warfighter successes. The document is available on the SPAWAR public Web site at www.spawar.navy.mil.

Dynamic examples from the current fight in Iraq and Afghanistan demonstrate the successful integration of intelligence and operations with the power of using the network to get information to the right person, at the right time, to add value to situational awareness and achieve warfighter success.

Aligned with higher-level guidance and policy, the technical vision communicates complex concepts, technologies and visionary strategies that depict examples of programs planned within the Program Objective Memorandum (POM) cycle — major investments for tomorrow that will enhance future capability, cyberwarfare, workforce requirements, and include investments in science and technology research.

Large Stakeholder Community

While the C4ISR, business IT and Space Community are diverse, naval forces have a long history of research and investment in IT to meet the communications challenges of dispersed operations. The publication illustrates how groups within SPAWAR; OPNAV; Headquarters Marine Corps; the newly forming Fleet Cyber Command (FLTCYBERCOM/10th Fleet); Marine Corps Systems Command; Team SPAWAR Program Executive Offices (C4I), Space Systems and SPAWAR Space Field Activity, and Enterprise Information Systems; and Joint Program Executive Office, Joint Tactical Radio System; NETWARCOM; and others are sustaining and

creating capabilities while continuing to evolve and improve the naval C4ISR suite. These capabilities are an essential and vital element of the national security strategy in today's networked world.

Land, Sea and Air

Naval IT, C4ISR, Space Systems, and Enterprise Support: Today and Tomorrow illustrates the value of end-to-end systems engineering in delivering integrated solutions to meet naval operational needs. This work is vital in linking network architectures to mission threads and warfare analysis for enhanced informational awareness among the Navy, Marines, joint forces, federal agencies and allies.

The publication illustrates the power of platform-independent C4ISR professionals collaborating across agencies and services to deliver "change at network speed," integrated warfighter and business infrastructure capabilities where needed most.

To name just a couple of examples, the vision highlights how C4ISR professionals can leverage domain expertise with ISR/Information Operations systems engineering data and using Naval Networking



Sailors man the watchfloor at NETWARCOM. U.S. Navy photo by Mass Communication Specialist 1st Class Corey Lewis.

Environment (NNE)~2016 top-level strategies to align programmatic efforts into the Next Generation Enterprise Network (NGEN) and Consolidated Afloat Networks and Enterprise Services (CANES) to accelerate technology delivery — all key components necessary for information dominance on the battlefield.

New Cyber Opportunities

The timely release of the technical vision coincides with key new Defense Department and Navy cyber initiatives: staff reorganization and consolidation of the OPNAV Directorates of Naval Intelligence (N2) and Communication Networks (N6) into a single organization, DCNO for Information Dominance; and the dynamic realignment of operational cyber capabilities under a single command, FLTCYBERCOM/U.S. 10th Fleet, to revolutionize and dominate warfighting capabilities in cyberspace and networks.

The reorganization will bring intelligence networks, electronic warfare, encryption operations, cyberspace communications and information gathering, as well as meteorology and oceanography under FLTCYBERCOM, the Navy Component to U.S. Cyber Command.

These new commands will play a major part in directing and shaping the crucial roles the C4ISR/business IT/Space Community are playing and will continue to play in the new Information Dominance Corps. For example, resource realignment has consolidated four major Naval Air

Systems Command programs: the Broad Area Maritime Surveillance Unmanned Aircraft System (BAMS UAS); E-2C (early warning aircraft); the Next-Generation Jammer; and Unmanned Combat Air System Demonstration (UCAS-D) into the DCNO for Information Dominance, with the concomitant need for the C4ISR/business IT/Space Community to collaborate with NAVAIR to create a unified position related to these unmanned systems and surveillance programs.

The Way Ahead

Naval IT, C4ISR, Space Systems, and Enterprise Support: Today and Tomorrow may be used as a communications tool within organizations to disseminate the criticality of naval IT, C4ISR, space systems, and enterprise support in advancing naval and joint warfighter objectives.

The publication aims for broad readership, including military personnel, Congress, the executive branch, the defense industry, mass media and the general public. CHIPS

Look for Naval IT, C4ISR, Space Systems, and Enterprise Support: Today and Tomorrow on the SPAWAR public Web site: www.spawar.navy.mil.



Air Traffic Controller 2nd Class Thomas Hartley stands watch in the Carrier Air Traffic Control center aboard USS John C. Stennis (CVN 74). Networked C4ISR systems are crucial enablers for battlespace awareness, information dominance and decision superiority. U.S. Navy photo by Mass Communication Specialist 3rd Class Walter M. Wayman.



The success of unmanned aerial surveillance platforms, such as the Navy Global Hawk UAV pictured here, have led to further investments in next-generation systems to improve Maritime Domain Awareness. U.S. Air Force photo by Jim Shryne.



WASHINGTON (Oct. 1, 2009) – Chief of Naval Operations (CNO) Adm. Gary Roughead delivers remarks for "Information Dominance: The Navy's Initiative to Maintain the Competitive Advantage in the Information Age" at the Center for Strategic & International Studies. U.S. Navy photo by Mass Communication Specialist 1st Class Tiffini Jones Vanderwyst.

Coalition Warrior Interoperability Demonstration

A unique environment of virtual reality, sophisticated technology and real warfighter conditions

By Sharon Anderson

It's not Afghanistan, but it will simulate the austere, remote and hostile conditions of being there. I'm talking about CWID — Coalition Warrior Interoperability Demonstration — where information technologies are assessed against simulated operational scenarios.

For 2009-2010, CWID is using an Afghanistan backdrop for combined operations. U.S. homeland security/defense scenarios will integrate virtual natural disasters, health pandemics and terrorist threats. CWID supports Department of Defense homeland defense and security acquisition decisions within a venue that provides significant savings to the government.

CWID's 18-month cycle begins with a Federal Business Opportunity posted on www.fbo.gov that asks industry to provide near-term technology solutions, also known as interoperability trials (ITs), designed to improve information sharing for both military and emergency first-responder operations.

CWID focuses on assessing new technologies and upgrades to existing versions of command and control (C2); communications systems; and intelligence, surveillance and reconnaissance (ISR) systems. CWID 2010 will execute in June.

The complexity of staging and executing approximately 40 ITs across multiple U.S. and international sites, with more than 1,500 participants and 20 participating nations, is immense and requires vigorous C2 and exhaustive planning, according to Dennis Warne, CWID site manager for Naval Surface Warfare Center Dahlgren.

"We are coordinating command and control over the Pacific and Atlantic, across Europe, Lillehammer, Norway, in Germany, in Italy. We run the trials during the day, but think of what time it is in Italy and Europe," Warne said. "No other virtual or real-world environment can duplicate the unique characteristics of the CWID infrastructure."

CWID is a Chairman of the Joint Chiefs of Staff-directed annual technology discovery and risk reduction event which identifies information-sharing solutions

for operational problems. The Defense Information Systems Agency (DISA) manages CWID's day-to-day operations using the CFBLNet, or Combined Federated Battle Laboratories Network, which will span 15 time zones, from New Zealand to the United States, and across Europe.

CWID encompasses an environment of virtual reality, sophisticated technology and real-world conditions that video game fans would love to enter. But there is nothing playful about CWID. To participate, proposed technologies must fill warfighting gaps and be interoperable, not only with joint partners, but with NATO partners, and at another level, with nongovernmental organizations to coordinate disaster relief responses and humanitarian aid.

CWID's Unique Environment Adds Complexity and Realism to Testing Warfighter Solutions

"This is a difficult battlefield. Coalitions are complex: different languages, different cultures; coalitions are ad hoc by nature. Sometimes there are different standing agreements with NATO countries," said U.S. Marine Corps Lt. Col. Bruce Downs, CWID's coalition forces land component commander and role player.

"We are also looking for opportunities to integrate information, collaborate and share information on the battlefield. This is a rare opportunity. This is the only place I know of where you can have a multi-domain trial and where you have classified and unclassified networks, and you are sharing information between those in the backdrop of something that is meaningful to a warrior," Downs said.

Technology plays a major role in CWID, where participants explore the "art-of-the-possible," according to Downs.

"We get ideas about how to apply technology, to try to stretch it to meet our needs for interoperability and allow us to have an advantage on the battlefield," Downs explained. "All of these coalition countries have come with their own solutions independently. Some of them are very technical; some of them are manual.

We take and use all of that information together to make good, effective decisions in those scenarios. There is everything from what we call kinetic warfare [which is] dropping bombs and shooting bullets and maneuvering on the battlefield, to running convoys with relief supplies, to humanitarian relief, to ship-to-shore movements."

There are so many fascinating technologies that will be explored in June, but I'll just highlight a few. CHIPS spoke with several CWID participants during the CWID Initial Planning Conference, which took place Nov. 16-20, 2009, in Williamsburg, Va., where more than 200 military, government and industry experts from around the world discussed their proposed ITs for CWID participation. While neither the Navy nor Defense Department endorses the commercial products used in the ITs; testing these products is the only way to determine warfighter utility.

IT001 – Service-oriented Infrastructure for Maritime Traffic Tracking (SMART)

The Italian-led Virtual Regional Maritime Traffic Center (V-RMTC) is a virtual network environment connecting the operational centers of participating navies to unclassified information on merchant shipping vessels to enhance maritime situational awareness (MSA).

In CWID 2010, Service-oriented Infrastructure for Maritime Traffic Tracking will undergo interoperability testing with system partners: Finland, Germany, the United Kingdom and United States. SMART represents the next-generation development of V-RMTC, according to Italian Navy Lt. Cmdr. Sergio Ciannamea.

But other frameworks can be easily exploited through this technology, for example, the Italian interagencies and for the European Union's new experiments, such as the demonstration for the Maritime Surveillance (EU MARSUR) network scheduled for the end of 2010, said Ciannamea. "SOA-based technology is still in its formative stages. It will be taking over where V-RMTC has left off in providing

the next spiral evolutionary step for the Italian Navy MSA technology systems, built upon the standards, strategies and capabilities of V-RMTC, to build and deploy MDA capabilities.

"Data are delivered according to specific formats (XML; MERSIT, developed by the Italian Navy; OTH-T-Gold; etc.) and gathered by a hub located at Italian Navy Fleet Headquarters (HQ CINCPAC)," Ciannonea said.

"More than 300 gross-ton (and passenger) ships are obliged to have the Automatic Identification System (AIS) for vessel identification, tracking, collision avoidance and coastal surveillance. But AIS is not tamper-proof," Ciannonea said, "bad guys can alter information within AIS, so it is not always a reliable source of information for identifying vessels of interest that's why MSA is so important. And it is not only the AIS-fitted vessels that are interesting in our MSA perspective."

Another boost to MSA is the Trans-Regional Maritime Network (T-RMN) project which is the addition of more partners within the three V-RMTC enclaves, already including 29 countries. The next expansion of the partnership, will include Persian Gulf countries: Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the United Arab Emirates.

IT002 – Inter Domain Services Manager (IDSM)

IDSM is a service oriented architecture (SOA) middleware application that provides integration and interoperational services for disparate data sources. Access to the integrated data is tailored for the user and can be accessed via: Web services, portals, thin or fat clients, or software as a service using a JBoss J2EE environment.

The system can rapidly take external data sources, such as systems, databases, streams, repositories and Web sites, and combine them under a mediated metadata layer that allows data mining, manual and automated analysis, and various visualization capabilities in a single application, explained William Sadler of Organizational Strategies, Inc.

The most innovative aspect of IDSM technology is in its ability to fuse and allow discovery of information at different classification levels — all within a unified security model. Users can view data, as well as photographs and video.

"We absolutely mediate all the traffic communication between one classification level and the other, and we have extensive workflow and document management capabilities built into the system. When somebody in a Top Secret enclave would build a Word document or a video out of pieces of unclassified, Secret or Confidential data that entire document would be classified as Top Secret.

"In our system, we maintain the metadata tags around traceable storage for each one of those information chunks. If that structure is not modified at the highest level, we can maintain that security traceability back to its original source," Sadler said.

"The person who is sending the document just has to push send. He doesn't need to worry about the declass situation. The workflow management system, however, looking at the tags on the data, will then alert the person with authority to declass and give him two choices: either declass the data, and here is the stuff that needs to be declassified to go down to this level, or the system can automatically redact the document. Then when the data is sent, it is missing the information that is not appropriate for a lower classification," Sadler said.



MARINE CORPS AIR GROUND COMBAT CENTER TWENTYNINE PALMS, Calif. Nov. 17, 2009 – A light armored vehicle with Company E, 3rd Light Armored Reconnaissance Battalion, fires its 25 mm Bushmaster chain gun during table one of qualifications at the Combat Center's Range 109. The chain gun is the main weapon used by the company. U.S. Marine Corps photo by Lance Cpl. M.C. Nerl.

The IDSM framework provides XML-based interaction with IDSM clients, validation of client-supplied messages, IDSM data store access, and the management of process flow through the system, including identification and service processing logic.

Surprisingly, IDSM is built on open source code, open standards and Alfresco products for document management and workflow. Sadler said the security technology and its cross-domain solution are the most advanced concepts of the system.

IDSM aggregates intelligence from disparate sources and processes the data into a usable format for the commander at all levels of authority. IDSM is primarily used for operations, but it can be used down to the tactical level, and at all levels, its aim is to improve situational awareness and enhance decision-making. IDSM's robust capabilities can be pushed down to personal digital assistants for convoy security and improvised explosive device (IED) detection.

Testing will require IDSM to interoperate with the Global Command and Control System, Theater Ballistic Missile Control System, Joint Mission Planning System, Joint Automated Deep Operations Coordination System, and more.

IT031 – Joint Asset Management Integrated Support System – Automated Armory (JAMISS-AA)

JAMISS-AA is a Web-based asset tracking and maintenance management system that uses government off-the-shelf technology for total life cycle management. JAMISS-AA was designed for bandwidth-challenged or disconnected environments, and it adheres to all DoD information assurance policies and guidelines.

JAMISS-AA leverages existing technology, according to Michael Daugherty, a special missions task manager for the JAMISS project, with the expeditionary electronic warfare system division. Daugherty, who is also an employee with the Naval Surface Warfare Center, Crane, Ind., explained the business rules for JAMISS.

Assets are tagged and tracked through IUID or radio frequency

identification (RFID). IUID, or Item Unique Identification, is an asset identification system instituted by the Defense Department to uniquely identify a discrete tangible item or asset.

Tangible items are distinguished from one another by the assignment of a unique identifier in the form of a unique data string and encoded in a bar code placed on the item. An item unique identifier is only assigned to a single item and is never re-used. Once assigned to an item, the IUID is never changed even if the item is modified or reengineered. IUID tagging is similar to Social Security numbering.

The JAMISS-AA system is Navy-developed but Marine-owned. The U.S. Marine Corps Light Armored Vehicle (LAV) program sponsored JAMISS development to track maintenance actions, vehicle usage, configuration and location, and provide global visibility of the information. The system supports operational, strategic and tactical level operations, missions and planning. Users include at point of action (point of maintenance or inventory control point level) up to program management.

"JAMISS-AA will leverage a CWID trial cross-domain solution to show interoperability with NATO partners," Daugherty said. "Since its exposure in CWID, the Navy, Air Force and the Department of Homeland Security have expressed an interest in the system. There are multiple armories spread across various agencies, and the services could leverage off JAMISS capabilities.

"Currently, tracking weapons via stubby pencils and spreadsheets is prone to data error. A 3 can be mistaken for an 8, and it can take hours, sometimes days to track down a weapon. When the Marines implemented JAMISS-AA utilizing IUID, the data quality and accuracy went from about 80 percent to nearly 100 percent," Daugherty said.

CWID will provide the environment to demonstrate the ability of JAMISS-AA to exchange IUID and asset information between the Marine Corps and NATO, and it will also provide the Marines with a warfighter utility assessment.

"JAMISS is adaptable to different communities of interest where asset accountability, accuracy, tracking, [and] configuration management, are essential to total life cycle management," said James Hamric, a contractor supporting JAMISS.

Space and Naval Warfare Systems Command and SPAWAR Systems Center Pacific

SPAWAR and SPAWAR Systems Center Pacific (SSC Pacific) in San Diego, Calif., have been involved with JWID and CWID since its inception. Acquisition successes began with the demonstration, evaluation and, ultimately, the transition of Radiant Mercury to the military community. The SPAWAR team focuses on technologies that fulfill requirements in two primary areas: maritime domain awareness and coalition interoperability.

The team functions as the Combined Forces Maritime Component Commander (CFMCC), and coalition staff members have included representatives from Germany, Canada, New Zealand, Italy and Australia. In 2010, an officer from Finland will join the team. The SPAWAR team also supports homeland security initiatives in the San Diego area by involving local stakeholders in the development of the homeland security scenario, evaluation of various technologies, and the development of procedures that will be effective during a wildfire or other domestic disaster in the Southern California area.

Some of the homeland security organizations with which the SPAWAR team has developed ongoing relationships include the City of San Diego, San Diego Police Department, San Diego State University, the Regional Terrorism Threat Assessment Center, U.S. Coast Guard, and the California Army and Air National Guard.

Naval Surface Warfare Center Dahlgren Division

CWID 2010 marks the 11th year that NSWC Dahlgren, a secondary Navy site, has hosted CWID trials. Dahlgren is the primary site for Marine Corps and Army demonstrations. SSC Pacific is CWID's primary Navy site.

"We are the site for the U.S. Coast Guard, the National Guard and Air National Guard demonstrations too," Warne said. "We are a multifaceted site. Last year we had nine separate operational centers, extremely high multidomain."

NSWC Dahlgren will also be working with the Maryland Emergency Operations Centers concurrently within CWID 2010, according to Warne. About 300 personnel support the NSWC Dahlgren site during CWID execution, a combination of military, government and contractor teams.

Keith Meyers, chair for CWID's systems engineering and integration working group, tracks the high-tech infrastructure that is needed to support CWID's unique requirements, such as the Global Command and Control System and Advanced Field Artillery Tactical Data System.

CWID's Rich History

Over the past 16 years, CWID has grown from a U.S. Army initiative to a global event to discover new and emerging technologies and to test and evaluate them for warfighter utility.

CWID 2007 was the first year a concerted effort was made to involve programs of record which resulted in several interoperability trials to be more rapidly fielded by emergency responders and warfighters.

During CWID 2008, several technologies were close to implementation and another, Radio Inter-Operability System (RIOS) Incident Site Communications Capability (RISCC), was used in the U.S. Open 2007 and Kentucky Derby 2008.

In 2009, the U.S. Joint Forces commander directed U.S. CWID to use Afghanistan as the operational backdrop for the simulated, operational scenario providing richer context to the demonstration and more meaningful capability assessments. U.S. homeland security/defense scenarios increased interaction with worldwide organizations to improve interoperability.

CWID continues to develop and triumph over challenges presented throughout the years, and the team looks forward to a bright future in assisting warfighters and first responders with solutions to their difficult missions. Participating in CWID is both exciting and exhausting as demonstrators strive to provide warfighters with what they need to dominate the battlespace and interoperate with mission partners. **CHIPS**

Sharon Anderson is the CHIPS senior editor. She may be reached at chips@navy.mil. For more information about CWID, go to the CWID Web site at www.cwid.js.mil.



Collaboration Tools for the Federal Government

By Christy Crimmins

Over the past few months, collaborative media has become a topic of interest and debate in both the Department of Defense and federal government. As a result of this interest, collaborative sites restricted to myriad combinations of defense, intelligence and federal government communities have begun to see a rise in participation. Some of them, such as Intelink, are sponsored by government agencies and limited to a select subset of the federal government, while others, like GovLoop, aim to connect employees at the federal, state and local levels. Below is a selected overview of a few of these tools.

GovLoop was launched in 2008 and now has 20,000 members across federal, state and local government. GovLoop, called "Facebook for feds" by some pundits, does at first appear to be a straightforward social networking site; however, the site, www.govloop.com/, also hosts blogs, a wiki and a listing of job openings. The site is open to all members of the government community, including contractors and students, and individuals interested in government service.

Intelink was developed by the Intelligence Community Enterprise Services (ICES), within the Office of the Director of National Intelligence and is home to Intellipedia, the U.S. government's unclassified wiki. To be eligible for an account, users must belong to or provide direct support to the intelligence, defense, homeland security, law enforcement or diplomatic communities. In addition to Intellipedia, other services offered by ICES through Intelink are a blogging capability, video, instant messaging, and a Web-based document management system called Inteldocs. An outline of these services, as well as information on ICES, can be found on Intellipedia at <https://www.intelink.gov/>.

Chirp is a microblogging pilot that is part of the Intelink suite of tools described above. The site, modeled after microblogging sites like Twitter, is intended to provide situational awareness and information on breaking news. Chirp promotes collaboration through informal messaging. Like other microblogging tools, Chirp allows users to post messages of up to 140 characters. At (@) tags are used to bring chirps to the attention of a specific user. These are usually used when replying to a previous chirp posted by that user. Hash (#) tags are used to tag a chirp with metadata and allow users to search on particular key terms. More information about Chirp can be found at <https://www.intelink.gov/chirp/>.

milSuite is a group of collaborative tools launched by the Army in October 2009. These tools focus on three main objectives: locating information, sharing knowledge and connecting people. These tools are available to military, civilian and contractor personnel across the DoD who have Defense Knowledge Online (DKO) accounts. The suite of tools includes three separate capabilities:

milWiki is a knowledge management tool made up of a collection of Web pages that are editable by anyone who can access them. This allows for a living knowledge bank where experts are encouraged to contribute their experience and knowledge and update information in real time. The tool also allows users to integrate and interlink knowledge into topical-based articles and collaborate on issues up to and including unclassified/"For Official Use Only" documentation. milWiki's goal is to capture the intellectual capital of the DoD community and allow users to easily locate and expand upon that knowledge through community updates.

milBlog is a place to find and share the latest news, insider articles, comments and posts from the community. It is designed to invite collaboration through discussion and comments. milBlog provides quick, easy access, and a secure awareness for mission-related knowledge and information.

milBook is an initiative to connect people across the DoD community. milBook acts as a central hub for networking DoD professionals with others who have similar interests and work responsibilities, much like the popular commercial sites Facebook and LinkedIn. Users have the ability to share information through group blogs, discussions and private wiki documents allowing secure communities of interest to grow and connect with others across the greater military community.

To access the milSuite community, please visit <https://www.kc.army.mil/book/index.jspsa>. You can either log on via your Common Access Card or with your DKO username and password. As interest in collaboration and transparency in government increases, the federal government will continue to explore and make use of collaborative tools. CHIPS

Christy Crimmins provides support to the DON CIO communications and emerging technology teams.

Remote Testing Using ADEPT

By Joel H. Timm

Trident Warrior is the Navy's major annual Sea Trial event. Trident Warrior 2009 (TW 09) marked the first time that remote test equipment information was used in real time and controlled from a shore installation while on an operational ship underway off the Virginia Capes. Among the distance support objectives accomplished were: (1) real-time connectivity from ship-to-shore of the equipment; and (2) the capture and transfer of the information in near-real time for analysis.

This testing was made possible by the Adaptive Diagnostic Electronic Portable Testset. ADEPT is a lightweight ruggedized touch-screen system which can be used to maintain and troubleshoot the SPY-1 radar on Aegis ships by integrating maintenance procedures, test equipment and data collection into a single system.

ADEPT is an electronic test tool originally designed for the SPY-1A radar by Mikros Systems Corp. It consolidates multiple test equipment (digital multimeter, oscilloscope, power meter) into one portable unit.

The test set incorporates various instrumentation cards and XML-tagged maintenance requirement cards (MRCs), linked to an integrated Structured Query Language database. The test set provides unique distance support capabilities and has been shown to significantly reduce the time it takes to perform maintenance and to align complex electronic systems. ADEPT is a Small Business Innovation Research (SBIR)-funded project that is currently in development and testing.

Shipboard technicians can use ADEPT to run integrated MRCs. The MRCs are displayed on the screen of the ADEPT unit, and during the measurement step of the procedure, the test equipment is automatically configured for the measurement.

Maintenance information and equipment status data, such as oscilloscope displays, are collected and transferred to on-board Distance Support servers for viewing by In-Service Engineering Agents (ISEAs). Using designated shipboard Distance Support connections, ISEAs can remotely control ADEPT in real time, thereby assisting shipboard technicians in the troubleshooting process.

During the exercise, the USS Farragut

(DDG 99) was underway in the Virginia Capes. Aboard the ship, ADEPT was connected to Operational Readiness Test System Tech Assist Remote Support (ORTSTARS). A virtual network server client tool and secure shell are used in ORTSTARS to enable application sharing between the Unix and Windows operating systems through a secure network.

While underway, ADEPT successfully demonstrated three sessions of real-time SPY-1 support via ORTSTARS and one SPY-1 data transfer via the Navy Information Application Product Suite infrastructure to the Naval Surface Warfare Center, Port Hueneme Division for analysis. The sessions were accomplished over several hours each with solid connectivity.

As the ship's users became increasingly familiar with the ADEPT system, they frequently used it without assistance from NSWC Port Hueneme personnel. The response from the ship's crew was excellent, and their feedback was positive.

ADEPT completed its official TW 09 experimentation which included troubleshooting an issue with the SPY-1 radar aboard the USS Farragut. About 10 NSWC Port Hueneme subject matter experts were able to see, control and resolve the issue with ADEPT in real time via ORTSTARS while working with Fire Controlman 2nd Class Sullivan, the SPY technician on board the USS Farragut.

FC1 (SW) Cooper, the SPY technician at NSWC Port Hueneme, said, "It gives us the ability to view the 'O'Scope' readings and see exactly what they (ship's force) are seeing."

The SPY-1 engineering team at Port Hueneme could review and control the ADEPT instrument displays, such as RF power meters, oscilloscopes and the Operational Readiness Test System (ORTS), in real time while the shipboard technicians performed SPY-1 maintenance activities.

The SPY-1 engineering team said they experienced minimal latencies of 1 to 2 seconds in the connection while in control of the ADEPT system aboard the ship. Additionally, they were able to place the ADEPT display on a large screen at NSWC Port Hueneme giving several engineers the opportunity to troubleshoot SPY-1 simultaneously.

During the troubleshooting of an ir-



ATLANTIC OCEAN (Feb. 29, 2008) – The guided-missile destroyer USS Farragut (DDG 99) approaches the aircraft carrier USS George Washington (CVN 73) in preparation for a refueling at sea. U.S. Navy photo by Mass Communication Specialist Seaman Luis Ramirez.

regular SPY-1 reading, the SPY-1D(V) engineering team at NSWC Port Hueneme was able to walk the ship's crew through a step-by-step procedure in real time while viewing and operating the ADEPT equipment.

Sanitized pictures were taken of the SPY-1 backplane and shared with the engineering team via ADEPT and ORTSTARS. Group collaboration continued until the irregularity was resolved.


Lt. j.g. Darryl Diptee, from Naval Network Warfare Command, referred to ADEPT's immediate technical reach-back capability as the "technical 911" for the eyes of Aegis.

Furthermore, the ADEPT unit can also store technical documentation which is useful to a shipboard technician during the troubleshooting process. SPY-1 radar engineer Marc Dasca at NSWC Port Hueneme said, "[ADEPT] gives us the ability to assist the fleet and be their distance support resource."

The need for immediate technical assistance for tactical systems in today's high operational tempo is obvious. An Aegis-class ship with an inoperative SPY-1 radar would have a substantially reduced mission capability.

Flying SPY-1 engineering teams to distant parts of the globe is costly and time-consuming. But with ADEPT and ORTSTARS, the waiting time required for expert assistance is reduced to minutes instead of days — which translates directly to increased fleet readiness while at the same time reducing costs and manpower requirements. CHIPS

Joel Timm is in the office of engineering and technology at NSWC PHD. Timm has a Master of Science degree in systems engineering (MSSE).



Hold Your Breaches!

By Steve Muck

Your Office Copier/Printer May Present Information Security Risks

The following is a recently reported compromise of personally identifiable information (PII) involving the disposal of copiers containing personal information stored on their hard drives. Incidents such as this will be reported in each CHIPS magazine to increase PII awareness. Names have been changed or removed, but details are factual and based on reports sent to the Department of the Navy Chief Information Officer Privacy Office.

The Incident

Recently, a command disposed of numerous copiers that had reached the end of their service life. The copiers were originally leased and subsequently purchased by the government with a typical copier maintenance agreement. The command was under the impression that the copiers did not contain hard drives and therefore did not require sanitization or removal of hard drives before disposal. A few weeks after disposal, the command learned that the copiers did, in fact, contain hard drives. This particular breach did not result in a loss or compromise of PII because the machines were recovered by the government soon after disposal.

Many copiers, printers and multifunctional reproductive machines manufactured today have hard drives capable of storing documents that have been scanned, printed or faxed as digitized images. These machines are often connected to Department of the Navy (DON) networks to ease workload and increase efficiency.

Reproductive office equipment manufactured in the last seven years employ hard drives that store digital images. While much of the hard drive space is used for processing, the machines in this scenario stored up to 6,000 pages of information. The information copied may include PII, classified or sensitive but unclassified information, depending on the machine. Once the hard drive memory has been exceeded, files are automatically overwritten. "Cap points" limit the number of pages stored to hard drives, and the cap limitation can vary on each make and model number.

Depending on the type of machine, information from small print jobs may be stored in random access memory (RAM) only, and the files may be overwritten with each new print request, or lost when the machine is powered off. Manufacturers of the newest reproductive office equipment may advertise that their hard drives use encryption software to safeguard data, but as of this writing, that encryption capability is not DON-approved. Approved DON encryption solutions do not encrypt reproductive equipment hard drives.

DON copiers, printers and multifunctional machines are either leased from a vendor or government-owned. In either scenario, the possibility of PII loss presents challenges when equipment is repaired or turned-in for replacement. Stand-alone fax machine memory is generally nonvolatile and is lost as soon as the machine is turned off. CHIPS

Lessons Learned

The DON CIO is drafting tighter policy controls regarding the turn-in and disposal of reproductive equipment. Until release of the new policy, DON personnel should comply with the following best practices.

For CLASSIFIED copiers/printers:

Guidance for reproductive equipment can be found in SEC-NAV M-5510.36, paragraphs 7-15(2), (3), available on the Chief of Naval Operations (N09N2) Information and Personnel Security Web site at www.navysecurity.navy.mil/info-551036.htm.

For UNCLASSIFIED copiers/printers:

- Identify the hard drive capabilities (and security risks) of your photographic equipment and educate office personnel regarding that information.
- For government-owned equipment, hard drives should be removed and physically destroyed before disposal. Hard drives are not easily accessible, so removal will probably require a technician.
- For leased equipment, the hard drives should be reformatted to remove all data. Refer to the equipment manual or service technician for instructions on the reformatting process.
- Place a sticker or placard on the copier/printer with the following: "Warning, this government-owned copier uses a hard drive that must be physically destroyed before turn-in" or "Warning, this leased copier uses a hard drive that must be reformatted before turn-in."

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

Steve Muck is the DON CIO privacy team lead.

NAVY'S CHIEF TRAINING OFFICER ADDRESSES DEFENSE CONTRACTORS AND DoD REPS

By Joy Samsel, NETC Public Affairs

Citing Navy training's ability to flex and change to meet the needs of the fleet, Rear Adm. Joseph Kilkeny, commander of Naval Education and Training Command (NETC) spoke to the audience at the Interservice/Industry Training, Simulation and Education Conference in Orlando, Fla., Dec. 1. The address was part of the General/Flag Officer Panel, which gave participants an opportunity to talk about how their organizations are supporting military missions, as reflected in the conference theme, "Train to Fight ... Fight to Win."

"We must gain more proficiency and our students more expertise in less time to keep up with the rapidly evolving challenges throughout the world," Kilkeny said. "The technology on display throughout this conference is indeed impressive, but we all acknowledge that it is our people who enable our services to be combat ready. We all go to great lengths to select training instructors who can teach, and we select those best suited to learn and develop into the most combat-ready Sailors, Soldiers, Marines [and] Coast Guardsmen [in] highly technical and challenging positions. This is also true whether you are a Fortune 500 company or a small independent contractor. And it is especially true of the United States armed forces."

Kilkeny gave a brief overview of the Navy training domain, which includes more than 19,000 military and civilian personnel, who provide training at more than 230 subordinate activities around the world. More than 35,000 students are taking part in Navy training on any given day. NETC logged more than 615,000 graduations in fiscal year 2008, including students from the Navy, Marine Corps, Army, Air Force and Coast Guard. The U.S. Navy also trains more than 12,000 international students from more than 150 countries annually.

The admiral talked about a few of the changes which occurred within NETC over the last decade, including the Executive Review of Navy Training, directed by then Chief of Naval Operations Adm. Vern Clark, which led to the Navy's "Revolution in Training."

"What followed was a massive restructuring that enabled us to work closer with the fleet to understand their requirements for trained Sailors, and to concurrently embrace a new approach in the methods used to train them," Kilkeny said. "Training works collaboratively with the fleet to take a human performance approach to analyzing and solving performance gaps. We identify Sailors' knowledge, skills and abilities required to be successful at a job, task or function, and design training to respond to those requirements — as they are determined by the fleet."

The admiral said changes to Navy training will continue because the missions of the Navy continue to change.

"In support of the expanded role for Sailors on the ground [in] Overseas Contingency Operations, our Center for Security Forces has adapted training to meet the demands for individual augmentees in Iraq and Afghanistan, and other parts of the world," Kilkeny said. "The understanding of foreign cultures, customs and languages is a direct joint force multiplier that enables service members to sustain our long-standing alliances

NORFOLK, Va. (Dec. 4, 2009) – Fire Control Technician 3rd Class Zamir Wolfe logs on to the Submarine On Board Training portion of the Naval Education and Training Command Web site. Submariners can also download and take the training with them on deployment. U.S. Navy photo by Mass Communication Specialist 1st Class Todd A. Schaffer.



and forge new relationships with emerging partners. For Sailors, the Navy achieves this understanding through training in Language, Regional Expertise and Culture at our Center for Information Dominance."

Kilkeny said the development of training begins with the weapons and platforms the Navy purchases. "We must work closely with you in the defense development and construction arena to ensure when we buy a system, the training is developed in parallel and fully supports the Sailors and joint service partners in the mission required of the system delivered."

Kilkeny also addressed the issue of technology in training, saying NETC has embraced technology to support training, in schools, as well as in exporting training to the fleet.

"These endeavors resulted in the use of blended learning solutions that include instructor-led training, computer-based training, simulation and technical training equipment," Kilkeny said. He gave a few examples of training initiatives, including the Submarine Learning Center's Submarine On Board Training. It provides Sailors with training developed by subject matter experts which is approved by the fleet as meeting its requirements. Sailors can also download and take the training with them on deployment.

Looking at the future, NETC is partnering with the Office of Naval Research and the Defense Advanced Research Projects Agency on a project called Digital Tutor. This adaptive project leverages the expertise of Silicon Valley information technology specialists to model how best to train the next generation of cyberwarfare experts.

While citing the requirement for the best training possible, Kilkeny tempered his comments with the reality of fiscal constraints. "How can industry deliver highly technical, complex and secure solutions at a price that the services can afford? This is a challenge for both of us. As we have always done, NETC will continue to work closely with the fleet to determine the best training to support their needs. We have never, and will never, create our training in a vacuum," the admiral continued.

"The training we provide America's Sailors and our joint service partners is outstanding — if it was not — we would not have more than 150 nations knocking at our door to send their military members through our courses." CHIPS

For more information about the Naval Education and Training Command, visit <https://www.netc.navy.mil/>.



GOING MOBILE

NMCI Gets Into A Hotspot

By Mike Hernon

For years now, Navy Marine Corps Intranet (NMCI) users have jealously eyed the laptop-wielding, Wi-Fi-connected masses in coffee shops, hotels and airports as they turned idle time into productive time. Barred from full network access, NMCI users on the go had to settle for cellular phones, air cards and Outlook Web Access to provide mobile support. While these capabilities provide some fairly productive mobility tools, access to the information and resources on NMCI that would further support the mobile worker remained unavailable — until now.

With the release of Wireless Public Hotspots (WPH) service, NMCI users within the continental United States can now use free or for-fee public Wi-Fi hotspots to securely access NMCI. This capability provides mobile users with the same computing environment they would have when sitting at their wired computer. This enhanced capability will allow remote users to remain better connected and more productive outside of their wired environment, whether on travel, telecommuting from home, or in any location outside the office where Wi-Fi is available.

Private Network, Public Wi-Fi

Integrating any secure, private network, such as the NMCI, with public Wi-Fi access points outside the control of network administrators is not done lightly. Before delivering any enterprise mobility capability to the Department of the Navy workforce, a careful analysis of the delicate balance between the benefits and inherent risks of wireless technologies is conducted.

Opening up network access through publicly available Wi-Fi hotspots presents significant information assurance (IA) concerns about introducing threats that might potentially harm the network. The use of public Wi-Fi access points, which are normally unsecured and unencrypted by design to foster maximum sharing of the signal, brings a number of

widely known vulnerabilities that may be exploited. For example, is that wireless network named “FREE STARBUX Wi-Fi” that shows up as available for connection really coming from the coffee shop you’re in or from the van in the parking lot?

Setting up such imposter or “rogue” access points that can divert your laptop to a hacker-controlled destination and/or install malware is just one potential avenue for hackers. Another common attack is to take advantage of the lack of encryption on a public access point to intercept and read the traffic transmitted between the laptop and the network.

Of course, these threats are above and beyond the fact that you are conducting official business in the middle of a bustling coffee shop or airport terminal, and wearing a uniform or sporting a Defense Department badge that just might make you a more attractive target for hackers.

Locking It Down to Open It Up

The threat to the network from these vulnerabilities is real; the impact from a breach could not only affect the user that is being targeted, but the entire network. Clearly, before approval could be given by the Navy and Marine Corps Designated Accrediting Authorities (DAA), network engineers had to develop a solution that would minimize the risks of Wi-Fi access.

As a result of these efforts, connecting to NMCI via a public hotspot is done in a significantly different way than how you would normally use your laptop’s internal Wi-Fi antenna to connect to a hotspot at home or in a public location.

The NMCI solution relies on two components that reside on the laptop; one is hardware, and the other is software-based. The hardware consists of an approved wireless network interface card which installs in the laptop’s PCMCIA slot. (Laptops with an ExpressCard slot will require an adapter.) The necessary client software component is the Wireless Cli-

ent Encryption, which is available only through NMCI. This allows you to securely connect to NMCI via an encrypted virtual private network. Additional security includes the encryption of data-at-rest and the Host Based Security System for intrusion prevention.

This newly announced Wi-Fi hotspot offering is distinct from, and in addition to the existing solution for wireless local area networks (WLAN) for access on those Navy or Marine Corps bases and installations (i.e., base area networks), where WLANs are currently in place. Depending on your needs, you may install either or both solutions on your laptop.

Cutting the Cord

All components required to enable wireless access to either public or base access points are available through the Contract Line Item Numbers (CLIN) on the NMCI contract. There are one-time costs to procure the hardware and software, as well as a monthly recurring fee, each ordered through a separate CLIN. Additionally, the following constraints apply:

- Windows XP operating system installed;
- Broadband Unclassified Remote Access Service (BuRAS v4.0.5) installed;
- Navy NMCI domain only (as of this writing, the Marine Corps DAA has not approved the solution);
- Unclassified use only; and
- Not available for non-NMCI networks, such as the science and technology domains.

For the latest offerings and pricing information, visit the NMCI Homeport wireless page at <https://www.homeport.navy.mil/services/wireless>. Additional resources on the site include a user guide and an online tutorial. CHIPS

Mike Hernon is an independent consultant to the DON CIO on a variety of telecommunications-related topics. He was formerly the chief information officer for the City of Boston.

Identity Management Operations to Improve Cybersecurity

By Sonya Smith

The December 2008 report written by the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency, "Securing Cyberspace for the 44th Presidency," began with one central finding: "The United States must treat cybersecurity as one of the most important security challenges it faces."

The report went on to state, "Creating the ability to know reliably what person or device is sending a particular data stream in cyberspace must be part of an effective cybersecurity strategy." The report urged the government to accelerate the adoption of identity authentication.

The administration's Cyberspace Policy Review, released in April 2009, stated very clearly that: "We cannot improve cybersecurity without improving authentication, and identity management is not just about authenticating people."

The National Security Telecommunications Advisory Committee's "Report to the President on Identity Management Strategy" of May 2009 states: "... this lack of trusted identification enables harmful and/or malicious activity and diminishes national security/emergency preparedness capabilities, endangering national and homeland security as well as individual privacy and security."

The Department of Defense understands the magnitude of the threat we face in cyberspace. The threat is advanced, persistent and constantly changing. In addition, the increasing popularity of collaborative Web applications, such as blogs, social networks, podcasts and wikis, and mobile devices, has brought a new set of challenges to cybersecurity.

There is a clear appreciation of the relationship between cybersecurity and identity management; we must be able to authenticate entities, as either human or nonhuman, with DoD resources and then be able to manage access privileges.

A major vulnerability on DoD networks is the use of usernames and passwords. Therefore, the DoD has increased assur-



ance of user authentication by replacing the requirement for usernames and passwords with the DoD Common Access Card (CAC) and associated public key infrastructure (PKI) to cryptographically logon to DoD unclassified networks. This effort is now being extended to the classified network as well.

The DoD has seen the benefits of this effort. Retired Air Force Lt. Gen. Charles Croom, when director of the Defense Information Systems Agency and commander of the Joint Task Force - Global Network Operations, said in January 2007 that successful intrusions to DoD unclassified networks had declined 46 percent due to CAC use. The DoD is now also requiring PKI-based user authentication to access the majority of its private Web sites.

Those same PKI certificates are being used to encrypt personally identifiable information (PII) and sensitive information to ensure its confidentiality while in transit. Digital signatures, also using PKI, provide nonrepudiation services, enabling a higher level of assurance that the e-mail users receive is authentic. Digital signatures also help thwart e-mail spoof-

The Defense Department is making a number of improvements to the Common Access Card to enhance identity authentication and physical and network security

ing attempts. In the Department of the Navy (DON), these protections are being extended to mobile personal electronic devices such as BlackBerrys.

Identity management initiatives utilizing the CAC with PKI certificates have changed the way the Defense Department does business. But, as with all things, there is always room for improvement. The use of Homeland Security Presidential Directive-12 (HSPD-12) and Federal Information Processing Standards-201 (FIPS-201) are mandatory across the federal government and provide a common language and standard to improve identity assurance.

The CAC is the DoD's vehicle to HSPD-12 compliance, and improvements are being made to the CAC to comply with FIPS-201. These include making the card/token itself more resistant to tampering and counterfeiting, meeting interoperability requirements, improving the vetting process before card issuance to ensure the applicant's eligibility and uniqueness within the database, and the addition of biometrics to the CAC.

The CAC improvements to comply with

the FIPS-201 standard are helping to raise the confidence level within the CAC infrastructure. Issuance is the critical point of identity management and because of the FIPS-201, DoD now requires:

- an individual's eligibility for a CAC;
- verification of DoD affiliation from an authoritative data source instead of a paper form;
- completion of the FIPS-201 required background check; and
- verification of a claimed identity per FIPS-201.

The enterprise authentication solutions for cybersecurity are currently PKI-based. The DoD has deployed a significant number of "next-generation CACs," or CACs that are being used as part of the HSPD-12 transition.

As part of the transition, some biometrics information is being stored on the next-generation CACs. At a minimum, the fingerprints information on the CAC could be utilized as a stronger form of multifactor authentication.

The focus of identity management must build on successes to date and move forward to a more all-encompassing approach to include meeting the requirements of interoperating with other HSPD-12 compliant federal credentials and securely sharing information with other mission partners.

The new CAC contains advanced technology that will enhance the security of federally controlled facilities and computer systems and ensure a safer work environment for all federal employees and contractors. CHIPS

Out with the old.

In with the smart.

For more information about the Defense Department's next-generation Common Access Card, go to the CAC Web site at www.cac.mil or the DON CIO Web site at www.doncio.navy.mil.

Sonya Smith is the deputy director of the DON CIO cybersecurity and critical infrastructure team.

The DoD is proud to be among the first government agencies to issue the HSPD-12 compliant federal credential — the next-generation CAC.

The gold standard of advanced identification.

This initiative is part of an ongoing effort to provide government personnel with the most secure and reliable forms of identification possible. The next-generation CAC represents significant strides in contactless technology and heralds a critical step in the evolution of personnel and national security.

The next-generation CAC is more sophisticated:

- Increased data storage and memory capacity
- Integrated circuit chips, magnetic stripe, bar codes and contactless capability
- DoD's solution to the new federal credential

The next-generation CAC is safer than ever:

- Used for identification purposes when entering federal buildings and controlled spaces
- Improved vetting and background check requirements
- Meets or exceeds requirements of all applicable privacy laws
- Electronic authentication to gain physical and logical access improves security
- The next-generation CAC can be used with complete confidence to:
 - Log on securely to DoD networks, systems and Web sites
 - Access public key infrastructure (PKI)-compliant systems
 - Encrypt and electronically "sign" e-mails and documents

Whether you are getting a CAC for the first time or renewing your current CAC, the same process is required for the next-generation CAC. Please note that you do not need to replace your CAC until your current card expires.

Renew your CAC in three easy steps.

1. Meet all Defense Enrollment Eligibility Reporting System (DEERS) requirements.

To receive a next-generation CAC, all eligible personnel must be entered into DEERS. To establish a DEERS record, all personnel must undergo proper identity vetting.

A next-generation CAC can only be issued once:

- A Federal Bureau of Investigation (FBI) fingerprints check has been completed and approved
- A National Agency Check with Inquiries (NACI)* background security check is in the process of being completed

*Note: Since the NACI process can take up to 18 months, an individual may be issued a CAC before the process is completed. However, if the NACI process is completed and a person does not get "cleared," his or her CAC will then be revoked.

2. Meet all Real-Time Automated Personnel Identification System (RAPIDS) requirements.

Required RAPIDS documentation and information for active duty military personnel, Selected Reserve, DoD civilian employees, eligible contractor personnel, eligible federal personnel, and other DoD-sponsored eligible populations:

- Two Forms of ID. Both IDs must be among those listed on the I-9 Form (available from www.cac.mil). One must bear a photo (e.g., passport, driver's license). A current/unexpired CAC is considered a valid form of ID.
- A six (6) to eight (8) digit number to use as a personal identification number (PIN). All personnel will be asked to create a PIN that can be easily remembered. Please do not use easily traced numbers such as part of your Social Security number (SSN), birthday, anniversary date, telephone number or address.

3. Visit any of the 1,500+ RAPIDS centers worldwide to obtain your next-generation CAC.

Remember, you will only receive a CAC, if your DEERS account is vetted AND you have all required documentation and information. To locate a RAPIDS center near you, please visit the RAPIDS site locator at www.dmdc.osd.mil/rsl/owa/home.

Note: If you encounter a problem obtaining your next-generation card at the RAPIDS center, and the problem is related to vetting, please follow up with your personnel security representative to update your DEERS profile.

NSIPS Enhancements Help Navy's Aspiring Healthcare Professionals Receive Faster, More Accurate Financial Benefits

By Deborah Gonzales

Thanks to new functionality in the Navy's largest pay and personnel system, medical, dental, optometry, physician assistant, podiatry and nursing students are receiving faster, more accurate reimbursements and tuition payments as part of their Navy scholarship benefits. In addition, the new functionality has boosted the efficiency of participant tracking and communication for managers of the scholarship programs.

Enhancements to the Navy Standard Integrated Personnel System (NSIPS) have provided the Navy Medicine Manpower, Personnel, Training and Education (NAVMED MPT&E) Medical Accessions Department (NMAD) with efficient tools to manage personnel, tuition payments, reimbursements, incentive payments, logistics and training data for more than 1,700 Navy Reservists enrolled in its Health Professions Incentives Programs (HPIP).

Another improvement is the Navy's ability to report core strength and demographic data required by Congress for the military's Medical Accessions programs.

Personnel with the Space and Naval Warfare Systems Center (SSC) Atlantic New Orleans Office, which provides a complete range of life cycle support, engineering, and maintenance services for NSIPS, deployed the functionality in June 2008 in response to NMAD's requirement for a more efficient and accurate system to manage HPIP data and to administer the \$100 million doled out annually in stipends, bonuses, tuition payments, reimbursements, and active duty annual training pay and entitlements.

Also required was a system that could

interface with multiple Reserve and active duty systems to initiate, pay and track appropriate entitlements.

The goal of the development effort, said Edura Baham, SSC Atlantic's NSIPS project director, was to provide a standardized and integrated field-level data collection system for entering and tracking HPIP data for Navy personnel, leveraging the existing data, hardware and network infrastructure of NSIPS, which is based on PeopleSoft commercial software and an Oracle database.

"Minimum customization kept development costs in check," said Baham, who was the NSIPS deputy program manager during HPIP development.

The new component of NSIPS provides a Web-based system that is the single point of entry for information pertaining to HPIP-related pay and personnel data by support staff at the NAVMED MPT&E in Bethesda, Md.

With the critical first-year milestone now past, the system is receiving high marks from the staff who work with students and universities as they administer the scholarship programs.

Dr. Sandra Yerkes, NAVMED Accessions program manager, also gives the system a thumbs up. "The systems engineers who worked with us were exceptionally receptive to our needs and ideas for improved connectivity with existing Reserve and financial data systems, as well as with the individual scholarship participants," Yerkes said. "The new NSIPS mod-

ules and functionalities have significantly enhanced our tracking and communication abilities."

The new NSIPS functionality replaced a legacy system that lacked the modern, robust features needed to support NMAD staff and HPIP participants.

Initially developed and deployed in 1996 by the former SSC New Orleans, the Reserve Standard Training, Administration and Readiness Support - Health Professions (RSTARS-HP) application was a successful PC-based application that authorized payment for stipends, bonuses, reimbursements and annual training entitlements for qualified Navy health professional students.

Prior to the deployment of RSTARS-HP, the application process was manual and took up to six weeks. RSTARS-HP allowed staff to enter payment data, which was uploaded to the Reserve Headquarters Support (RHS) system and then processed through an interface to the Defense Joint Military Pay System-Reserve Component (DJMS-RC), the system used by the Defense Finance and Accounting Service to issue payments.

As technology changed, RSTARS-HP became more costly to maintain and would have required significant investments to upgrade operating systems, databases and hardware, and to comply with new security mandates and pay for scholarship benefit expansion.

In 2007, NAVMED MPT&E received permission and funding to migrate the lega-

NAVMED MPT&E Medical Accessions Department staff members discuss the new Health Professions Incentives Programs (HPIP) functionality that is now part of the Navy Standard Integrated Personnel System (NSIPS). Standing from left are Hospital Corpsman Chief Michael McGovern, Dr. Sandra Yerkes, HM3 Crystal Copeland, Garcia Elliott, Frances Smith and Yeoman 3rd Class Zoe Hepler. Seated is Sean Hughes. Photo by HM1 James Royal, Navy Medicine Support Command.



cy system's functionality to NSIPS, a logical choice since the system contains many functions that RSTARS-HP users required, including the ability to process personnel gains and losses, enter personnel data and record annual training.

"NSIPS was a feasible migration path forward as it provided the flexibility to add the existing RSTARS-HP functionality while leveraging its existing interfaces with personnel and pay-related systems and the ability to add new ones," said Catherine Folse, former NSIPS HPIP project manager, who spearheaded development.

NSIPS already interfaced with DJMS-RC, eliminating the need to route pay-related transactions through RHS, although the interface required some modification.

Only two new interfaces were needed. One interface was with the Inactive Manpower and Personnel Management Information System (IMAPMIS), needed for personnel-related transactions. IMAPMIS maintains personnel master records for members of the Selected Reserve (SELRES), Individual Ready Reserve (IRR), Standby Reserve, and all retired U.S. Navy and U.S. Navy Reserve personnel. The system also supports IRR mobilization and personnel data reporting.

Also required was an interface with the Navy Reserve Order Writing System (NROWS) to ensure timely issuance of annual training payments to HPIP participants.

Despite some challenges, including conversion of data not resident in the legacy system and configuration of data to align with the NSIPS drop-down menu structure, the NSIPS team completed the development and migration project in only nine months, meeting the customer's requirements on time and within budget.

"NSIPS provided the HPIP staff with a comprehensive system to receive timely and accurate personnel and pay-related data to not only manage HPIP personnel but to report on them using the robust ad hoc reporting capability inherent to NSIPS," Folse said.

Baham credits Folse and her team's close coordination and partnership with the customer as a major factor in the successful delivery. "We viewed this project totally from the customer's perspective and really worked hard to listen and understand their requirements and maintain regular communication," Baham said.

The HPIP component of NSIPS has vastly improved data reliability and accuracy, as well as the accuracy and speed of payments. Previously, numerous manual transactions were required in the HPIP payment process, which frequently caused errors that delayed or generated incorrect deposits to bank accounts.

Now, it is entirely possible for students to begin receiving payments within a few days of their gain in the system, said Lt. Elijah Sanders, current NSIPS HPIP project manager.

In addition, NMAD staff have complete visibility of student data, university information and tuition payments, and can track and run reports on all types of financial data, including reimbursable expenses for items such as stethoscopes, lab coats and goggles.

Business intelligence tools embedded in the analytics portion of NSIPS will provide trend analysis and other forward-leaning capabilities to NMAD staff in the future, Baham added.

Programs supported under the HPIP umbrella include the Health Professions Scholarship Program (HPSP), Navy Active Duty Delay for Specialists (NADDS), the Financial Assistance Program (FAP) and Nurse Candidate Program (NCP).

Qualified applicants are recruited, appointed and remunerated in exchange for an active duty obligation after graduation, ensuring the availability of appropriately trained health professionals to meet Navy Medicine's mission-essential requirements.

HPSP is an IRR program created to obtain adequate numbers of commissioned officers on active duty who are qualified in the various health professions. The program is the primary source for the Navy's core medical pool, supplying 80 percent of physicians and 75 percent of dentists.

HPSP provides full tuition, stipend and equipment, and book reimbursement to students pursuing training or doctoral degrees in medicine, dentistry, osteopathy, podiatry and optometry, or master's degrees as physician assistants. Each student is also entitled to 45 days of annual training for each year of scholarship.

In return for the scholarship benefit, students fulfill a minimum three-year commitment as active duty medical, dental or Medical Service Corps officers.

NADDS supports former HPSP students who have been granted a delay in going

on active duty to complete residency training.

The FAP is an IRR program for physicians and dentists currently accepted to or enrolled in an accredited residency or fellowship program progressing toward a degree in a specialty designated as critical to the Department of Defense.

FAP participants receive a monthly stipend, yearly grant, paid tuition and supplies, in addition to 14 days of annual training per year. In exchange, FAP participants agree to serve on active duty for a set number of years with a minimum two years as active duty Medical or Dental Corps officers.

The Nurse Candidate Program provides financial assistance to students who are within 24 months of completing an accredited baccalaureate degree in nursing. Students receive monthly stipends and a signing bonus. After graduation, NCP participants join the Navy Nurse Corps as officers and must complete an active duty service obligation.

These healthcare education incentive programs currently serve participants enrolled in more than 160 institutions scattered across the United States and Puerto Rico. Most participants have no prior naval service and are enrolled in private healthcare education institutions.

The Navy Health Professions Incentives Programs offer attractive incentives, including sign-on bonuses, to help with the extremely high costs of medical education, enabling students to leave school with minimal debt.

SSC Atlantic New Orleans Office provides various products and services for NSIPS and its HPIP modules as the technical agent for the PMW 240 Sea Warrior program, a component of the Naval Program Executive Office for Enterprise Information Systems (PEO EIS).

Support includes software development and sustainment; systems engineering; project management; risk management; installation support; software changes; and customer support center and help desk services.

For more information about Navy Medicine, go to www.med.navy.mil. **CHIPS**

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



I am a frustrated Dick Tracy fan. I have been waiting for my two-way TV wristwatch since 1964. The best anyone has come up with is a cell phone that will show a picture of the person calling and then only if users upload photos and associate their contacts in advance.

The "Star Wars" trilogy introduced the idea of three-dimensional holographic images for communications in the "The Empire Strikes Back" in 1980, but 3-D images are still not available for home, vehicle or desktop use today.

In short, despite the fact that we may have the technology to do so, we have not created practical versions of all the wonderful toys we have seen in movies over the last 50 years. In this issue, we will look at one offshoot of these technologies: desktop video teleconferencing. Yes, we have the technology, but a VTC is still a long way from becoming a ubiquitous replacement for voice or text-only communications for both technical and cognitive reasons.

TALKING PICTURES

Humans communicate most effectively face-to-face. There is always a certain amount of information lost when we communicate over a distance. Text conveys our words but not voice inflection, tone, timbre or pitch. Radios and telephones can recreate some, but not all of the aural signal.

The advent of television brought the first technologies that transmitted both real-time moving images and speech electronically. The earliest attempts at video teleconferencing used closed-circuit analog television systems connected by cable. Broadcast technologies soon advanced, and television signals via radio waves were transmitted over greater distances including, most famously, the live broadcast of Neil Armstrong walking on the moon in 1969.

But transmitting signals via analog waveforms was an inefficient and expensive way to hold a long-distance chat, particularly because of poor video quality, a need for a van full of equipment, and satellite capability to communicate over the horizon. Another limiting factor during the initial development period in the 1970s was a lack of an efficient video compression capability. That meant videophones, primarily the AT&T Picturephone, required a lot of bandwidth and bit transmission relative to the networks available.

The emergence of the integrated services digital network (ISDN) and better video compression technologies in the 1980s

made it possible for video teleconferencing to be more efficient and economical. The expansion of digital VTC systems coincided with the worldwide expansion of ISDN networks. While the first digital systems consisted of expensive proprietary technology, during the 1990s, Internet Protocol, more efficient video compression, and emerging international standards facilitated a migration toward standards-based systems. While most higher quality VTC installations currently follow the conference room model, there are a variety of Internet and Web-based technologies, like small universal serial bus (USB) cameras, and software, like Yahoo! Messenger and MSN Messenger, that give users inexpensive, though low-quality, desktop VTC.

A typical desktop VTC setup includes the following components: video camera; video display; one or more microphones for audio input; one or more speakers for audio output; video and audio processing capability in the desktop PC, either hardware (dedicated device/card) or software; and a data connection to a telephone or data network.

Desktop VTC systems generally follow one of two international standards. The International Telecommunication Union (ITU) standard H.323 defines audio-visual communication sessions on packet networks. The other, slightly newer standard for desktop VTC, is the Internet Engineering Task Force Session Initiation Protocol (SIP), a signaling protocol used to control multimedia communication sessions that include voice and video calls over IP. Both standards are proven and widely implemented. The main difference between the two is that SIP offers more options for multiple media streams such as converged voice, video, chat, presentation and multi-party connections.

So, we have a wide variety of available desktop VTC platforms, some of which come with everything you need to hold video teleconferences right out of the box. And yet, I realized while preparing for this article that I have never placed a single video call. Not one. Zip. Nada. Zilch.

Since I do not consider myself a Luddite when it comes to IT that led to a little self-reflection on why I have never used a desktop VTC.

TO VTC OR NOT TO VTC?

Why do I keep phoning or e-mailing people when I could try a VTC? Well, if I want an immediate answer I stand a better chance by phoning rather than finding someone at a computer with video chat software running. Because my smiling face probably does not add much to what I want to discuss, using speed dial to have the cellular phone network track someone down is a much more convenient way of communicating.

If the receiver is not available, it will only take me longer to find that out going through the VTC interface. (I am a Lazy Person, after all.) If I want to make sure a receiver gets my message in a more permanent form, e-mail will lay in wait until it is checked, at which point the system will obligingly display my message (and send me a read receipt if I want delivery confirmation).

In addition to the synchronous communication issues outlined, unless you have a recorder running, VTC is not a persistent medium.

Essentially, habit and convenience keep me from trying to video call everyone I know. Most of the people I know have a phone and e-mail, but virtually none use desktop VTC. There is no critical mass of users to work with. Until use of VTC software



starts spreading through my network of friends like Facebook has, and it can be used on smartphones, I will never get in the habit of using it.

That leads to a second consideration: What would desktop video teleconferencing give me that a phone conversation or e-mail does not? I can think of two things, though one that initially looks like a positive comes with an interesting side issue that could count as a negative with many people.

The first and most obvious advantage is that you can see the person you are talking with. We humans are social creatures and, as I mentioned earlier, we lose a lot of the nuances of communication without visual attention. Seeing the other person (or people) generally gives us a sense of personal security about whom we are dealing with.

Second, a VTC is not always just about having a picturephone conversation. Good VTC software can also allow for collaborative work on documents.

THE PARALLAX VIEW

Now, however, to the side issue: eye contact. Or more specifically, the lack of true eye contact in videoconferencing. When humans communicate face-to-face, we tend to watch one of two body parts: eyes or mouths. Eye contact establishes a very primal connection, while people who watch mouths may depend on it to identify who is talking. But even a mouth-watcher is aware of how the other person's eyes are moving.

And herein is the problem with desktop VTC: no meaningful eye contact occurs. To do that, we would have to look directly into the camera. Unfortunately, if the camera is anywhere besides dead center in the video picture of the person we are talking to, the image on the monitors will be looking above or below, and because we are looking at the camera we will not see the participants looking at us.

The farther away from the camera, the less parallax (displacement or difference of orientation) you experience. While parallax can be very useful for calculating the distance to an object based on the angle of inclination and distance separating origin points between two lines of sight, it is disconcerting for humans when we cannot make eye contact even periodically during a conversation. And that is likely another reason that desktop VTC has not quite caught on: We do not have similar cognitive expectations when using e-mail or a phone, therefore they remain more comfortable to use.

Full-size conference room setups reduce the parallax effect because the camera is farther away from us, but the next time you are in a VTC, see if you really can make eye contact with someone on the other side of the camera.

TECHNICAL REQUIREMENTS

Now that we have looked at the whys and wherefores of desktop VTC, let's take a quick look under the hood.

While early desktop videoconferencing solutions required the use of custom equipment, a modern desktop VTC can run

on most desktop PCs or notebooks with either a built-in or USB webcam.

However, enterprise-level network-based desktop VTC solutions may require the use of some additional hardware or software components. For example, multi-point sessions that include more than two participating clients generally require a video bridge.

If your enterprise VTC system is going to communicate with other enterprise VTC systems, you may need a dedicated gateway for connectivity and gatekeeper software to control call admission and track usage. You will also likely need dedicated firewalls and servers for streaming or recording transmissions. In particular, if we expect to successfully host network-based desktop VTC traffic, we really need a solid understanding of just what type and size of infrastructure is required to make it work.

First and foremost, VTC traffic can consume a significant amount of bandwidth. While modern video compression techniques have reduced the bandwidth required for videoconferencing, a good quality desktop VTC call (about 15 frames per second) still requires about 500 kbps of bandwidth per participant.

A high-definition VTC call (about 24 frames per second) will likely require at least 1 Mbps per client (which is why most conference room setups use a primary rate interface connection operating at T1 speeds).

In addition, conducting a VTC over a network will require the ability to adjust network bandwidth utilization in real time to adapt to changing usage.

Second, while other popular networked applications, like e-mail, file services or Web browsing, send and receive traffic in bursts of data, VTC network traffic is usually a constant stream of data that more closely resembles circuit-switched operations than packet-switched. Any significant latency (taking more than 100 milliseconds to deliver a packet) and jitter (the variation in the time between packets arriving) will have a negative impact on the quality of the transmission.

A large part of providing an acceptable quality of service rests with managing network bandwidth. Time-sensitive, rich-media applications, like videoconferencing, require dedicated bandwidth provided by call admission control; setting and enforcing bandwidth usage limits for each user and location; and having some way to adapt on-the-fly to changing network conditions.

On a smaller scale, you can see this with home VTC usage. My home Internet connection is a DSL that maxes out at around 780 kbps (about half of a T1 line) and usually runs at speeds between 300 kbps and 550 kbps. The desktop VTC applications on home computers and laptops can allegedly run with 128 kbps of bandwidth, as will (in theory) most of the online computer or console games we play.

But I can tell you from personal experience that one teenager watching YouTube combined with another teenager trying to do video chat over our relatively unmanaged wireless router and default firewall will bring each other's applications to a crawl. And the lag generated by the low quality video chat application hogging the connection will also get you "killed" repeatedly while playing something like Halo or Call of Duty online.





So, regardless of whether we want to video teleconference from home or at an enterprise level, we need to engineer our packet networks for high throughput, low latency and low packet loss. A network-based VTC call will not be a fun or satisfying experience if late or lost packets result in the signal looking worse than the video quality of the "Blair Witch Project."

I want a nice, clear, high definition signal so I can at least try to see the other person's eyes.

Finally, there are security issues, particularly at the enterprise level. Standard H.323-based videoconferencing, in particular, uses a large number of network ports across a wide range, and complicating matters further, the ports used will vary almost with every call.

On the one hand, most desktop video conferencing systems include some form of firewall traversal capability that allows traffic to pass through the firewall without the need to change firewall rules or settings, enabling fairly seamless communications and reducing the burden on network administrators.

Then again, this means a lot of bits and bytes will be passing through the firewall without much adult supervision, thus making network security folks just that much more anxious.

CONCLUSIONS

Maybe I am a Luddite, because despite my desire for that Dick Tracy two-way TV wristwatch, I just do not have a great burning desire to do much more than pick up the phone or send an e-mail. Yes, there are times where we can use a VTC to hold a big meeting with participants in lots of different places and save the cost and carbon footprint of all those airline tickets, but only with a high-quality dedicated VTC system. Desktop VTC is still just a bit quirky for me.

But even if someone solves the parallax issue, as, for example, Microsoft is attempting with its GazeMaster project, and we get desktop VTC software that can display multiple callers simultaneously, and there is enough network capacity available that we do not throttle the rest of our users into a network breakdown, is it really worth the extra expense just so I can see a moving picture of who I am talking to?

Maybe. And definitely, if it can work on my wristwatch. CHIPS

HAPPY NETWORKING!

Long is a retired Air Force communications officer who has written for CHIPS since 1993. He holds a Master of Science degree in information resources management from the Air Force Institute of Technology. He currently serves as a telecommunications manager in the Department of Homeland Security.

Iraqi Government Begins Management of High Frequency Radio Band

The Government of Iraq (GoI) began managing the high frequency radio band throughout the country in October '09

By Multi-National Force-Iraq Public Affairs

Multi-National Force-Iraq turned over responsibility for management of the high frequency radio band to the Government of Iraq after a months-long process that included training, fielding management systems and development of Iraqi procedures for utilization of the electromagnetic spectrum.

In accordance with the Security Agreement, both parties formed the Frequency Management Joint Sub-Committee in January 2009 to address any issues regarding frequency management.

Dr. Hiyam Al Yassiri, of the Ministry of Communications, and Rear Adm. David Simpson, Deputy Chief of Staff, Communications and Information Systems (CJ6), Multi-National Force-Iraq, co-chairman of the sub-committee, oversaw the development of Iraqi spectrum management capacity to allow the transition of the high frequency (HF) band to the Iraqi Government.

The sub-committee will continue to work together to develop an Iraqi process for each successive band. Each band has very different commercial, government and security uses and will need different procedures to accommodate all of the Iraqi user groups. The sub-committee is now working on the transition of both the very high frequency (VHF) and ultra high frequency (UHF) bands with the ultimate goal of turning over management responsibilities for all frequencies to the GoI.

In May 2009, U.S. forces conducted frequency management training for GoI personnel in various ministries. The purpose of the training was to establish a cadre of individuals capable of staffing a Communications and Media Commission and for Ministries that depend on radio frequencies as a critical resource. The training produced GoI staff capable of training and certifying future spectrum and frequency managers.

"The radio spectrum is a limited natural resource for every nation. Governments must balance domestic needs and international responsibilities as they manage their spectrum resources. The demand for radio frequency use is on the rise and will continue to grow in the foreseeable future. Iraq's Communications and Media Commission and Ministry of Communications are committed to preserving the equities of Iraqi citizens," Simpson said.

"This talented Government of Iraq team of engineers, technicians and managers are ready to serve Iraq as stewards of the [Iraqi] nation's spectrum resources consistent with international treaty obligations and with due regard for the rights of neighboring nations." CHIPS

For more information about Multi-National Force-Iraq, visit WWW.MNF-IRAQ.COM or contact the public affairs office at MNFI PRESSDESK@iraq.centcom.mil.



Enterprise Software Agreements

The **Enterprise Software Initiative (ESI)** is a Department of Defense (DoD) initiative to streamline the acquisition process and provide best-priced, standards-compliant information technology (IT). The ESI is a business discipline used to coordinate multiple IT investments and leverage the buying power of the government for commercial IT products and services. By consolidating IT requirements and negotiating Enterprise Agreements with software vendors, the DoD realizes significant Total Cost of Ownership (TCO) savings in IT acquisition and maintenance. The goal is to develop and implement a process to identify, acquire, distribute and manage IT from the enterprise level.

Additionally, the ESI was incorporated into the Defense Federal Acquisition Regulation Supplement (DFARS) Section 208.74 on Oct. 25, 2002, and DoD Instruction 5000.2 on May 12, 2003.

Unless otherwise stated authorized ESI users include all DoD components, and their employees including Reserve component (Guard and Reserve) and the U.S. Coast Guard mobilized or attached to DoD; other government employees assigned to and working with DoD; nonappropriated funds instrumentalities such as NAFI employees; Intelligence Community (IC) covered organizations to include all DoD Intel System member organizations and employees, but not the CIA, nor other IC employees, unless they are assigned to and working with DoD organizations; DoD contractors authorized in accordance with the FAR; and authorized Foreign Military Sales.

For more information on the ESI or to obtain product information, visit the ESI Web site at <http://www.esi.mil/>.

Software Categories for ESI:

Asset Discovery Tools

Belarc

BelManage Asset Management – Provides software, maintenance and services.

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

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

Ordering Expires: 30 Sep 11

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

BMC

Remedy Asset Management – Provides software, maintenance and services.

Contractor: *BMC Software Inc.* (W91QUZ-07-A-0006)

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

Ordering Expires: 29 Jan 10 (Please call for extension information.)

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

Carahsoft

Opware Asset Management – Provides software, maintenance and services.

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

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

Ordering Expires: 18 May 10

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

DLT

BDNA Asset Management – Provides asset management software, maintenance and services.

Contractor: *DLT Solutions Inc.* (W91QUZ-07-A-0002)

Authorized Users: This BPA has been designated as a GSA Smart-BUY and is open for ordering by all Department of Defense (DoD) components, authorized contractors and all federal agencies.

Ordering Expires: 01 Apr 13

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

Patriot

BigFix Asset Management – Provides software, maintenance and services.

Contractor: *Patriot Technologies Inc.* (W91QUZ-07-A-0003)

Authorized Users: This BPA has been designated as a GSA Smart-BUY and is open for ordering by all Department of Defense (DoD) components, authorized contractors and all federal agencies.

Ordering Expires: 08 Sep 12

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

Business and Modeling Tools

BPWin/ERWin

BPWin/ERWin – Provides products, upgrades and warranty for ERWin, a data modeling solution that creates and maintains databases, data warehouses and enterprise data resource models. It also provides BPWin, a modeling tool used to analyze, document and improve complex business processes.

Contractor: *Computer Associates International, Inc.* (W91QUZ-04-A-0002); (813) 612-7352

Ordering Expires: Upon depletion of Computer Hardware, Enterprise Software and Solutions (CHES) inventory.

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

Business Intelligence

Business Objects

Business Objects – Provides software licenses and support for Business Objects, Crystal Reports, Crystal Enterprise and training and professional services. Volume discounts range from 5 to 20 percent for purchases of software licenses under a single delivery order.

Contractor: *EC America, Inc.* (SP4700-05-A-0003)

Ordering Expires: 04 May 10

Web Link: <http://www.gsawebblink.com/esi-dod/boa/>

www.it-umbrella.navy.mil

Database Management Tools

Microsoft Products

Microsoft Database Products – See information under Office Systems on page 49.

Oracle (DEAL-O)

Oracle Products – Provides Oracle database and application software licenses, support, training and consulting services. The Navy Enterprise License Agreement is for database licenses for Navy customers. Contact the Navy project manager.

Contractors:

Oracle Corp. (W91QUZ-07-A-0001); (703) 364-3351

DLT Solutions (W91QUZ-06-A-0002); (703) 708-9107

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

Small Business; (703) 752-0632

Mythics, Inc. (W91QUZ-06-A-0003); Small Business; (757) 284-6570

TKC Integration Services, LLC (W91QUZ-09-A-0001);

Small Business; (571) 323-5584

Ordering Expires:

Oracle: 30 Sep 11

DLT: 1 Apr 13

immixTechnology: 26 Aug 11

Mythics: 18 Dec 11

TKCIS: 29 Jun 11

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

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

Special Note to Navy Users: See the information provided on page 50 concerning the Navy Oracle Database Enterprise License under Department of the Navy Agreements.

Sybase (DEAL-S)

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

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

Ordering Expires: 15 Jan 13

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

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

Enterprise Application Integration

Sun Software

Sun Products – Provides Sun Java Enterprise System (JES) and Sun StarOffice. Sun JES products supply integration and service-oriented architecture (SOA) software including: Identity Management Suite; Communications Suite;

Availability Suite; Web Infrastructure Suite; MySQL; xVM and Role Manager. Sun StarOffice supplies a full-featured office productivity suite.

Contractors:

Commercial Data Systems, Inc. (N00104-08-A-ZF38); Small Business; (619) 569-9373

Dynamic Systems, Inc. (N00104-08-A-ZF40); Small Business; (801) 444-0008

World Wide Technology, Inc. (N00104-08-A-ZF39); Small Business; (314) 919-1513

Ordering Expires: 24 Sep 12

Web Link:

http://www.it-umbrella.navy.mil/contract/enterprise/application_integration/sun/index.shtml

Enterprise Architecture Tools

IBM Software Products

IBM Software Products – Provides IBM product licenses and maintenance with discounts from 1 to 19 percent off GSA pricing. On June 28, 2006, the IBM Rational Blanket Purchase Agreement (BPA) with immixTechnology was modified to include licenses and Passport Advantage maintenance for IBM products, including: IBM Rational, IBM Database 2 (DB2), IBM Informix, IBM Trivoli, IBM Websphere and Lotus software products.

Contractor: immixTechnology, Inc. (DABL01-03-A-1006); Small Business; (800) 433-5444

Ordering Expires: 31 Jan 10 (Please call for extension information.)

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

Enterprise Management

CA Enterprise Management Software (C-EMS2)

Computer Associates Unicenter Enterprise Management Software – Includes Security Management; Network Management; Event Management; Output Management; Storage Management; Performance Management; Problem Management; Software Delivery; and Asset Management. In addition to these products, there are many optional products, services and training available.

Contractor: Computer Associates International, Inc. (W91QUZ-04-A-0002); (703) 709-4610

Ordering Expires: 22 Sep 12

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

Citrix

Citrix – Provides a full range of Metaframe products including Secure Access Manager, Conferencing Manager, Password Manager, Access Suite & XP Presentation Server. Discounts range from 2 to 5 percent off GSA schedule pricing plus spot discounts for volume purchases.

Contractor: Citrix Systems, Inc. (W91QUZ-04-A-0001); (772) 221-8606

Ordering Expires: 31 Jan 10 (Please call for extension information.)

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

Microsoft Premier Support Services (MPS-2)

Microsoft Premier Support Services – Provides premier support packages to small and large-size organizations. The products include Technical Account Managers, Alliance Support Teams, Reactive Incidents, on-site support, Technet and MSDN subscriptions.

Contractor: Microsoft (W91QUZ-09-D-0038); (980) 776-8413

Ordering Expires: 31 Mar 10 (Please call for extension information.)

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

NetIQ

NetIQ – Provides Net IQ systems management, security management and Web analytics solutions. Products include: AppManager; AppAnalyzer; Mail Marshal; Web Marshal; Vivinet voice and video products; and Vigilant Security and Management products. Discounts are 8 to 10 percent off GSA schedule pricing for products and 5 percent off GSA schedule pricing for maintenance.

Contractors:

NetIQ Corp. (W91QUZ-04-A-0003)

Northrop Grumman – authorized reseller

Federal Technology Solutions, Inc. – authorized reseller

Ordering Expires: 05 May 14

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

Planet Associates

Planet Associates Infrastructure Relationship Management (IRM) Software Products

– Provides software products including licenses, maintenance and training for an enterprise management tool for documenting and visually managing all enterprise assets, critical infrastructure and interconnectivity including the interdependencies between systems, networks, users, locations and services.

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

Ordering Expires: 01 Jun 14

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

Quest Products

Quest Products – Provides Quest software licenses, maintenance, services and training for Active Directory Products, enterprise management, ERP planning support and application and database support. Quest software products have been designated as a DoD ESI and GSA SmartBUY. Only Active Directory Products have been determined to be the best value to the government and; therefore, competition is not required for Active Directory software purchases. Discount range for software is from 3 to 48 percent off GSA pricing. For maintenance, services and training, discount range is 3 to 8 percent off GSA pricing.

Contractors:

Quest Software, Inc. (W91QUZ-05-A-0023); (301) 820-4800

DLT Solutions (W91QUZ-06-A-0004); (703) 708-9127

Ordering Expires:

Quest: 30 Sep 10

DLT: 01 Apr 13

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

Enterprise Resource Planning

Oracle

Oracle – See information provided under Database Management Tools on page 46.

RWD Technologies

RWD Technologies – Provides a broad range of integrated software products designed to improve the productivity and effectiveness of end users in complex operating environments. RWD's Info Pak products allow you to easily create, distribute and maintain professional training documents and online help for any computer application. RWD Info Pak products include Publisher, Administrator, Simulator and OmniHelp. Training and other services are also available.

Contractor: RWD Technologies (N00104-06-A-ZF37); (410) 869-3014

Ordering Expires: Effective for term of the GSA FSS Schedule

Web Link: www.it-umbrella.navy.mil/contract/enterprise/erp_software/rwd/rwd.shtml

SAP

SAP Products – Provides software licenses, software maintenance support, information technology professional services and software training services.

Contractors:

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

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

Carahsoft Technology Corporation (N00104-08-A-ZF43); Small Business; (703) 871-8583

Oakland Consulting Group (N00104-08-A-ZF44); Small Business; (301) 577-4111

Ordering Expires: 14 Sep 13

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/erp_software/sap_products/sap_hdr.shtml

Information Assurance Tools

Data at Rest Solutions BPAs offered through ESI/SmartBUY

The Office of Management and Budget, Defense Department and General Services Administration awarded multiple contracts for blanket purchase agreements (BPA) to protect sensitive, unclassified data residing on government laptops, other mobile computing devices and removable storage media devices.

These competitively awarded BPAs provide three categories of software and hardware encryption products — full disk encryption (FDE), file encryption (FES) and integrated FDE/FES products. All products use cryptographic modules validated under FIPS 140-2 security requirements and have met stringent technical and interoperability requirements.

Licenses are transferable within a federal agency and include secondary use rights. All awarded BPA prices are as low as or lower than the prices each vendor has available on GSA schedules. The federal government anticipates significant savings through these BPAs. The BPAs were awarded under both the DoD's Enterprise Software Initiative (ESI) and GSA's governmentwide SmartBUY programs, making them available to all U.S. executive agencies, independent establishments, DoD components, NATO, state and local agencies, Foreign Military Sales (FMS) with written authorization, and contractors authorized to order in accordance with the FAR Part 51.

Service component chief information officers (CIO) are developing component service-specific enterprise strategies. Accordingly, customers should check with their CIO for component-specific policies and strategies before procuring a DAR solution. The Department of the Navy and Army released service-specific DAR guidance for their personnel to follow. Go to the ESI Web site at www.esi.mil for more information.

The DON CIO issued an enterprise solution for Navy users purchasing DAR software. See the information provided on page 50 under Department of the Navy Agreements. The Department of the Army issued an enterprise solution for Army users purchasing DAR software. See the information provided on the Army CHES Web site at [https://chess.army.mil/ascp/commerce/contract/FA8771-07-A-0301_bpaorderinginstructions\(2\)_ARMY.jsp](https://chess.army.mil/ascp/commerce/contract/FA8771-07-A-0301_bpaorderinginstructions(2)_ARMY.jsp).

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

Mobile Armor – MTM Technologies, Inc. (FA8771-07-A-0301)

Safeboot/McAfee – Rocky Mountain Ram (FA8771-07-A-0302)

Information Security Corp. – Carahsoft Technology Corp. (FA8771-07-A-0303)

Safeboot/McAfee – Spectrum Systems (FA8771-07-A-0304)

SafeNet, Inc. – SafeNet, Inc. (FA8771-07-A-0305)

Encryption Solutions, Inc. – Hi Tech Services, Inc. (FA8771-07-A-0306)

Pointsec/Checkpoint – immix Technologies (FA8771-07-A-0307)

SPYRUS, Inc. – Autonomic Resources, LLC (FA8771-07-A-0308)

CREDANT Technologies – GTSI Corp. – (FA8771-07-A-0309)

WinMagic, Inc. – Govbuys, Inc. (FA8771-07-A-0310)

CREDANT Technologies – Intelligent Decisions (FA8771-07-A-0311)

GuardianEdge Technologies – Merlin International (FA8771-07-A-0312)

Ordering Expires: 14 Jun 12 (If extended by option exercise.)

Web Link: <http://www.esi.mil>

McAfee

McAfee – Provides software and services in the following areas: Anti-Virus; E-Business Server; ePolicy Orchestrator; GroupShield Services; IntruShield; Secure Messaging Gateway and Web Gateway.

Contractor: *En Pointe* (GS-35F-0372N)

Ordering Expires: 16 Sep 10 (Please call for extension information.)

Web Link: <http://www.esi.mil>

Antivirus Web Links: Antivirus software available at no cost; download includes McAfee, Symantec and Trend Micro Products. These products can be downloaded by linking to either of the following Web sites:

NIPRNET site: https://www.jtfgno.mil/antivirus/antivirus_index.htm

SIPRNET site: https://www.cert.smil.mil/antivirus/av_info.htm

Securify

Securify – Provides policy-driven appliances for network security that are designed to validate and enforce intended use of networks and applications; protects against all risks and saves costs on network and security operations. Securify integrates application layer seven traffic analysis with signatures and vulnerability scanning in order to discover network behavior. It provides highly accurate, real-time threat mitigation for both known and unknown threats and offers true compliance tracking.

Contractor: *Patriot Technologies, Inc.* (FA8771-06-A-0303)

Ordering Expires: 04 Jan 11 (If extended by option exercise)

Web Link: <http://www.esi.mil>

Symantec

Symantec – Symantec products can be divided into 10 main categories that fall under the broad definition of Information Assurance. These categories are: virus protection; anti-spam; content filtering; anti-spyware solutions; intrusion protection; firewalls/VPN; integrated security; security management; vulnerability management; and policy compliance. This BPA provides the full line of Symantec Corp. products and services consisting of more than 6,000 line items including Ghost and Brightmail. It also includes Symantec Antivirus products such as Symantec Client Security; Norton Antivirus for Macintosh; Symantec System Center; Symantec AntiVirus/Filtering for Domino; Symantec AntiVirus/Filtering for MS Exchange; Symantec AntiVirus Scan Engine; Symantec AntiVirus Command Line Scanner; Symantec for Personal Electronic Devices; Symantec AntiVirus for SMTP Gateway; Symantec Web Security; and support.

Contractor: *immixGroup* (FA8771-05-0301)

Ordering Expires: 12 Sep 10

Web Link: <http://var.immixgroup.com/contracts/overview.cfm> or www.esi.mil

Notice to DoD customers regarding Symantec Antivirus Products: A fully funded and centrally purchased DoD enterprise-wide antivirus and spyware software license is available for download to all Department of Defense (DoD) users who have a .mil Internet Protocol (IP) address.

Contractor: *TVAR Solutions, Inc.*

Antivirus Web Links: Antivirus software can be downloaded at no cost by linking to either of the following Web sites:

NIPRNET site: https://www.jtfgno.mil/antivirus/antivirus_index.htm

SIPRNET site: http://www.cert.smil.mil/antivirus/av_info.htm

Websense (WFT)

Websense – Provides software and maintenance for Web filtering products.

Contractor: *Patriot Technologies* (W91QUZ-06-A-0005)

Authorized Users: This BPA is open for ordering by all DoD components and authorized contractors.

Ordering Expires: 31 Aug 11

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

Xacta

Xacta – Provides Web Certification and Accreditation (C&A) software products, consulting support and enterprise messaging management solutions through its Automated Message Handling System (AMHS) product. The software simplifies C&A and reduces its costs by guiding users through a step-by-step process to determine risk posture and assess system and network configuration compliance with applicable regulations, standards and industry best practices, in accordance with the DITSCAP, NIACAP, NIST or DCID processes. Xacta's AMHS provides automated, Web-based distribution and management of messaging across your enterprise.

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

Ordering Expires: 24 Sep 14

Web Link: <http://esi.telos.com/contract/overview>

Lean Six Sigma Tools

iGrafx Business Process Analysis Tools

iGrafx – Provides software licenses, maintenance and media for iGrafx Process for Six Sigma 2007; iGrafx Flowcharter 2007; Enterprise Central; and Enterprise Modeler.

Contractors:

Softchoice Corporation (N00104-09-A-ZF34); (416) 588-9002 ext. 2072

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

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

Authorized Users: These BPAs are co-branded ESI/GSA SmartBUY BPAs and are open for ordering by all Department of Defense (DoD) components, U.S. Coast Guard, NATO, Intelligence Community, authorized DoD contractors and all federal agencies.

Ordering Expires: 31 Jan 14

Web Links:

Softchoice

www.it-umbrella.navy.mil/contract/enterprise/igrafx/softchoice/index.shtml

Softmart

www.it-umbrella.navy.mil/contract/enterprise/igrafx/softmart/index.shtml

SHI

www.it-umbrella.navy.mil/contract/enterprise/igrafx/shi/index.shtml

Minitab

Minitab – Provides software licenses, media, training, technical services and maintenance for products including Minitab Statistical Software, Quality Companion and Quality Trainer. It is the responsibility of the ordering officer to ensure compliance with all fiscal laws prior to issuing an order under a BPA, and to ensure that the vendor selected represents the best value for the requirement being ordered (see FAR 8.404).

Contractor: *Minitab, Inc.* (N00104-08-A-ZF30); (800) 448-3555 ext. 311

Authorized Users: This BPA is open for ordering by all Department of Defense (DoD) components, U.S. Coast Guard, NATO, Intelligence Community and authorized DoD contractors.

Ordering Expires: 07 May 13

Web Link: <http://www.it-umbrella.navy.mil/contract/minitab/minitab.shtml>

PowerSteering

PowerSteering – Provides software licenses (subscription and perpetual), media, training, technical services, maintenance, hosting and support for PowerSteering products: Software-as-a-Service solutions to apply the proven discipline of project and portfolio management in IT, Lean Six Sigma, Project Management Office or any other project-intensive area and to improve strategy alignment, resource management, executive visibility and team productivity. It is the responsibility of the ordering officer to ensure compliance with all fiscal laws prior to issuing an order under a BPA, and to ensure that the vendor selected represents the best value for the requirement being ordered (see FAR 8.404).

Contractor: *immixTechnology, Inc.* (N00104-08-A-ZF31); Small Business; (703) 752-0661

Authorized Users: All DoD components, U.S. Coast Guard, NATO, Intelligence Community, and authorized DoD contractors.

Ordering Expires: 14 Aug 13

Web Link: <http://www.it-umbrella.navy.mil/contract/powersteering/powersteering.shtml>

Office Systems

Adobe Desktop Products

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

Contractors:

Dell Marketing L.P. (formerly ASAP) (N00104-08-A-ZF33); (800) 248-2727, ext. 5303

CDW-G (N00104-08-A-ZF34); (703) 621-8211

GovConnection, Inc. (N00104-08-A-ZF35); (301) 340-3861

Insight Public Sector, Inc. (N00104-08-A-ZF36); (301) 261-6970

Ordering Expires: 30 Jun 13

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

Adobe Server Products

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

Contractor:

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

Ordering Expires: 14 Jan 14

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

Microsoft Products

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

Contractors:

CDW-G (N00104-02-A-ZE85); (888) 826-2394

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

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

GTSI (N00104-02-A-ZE79); (800) 999-GTSI ext. 2071

Hewlett-Packard (N00104-02-A-ZE80); (978) 399-9818

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

SHI (N00104-02-A-ZE86); (732) 868-5926

Softchoice (N00104-02-A-ZE81); Large Business; (877) 333-7638

Softmart (N00104-02-A-ZE84); (800) 628-9091 ext. 6928

Ordering Expires: 31 Mar 10

Web Link: <http://www.it-umbrella.navy.mil/contract/enterprise/microsoft/ms-ela.shtml>

Red Hat/Netscape/Firefox

Through negotiations with August Schell Enterprises, DISA has established a DoD-wide enterprise site license whereby DISA can provide ongoing support and maintenance for the Red Hat Security Solution server products that are at the core of the Department of Defense's Public Key Infrastructure (PKI). The Red Hat Security Solution includes the following products: Red Hat Certificate System and dependencies; Red Hat Directory Server; Enterprise Web Server (previously Netscape Enterprise Server); and Red Hat Fortitude Server (replacing Enterprise Server). August Schell also provides a download site that, in addition to the Red Hat products, also allows for downloading DISA-approved versions of the following browser products: Firefox Browser; Netscape Browser; Netscape Communicator; and Personal Security Manager. The Red Hat products and services provided

through the download site are for exclusive use in the following licensed community: (1) All components of the U.S. Department of Defense and supported organizations that utilize the Joint Worldwide Intelligence Communications System, and (2) All non-DoD employees (e.g., contractors, volunteers, allies) on-site at the U.S. Department of Defense and those not on-site but using equipment furnished by the U.S. Department of Defense (GFE) in support of initiatives which are funded by the U.S. Department of Defense.

Licensed software products available through the August Schell contract are for the commercial versions of the Red Hat software, not the segmented versions of the previous Netscape products that are compliant with Global Information Grid (GIG) standards. The segmented versions of the software are required for development and operation of applications associated with the GIG, the Global Command and Control System (GCCS) or the Global Combat Support System (GCSS).

If your intent is to use a Red Hat product to support development or operation of an application associated with the GIG, GCCS or GCSS, you must contact one of the Web sites listed below to obtain the GIG segmented version of the software. You may not use the commercial version available from the August Schell Red Hat download site.

If you are not sure which version (commercial or segmented) to use, we strongly encourage you to refer to the Web sites listed below for additional information to help you to make this determination before you obtain the software from the August Schell Red Hat download site (or contact the project manager).

GIG or GCCS users: Common Operating Environment Home Page
<http://www.disa.mil/gccs-j/index.html>

GCSS users: Global Combat Support System
<http://www.disa.mil/gccsj>

Contractor: **August Schell Enterprises** (www.augustschell.com)

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

Ordering Expires: 14 Mar 10 (Please call for extension information.)
All downloads provided at no cost.

Web Link: <http://iase.disa.mil/netlic.html>

Red Hat Linux

Red Hat Linux – Provides operating system software license subscriptions and services to include installation and consulting support, client-directed engineering and software customization. Red Hat Enterprise Linux is the premier operating system for open source computing. It is sold by annual subscription, runs on seven system architectures and is certified by top enterprise software and hardware vendors.

Contractors:

Carahsoft Technology Corporation (HC1028-09-A-2004)

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

Ordering Expires:

Carahsoft: 09 Feb 14

DLT Solutions, Inc.: 17 Feb 14

Web Link: <http://www.esi.mil>

WinZip

WinZip – This is an IDIQ contract with Eyak Technology, LLC, an "8(a)" Small Disadvantaged Business (SDB)/Alaska Native Corp. for the purchase of WinZip Standard, a compression utility for Windows. Minimum quantity order via delivery order and via Government Purchase Card to Eyak Technology, LLC is 1,250 WinZip licenses.

Contractor: **Eyak Technology, LLC** (W91QUZ-04-D-0010)

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

Ordering Expires: 31 Jan 10 (Please call for new agreement information.)

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

Operating Systems

Apple

Apple – Provides Apple Desktop and Server Software, maintenance, related services and support as well as Apple Perpetual Software licenses. These licenses include Apple OS X Server v10.5; Xsan 2; Apple Remote Desktop 3.2; Aperture 2; Final Cut Express 4; Final Cut Studio 2; iLife '08; iWork '08; Logic Express 8; Logic

Pro 7; Mac OS X v10.5 Leopard; QuickTime 7 Pro Mac; and Shake 4.1 Mac OS X. Software Maintenance, OS X Server Support, AppleCare Support and Technical Service are also available.

Contractor: Apple, Inc. (HC1047-08-A-1011)

Ordering Expires: 10 Sep 11

Web Link: <http://www.esi.mil>

Sun (SSTEW)

SUN Support – Sun Support Total Enterprise Warranty (SSTEW) offers extended warranty, maintenance, education and professional services for all Sun Microsystems products. The maintenance covered in this contract includes flexible and comprehensive hardware and software support ranging from basic to mission critical services. Maintenance covered includes Sun Spectrum Platinum, Gold, Silver, Bronze, hardware only and software only support programs.

Contractor: Dynamic Systems (DCA200-02-A-5011)

Ordering Expires: Dependent on GSA schedule until 2011

Web Link: http://www.disa.mil/contracts/guide/bpa/bpa_sun.html

Research and Advisory BPA

Research and Advisory Services BPAs provide unlimited access to telephone inquiry support, access to research via Web sites and analyst support for the number of users registered. In addition, the services provide independent advice on tactical and strategic IT decisions. Advisory services provide expert advice on a broad range of technical topics and specifically focus on industry and market trends. BPA listed below.

Gartner Group (N00104-07-A-ZF30); (703) 378-5697; Awarded 01 Dec 2006

Ordering Expires: Effective for term of GSA contract

Authorized Users: All DoD components. For the purpose of this agreement, DoD components include: the Office of the Secretary of Defense; U.S. Military Departments; the Chairman of the Joint Chiefs of Staff; Combatant Commands; the Department of Defense Office of Inspector General; Defense Agencies; DoD Field Activities; the U.S. Coast Guard; NATO; the Intelligence Community and Foreign Military Sales with a letter of authorization. This BPA is also open to DoD contractors authorized in accordance with the FAR Part 51.

Web Link: www.it-umbrella.navy.mil/contract/r&a/gartner/gartner.shtml



Department of the Navy Agreements

Oracle (DEAL-O) Database Enterprise License for the Navy

On Oct. 1, 2004 and May 6, 2005, the Navy established the Oracle Database Enterprise License, effective through Sept. 30, 2013. The enterprise license provides Navy shore-based and afloat users, to include active duty, Reserve and civilian billets, as well as contractors who access Navy systems, the right to use Oracle databases for the purpose of supporting Navy internal operations. Navy users in joint commands or supporting joint functions should contact the NAVICP Mechanicsburg contracting officer, at (717) 605-5659 for further review of the requirements and coverage.

This license is managed by the Space and Naval Warfare Systems Center (SPAWARSYSCEN) Pacific DON Information Technology (IT) Umbrella Program Office. The Navy Oracle Database Enterprise License provides significant ben-

efits, including substantial cost avoidance for the department. It facilitates the goal of netcentric operations by allowing authorized users to access Oracle databases for Navy internal operations and permits sharing of authoritative data across the Navy enterprise.

Programs and activities covered by this license agreement shall not enter into separate Oracle database licenses outside this central agreement whenever Oracle is selected as the database. This prohibition includes software and software maintenance that is acquired:

- a. as part of a system or system upgrade, including Application Specific Full Use (ASFU) licenses;
- b. under a service contract;
- c. under a contract or agreement administered by another agency, such as an interagency agreement;
- d. under a Federal Supply Service (FSS) Schedule contract or blanket purchase agreement established in accordance with FAR 8.404(b)(4); or
- e. by a contractor that is authorized to order from a Government supply source pursuant to FAR 51.101.

This policy has been coordinated with the Office of the Assistant Secretary of the Navy (Financial Management and Comptroller), Office of Budget.

Web Link: <http://www.it-umbrella.navy.mil/contract/enterprise/deal/oracle/oracle.shtml>

Data at Rest Solutions BPA - Navy Agreement only

The DON CIO has issued an enterprise solution for Navy users purchasing DAR software. Visit the DON CIO Web site at www.doncio.navy.mil and search for "Data at Rest" to read the new policy. The DON awarded MTM Technologies a BPA for purchase of the DON Mobile Armor software bundle. For Navy users, all purchases of DON enterprise DAR solutions must be executed through the enterprise BPA, which can be found on the DON IT Umbrella Program Web site at www.it-umbrella.navy.mil. Procurement of other DAR solutions for Navy users is prohibited.

Navy Enterprise BPA for DAR Users:

Mobile Armor – MTM Technologies, Inc. (N00104-09-A-ZF30)

Web Link: <http://www.it-umbrella.navy.mil/contract/mtm/mtm.shtml>

Visit our Web sites:

www.it-umbrella.navy.mil

www.itec-direct.navy.mil

www.esi.mil

www.chips.navy.mil

01 01 01 01 01 01 01

Page intentionally left blank

1 01 01 01 01

1 01 01 01

01

A person wearing a white t-shirt and blue jeans is shown from the waist down. A black mobile phone is tucked into the back pocket of the jeans. The phone's screen is lit up and displays a list of text, likely a directory or contact list. The background is a bright, sunny outdoor scene with a road curving into the distance under a blue sky with light clouds.

DON CIO MOBILE

www.dnncio.navy.mil/moalle

DEPARTMENT OF THE NAVY
COMMANDING OFFICER
SPAWARSSYSCOM ATLANTIC
CHIPS MAGAZINE
1458 FOURTH AVE
NORFOLK, VA 23611-2130
OFFICIAL BUSINESS

PERIODICAL POSTAGE AND
FEES PAID NORFOLK, VA AND
ADDITONAL MAILING OFFICE
380 ATLANTIC
CHIPS MAGAZINE
USPS 757 810
ISSN 1047-0982