Sharing Information - Technology - Experience

CHIPS

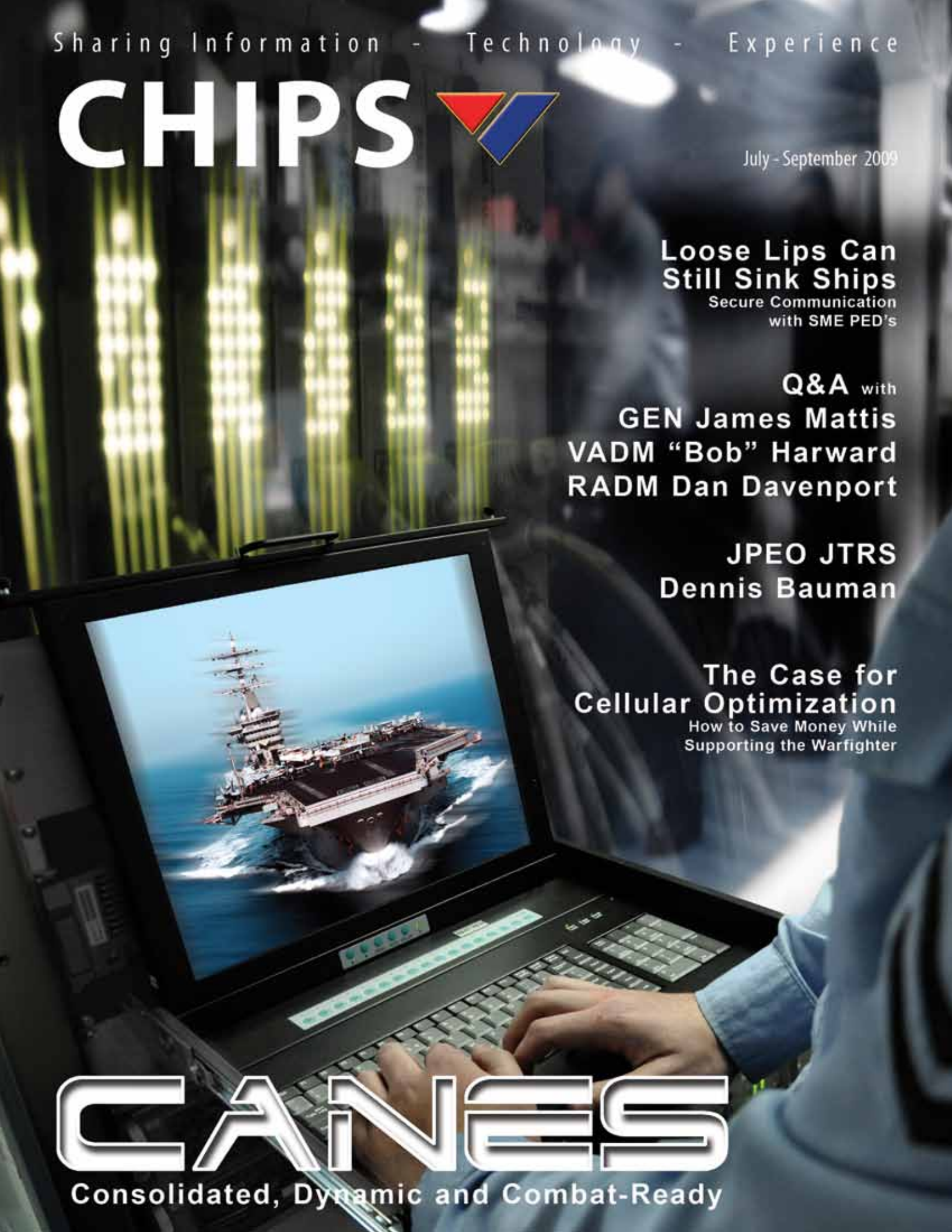
July - September 2009

Loose Lips Can Still Sink Ships
Secure Communication with SME PED's

Q&A with
GEN James Mattis
VADM "Bob" Harward
RADM Dan Davenport

JPEO JTRS
Dennis Bauman

The Case for Cellular Optimization
How to Save Money While Supporting the Warfighter



CANES
Consolidated, Dynamic and Combat-Ready

CHIPS

July-September 2009 | Volume XXVII Issue III

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
Holly Quick, SSC Atlantic

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) 443-0905; 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) 443-0905, DSN 646.

SPAWAR

CHARLESTOWN, Mass. (July 4, 2009) USS Constitution, the world's oldest commissioned warship, returns to her berthing at the Charlestown Navy Yard after firing 21-gun and 19-gun salutes in Boston Harbor during 4th of July celebrations. U.S. Navy photo by Mass Communication Specialist 1st Class Mark O'Donald.

Cover

CANES, the Consolidated Afloat Networks and Enterprise Services program, eliminates legacy, stand-alone networks with a single, agile enterprise system that strengthens shipboard network infrastructure, reduces hardware footprints and decreases overall life-cycle costs. CANES provides integrated voice, video and data management delivering combat-ready services to the warfighter. The Navy Tactical Networks Program Office oversees the CANES program, as part of the Program Executive Office for Command, Control, Communications, Computers and Intelligence.

Navigation Guide

Features

6 CANES
Delivering C4ISR to the fleet as an enterprise system

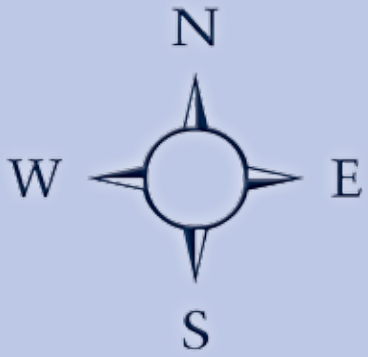
10 Communications Across the Joint Battlespace
JPEO for JTRS Dennis Bauman

13 Q&A with Gen. James Mattis
NATO Supreme Allied Commander Transformation
Commander, U.S. Joint Forces Command

20 Q&A with Vice Adm. Robert Harward
U.S. Joint Forces Deputy Commander and
Rear Adm. Dan Davenport
U.S. Joint Forces Joint Concept Development and Experimentation Directorate (J9)

In Every Issue

4 Editor's Notebook
5 Message from the DON CIO
27 Going Mobile
28 Full Spectrum
38 Hold Your Breaches!
40 Web 2.0
50 Lazy Person's Guide
53 Enterprise Software Agreements



From the DON CIO

9 In Memoriam … John J. Lussier

16 Hello PACOM? Baghdad Calling
By Mike Hernon

18 Optimizing Telecom Usage While Cutting Costs
By Mike Hernon, Ken Brennan and Shirley Dolengo

23 Universal Core – *Improving information sharing across the government*
By Dan Green

32 Defending Cell Phones and PDAs Against Attack
By DON CIO Privacy Team

35 DON CIO releases Next Generation Enterprise Network podcast
By DON CIO Communications Team

41 Today's Plan for Tomorrow's Cybersecurity Workforce
By Mary Purdy

Navy Network Enterprise

33 USS Truman Readies for Operational Testing of Key Data Integration
DCGS-N allows ashore and afloat ISR and IO sharing
By Michael Pobat

35 NMCI Links to Other Defense Branches Via JEDS
By NMCI Public Affairs

Going Green

44 ONR Partners with Car Industry to Test Energy-Efficient Vehicles
By ONR Corporate Strategic Communications

Information Sharing

49 DON IM/IT Conference Provides Venue for Feedback – *DON CIO leadership asks for input on important policy issues*
By Sharon Anderson

Maritime Domain Awareness

30 Detecting Conventionally Powered Submarines – *Team SPAWAR contributions to the DESI and Maritime Strategy*
By Frank Bantell, José Carreño, George Galdorisi and Russell Grall

39 COBRA: One Step Closer to Expeditionary Warfare Users – *Mine detection system passes critical Milestone "C" Decision for low-rate initial production*
By Jacqui Barker

43 TW09/OLC2: Sea Trial Experimentation of Critical Maritime Technologies
By Holly Quick

46 SSC Pacific Guam facility at the forefront of strategic military buildup efforts
By Tom LaPuzza

Technology Breakthroughs

24 IRIS – *Changing the fixed-circuit paradigm*
By U.S. Navy Lt. Cmdr. Tom Merkle, Rich Farrell and Steven Groves

36 Team SPAWAR's Fiber-Optic Technology Helps Nereus Reach Deepest Part of the Ocean
By Media Relations, Woods Hole Oceanographic Institution and SPAWAR Public Affairs

42 Joint and coalition warfighters test new and emerging technological solutions for combatant commanders at CWID 2009
By John J. Joyce

Training

45 Individual Augmentees Prepare for Afghanistan Mission
By Army Staff Sgt. Raheem Lay

Workforce

34 SPAWAR Systems Center Pacific offers guaranteed education, technical training and jobs
By SSC Pacific Public Affairs

Editor's Notebook

If you go to Merriam-Webster Online Dictionary and type in "enterprise," three different descriptions will pop up: (1) a project or undertaking that is especially difficult, complicated or risky; (2) a readiness to engage in daring or difficult action; and (3) a unit of economic organization or activity, especially: (a) a business organization; (b) a systematic purposeful activity.

If you were to apply these three definitions to the Consolidated Afloat Networks and Enterprise Services (CANES) and the Joint Program Executive Office Joint Tactical Radio System (JPEO JTRS), you would find a good match. Both these enterprise initiatives, CANES, a Department of the Navy program of record, and JPEO JTRS, a Defense Department program of record, are daring, difficult, purposely systematic and risky because they bust old acquisition paradigms, employ innovative technologies and challenge us to think differently about what it means to be part of an enterprise.

Thinking in terms of an enterprise means giving up individual control and putting our faith and efforts into making the enterprise as a whole a success. Change is difficult, but helping the DON and DoD become true enterprise organizations will yield tremendous cost savings and cost avoidance, invigorate competition and innovation, and enhance security and extend communications.

To me, becoming an enterprise also means having power and clout and the ability to make transformational changes for the benefit of the entire DON and DoD, and not just for our individual projects and organizations. There are many sound business reasons to think and act like an enterprise, but perhaps the best business case is to enable the warfighter on the pointy end of the spear. CANES and the JPEO JTRS have already demonstrated success in their enterprise business models and in enabling better communications for the warfighter. I urge you to read about their successes in this issue.

In May, the CHIPS staff manned the Team SPAWAR exhibit at the Joint Warfighting Conference at the Virginia Beach Convention Center. Thanks to those who stopped by to say hello. The JWC was cosponsored by U.S. Joint Forces Command, AFCEA International and the U.S. Naval Institute.

The JWC was held concurrently with the DON IM/IT Conference hosted by the DON CIO. Both conferences sparked a great deal of dialogue among subject matter experts, leadership and attendees. Many of the articles from the DON CIO and the Q&As with USJFCOM leadership in this issue were a result of the enthusiasm for topics discussed at the conferences. I hope you find this issue informing and maybe just a bit challenging to your way of thinking.

Welcome new subscribers!

Sharon Anderson

CHIPS webmaster, Tony Virata, CHIPS assistant editor, Nancy Reasor, Space and Naval Warfare Systems Center (SSC) Atlantic employees, Anthony Carbone and Kris Fogle, at the Team SPAWAR exhibit at the Joint Warfighting Conference in May.

SSC Atlantic employees Tom Gwiazdowski and Sandy Mieczkowski with CHIPS contributor Holly Quick at the Joint Warfighting Conference in May.

Please join us for the next DON IM/IT Conference, to be held Feb. 1-4, 2010, at the San Diego Convention Center. Go to the DON CIO Web site at www.doncio.navy.mil for details.

MESSAGE FROM THE

DON CIO

It is important for the Department of the Navy to think and act like an enterprise because of the potential to realize a number of important benefits including increased integration of our operating forces, improved interoperability, and consistent and improved information assurance. These benefits are in addition to cost savings, cost avoidance, and more effective use of the department's resources.

Many of the department's processes have traditionally revolved around individual programs and an environment where success is measured by a program's achievement of its acquisition milestones.

Mr. Robert J. Carey

Program managers are responsible for delivering capabilities based on program-specific cost, schedule and performance requirements. Although well intended, decisions based on individual programs, without consideration of enterprise requirements, can lead to operational inefficiencies and degraded interoperability.

Thinking like an enterprise enables managers to more effectively address requirements, develop realistic concepts of operations, and create synergy and rigor in engineering, testing, integration, budgeting, acquisition strategy and contracting — which results in improved capability delivery, a more affordable investment strategy and improved partnering between government and industry providers and the end-user community.

Consolidated Afloat Networks and Enterprise Services — The value of thinking and acting like an enterprise

A noteworthy example of "enterprise-think" is the Navy's Consolidated Afloat Networks and Enterprise Services (CANES) program. It represents a fundamental change in the way the department acquires networks and network security capability for the fleet. The goal of CANES is to provide a common computing environment, core services and enhanced network security, which can be leveraged by the majority of afloat IT systems.

By migrating to an enterprise afloat network architecture with a single backbone and uniform security and services, the Navy will significantly reduce its afloat network footprint achieving overall cost reductions through elimination of redundant systems and processes, increase network security, and add cutting-edge functionality more quickly than it can today.

However, program managers do not have direct responsibility or influence over the numerous IT systems that could potentially make use of a common IT infrastructure and core services. Therefore, they do not always have the leverage to fully achieve enterprise goals, such as the long-term goals of the CANES program.

To fully embrace and realize an enterprise vision, program managers, users, operators, resource sponsors, and the acquisition, technical and chief information officer communities must focus on achieving potential benefits to be gained by thinking and acting like an enterprise.

This would include aligning requirements and concepts of operation, performing budgeting from an enterprise perspective, synchronizing acquisition plans, developing a robust architecture that incorporates associated systems and implementing a set of enterprise standards. Another key aspect of achieving this vision will be to leverage and expand on the existing decision-making forums and processes of the department, such as acquisition gate reviews and Clinger-Cohen Act confirmations, to ensure they also focus on the enterprise perspective.

A significant opportunity for CANES is to align with the Next Generation Enterprise Network (NGEN). This alignment would facilitate improved interoperability between the department's primary ashore and afloat enterprise IT infrastructures, and would allow for CANES and NGEN to become the first concrete step toward achieving the DON's Naval Networking Environment vision and strategy.

The challenge of thinking and acting like an enterprise may seem daunting. However, I am confident that the department is up to this challenge and that we can work together towards achieving our common enterprise goals and objectives.

On a sad note, our Department of the Navy Principal Deputy CIO, John J. Lussier, passed away on June 17, 2009, after a courageous battle with pancreatic cancer. One of John's many superb accomplishments included the DON Computer Network Defense Roadmap, which CHIPS had already planned to include as an insert to this issue. John was a consummate team player, whose drive to serve the Nation and the Navy and Marine Corps team was only exceeded by his devotion to his family. A memorial to John appears on page 9. He is sorely missed by his DON colleagues.

DEPARTMENT OF THE NAVY - CHIEF INFORMATION OFFICER

www.doncio.navy.mil

CANES

Consolidated, Dynamic and Combat-Ready

By Sharon Anderson

Consolidating Navy ashore networks into an affordable, manageable, secure environment has been an ongoing effort since the notable development of the Navy Marine Corps Intranet in 2000. And while much attention has been given to the follow-on contract to the NMCI, the Next Generation Enterprise Network, or NGEN, an enormous effort is also underway to deliver the same economies of scale and enhanced security to fleet users through the Consolidated Afloat Networks and Enterprise Services program.

CANES represents a significant change in the way the Navy procures command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) capabilities. By using proven technology and industry standards, CANES will provide a common computing environment, including network hardware and software infrastructure, beginning in 2011.

CANES will deliver C4ISR capability as applications instead of complete systems, harvesting significant savings for the Navy while accelerating delivery of warfighting capability to the fleet.

The Program Executive Office for C4I Tactical Networks Program Office released the Request for Proposals (RFP) for CANES Increment I April 2. Responses were due June 3. The scope of the CANES Increment I RFP includes the design, development, integration and production of a common computing environment tactical network for the Navy. Implementation of CANES Increment I is expected to be completed by 2016.

The Naval Network Environment

CANES is part of a larger effort by the Department of the Navy to establish the Naval Networking Environment 2016.

CANES is the afloat piece of the four components of this significant undertaking. The others are NGEN; Base Level Information Infrastructure, or ONE-NET, the overseas network; and one the Navy terms as excepted networks, such as health care and training and education networks that will not be included in the NGEN enclave.

"We want to speed effort to catch the current wave of technology. That includes service oriented architectures, enterprise solutions, innovative security approaches and state-of-the-shelf hardware," said Vice Adm. Harry B. Harris, Deputy Chief of Naval Operations for communications networks and Deputy Chief Information Officer (Navy), earlier this year.

According to Harris, CANES will provide 75,000 seats on 192 ships and submarines and at nine maritime operation centers across the fleet.

The Naval Networking Environment is envisioned to be a fully integrated, enterprise-wide networking environment where data and services are ubiquitously available to naval users. It will ensure that all naval networks, including the future afloat networking infrastructure, are fully interoperable.

Increment I Acquisition Strategy

CANES is an ACAT I program of record. The program's acquisition strategy is to initially select two contractors from the RFP in the first quarter of fiscal year 2010 and then down select to one contractor. The total cost of the contract for Increment I is expected to be just under $1 billion. The Space and Naval Warfare Systems Command, headquartered in San Diego, is the contracting authority for CANES contracts.

"We are planning a dual award, and it is going to be a bake-off between the best competing designs," said Robert Wolborsky, Tactical Networks program manager for CANES. "When we down select to a single vendor, we will have two limited, low-rate initial production options where the bulk of the dollars associated with the contract are. The fly-off is 14 months from when we award the contract."

Wolborsky and Cmdr. John Sprague, CANES assistant program manager, talked about the development of CANES in early June from their office in San Diego. They said the need for CANES was urgent.

"CANES was envisioned in the POM-08 (Program Objective Memorandum). Currently, each shipboard C4I system operates on a separate network infrastructure — different equipment, different software — and requires dedicated personnel to operate them. CANES will replace those various, stovepiped afloat networks with a single, common network system," Sprague said.

Early testing of the CANES concept demonstrated the potential for significant savings for the Navy. The formal analysis of alternatives assessed major ISR and C2 systems that were migrating into the CANES network Infrastructure. These major systems included Global Combat Support System-Maritime, Distributed Common Ground System-Navy and Navy Tactical Command Support System, including several other key applications.

"The original estimate was more than $2.3 billion in potential cost avoidance and savings for the Navy by migrating a limited set of major applications into this enterprise network architecture of core services, application hosting and virtualization," Wolborsky said.

But the requirement went beyond saving money. The development of CANES is also in response to fleet demand for a robust tactical network. CANES is comprised of two main subprograms: the common computing environment, which consolidates all

CANES Will Consolidate:

- Integrated Shipboard Network Systems (ISNS)
- Combined Enterprise Regional Information Exchange System (CENTRIXS)
- Sensitive Compartmented Information (SCI) Local Area Network
- Submarine Local Area Network (SUBLAN)
- Video Information Exchange System (VIXS)

the hardware, racks, servers and communications media for shipboard applications, and the afloat core services, which is a consolidation of applications in use today.

"CANES is the culmination of the lessons learned in developing, producing, fielding and supporting all the backbone networks on ships and subs. In developing the requirement for CANES, we had intense interaction with the fleet to inform users and gather requirements. What the fleet wants is a network transformation from an administrative tool to a secure operational and tactical center of gravity. The fleet needs a flexible, agile, reliable and secure network," Wolborsky said.

CANES has an approved Requirements Document and is the first program of record to go through a Gate 3 Review inside what is known as the Navy's 2 Pass/6-Gate Review process.

"CANES has also successfully accomplished a Gate 4 and 5 review. We are the first program in DoD to successfully accomplish a Materiel Development Decision," Wolborsky said. "We have a signed Acquisition Decision Memorandum by AT&L (Under Secretary of Defense for Acquisition, Technology and Logistics) giving us permission to proceed, to award our contract and lead us to a Milestone B Decision."

The Office of Naval Research is currently conducting an independent technology readiness assessment on CANES. The three critical technology elements evaluated were Common Computing Environment, Cross Domain Solutions and Afloat Core Services. The program office evaluates all three at a high technology readiness level that translates into low risk to the program.

The Ubiquitous Tactical Network

Afloat networks have evolved from administrative tools to a vital piece of the shipboard infrastructure that supports key warfighting, operational and quality of life requirements.

Warfighters have a critical need to share information from highly classified networks down to unsecured coalition networks. In the past, bridge solutions were developed within each organization for their specific applications. The overhead was tremendous with independent sustainment tails, countless interconnections, inconsistent security and risk-mitigation practices, and confusing sharing policies.

"How many security domains can be consolidated? How much information sharing can we potentially facilitate between the domains? How much infrastructure can we reduce by doing so?" Wolborsky said. "Those are the questions and benefits that are yet to be defined. We are waiting for the proposals to come in to see how well we meet those targets and goals from a technology perspective."

According to Sprague, CANES is expected to reduce the footprint of physical infrastructure on ships through virtualization. By running multiple, independent virtual operating systems on a single physical computer, increased computing power can be achieved and hardware investments and physical resources can be maximized.

"By having a consolidated, virtualized set of racks, we can load all of the applications and maintain them instead of each application bringing its computing power and only utilizing 20 percent of it," Sprague said.

Decoupling systems and applications from hardware allows applications to be lightweight and agile. Simplifying sustainment and maintenance is key because different classes of ships have different systems and configuration baselines depending on their missions and age.

"Moving to an enterprise network architecture and decoupling the applications from their organic hardware, and even from some of their services, will allow us to coordinate future changes faster," Sprague said.

CANES will enforce configuration management through its enterprise architecture and free program managers from worrying about compatibility issues, hardware, databases and directories. It will provide disciplined configuration management based on the Acoustic Rapid COTS Insertion model used by the submarine community. Hardware will be updated every four years and software (operating systems and systems management) will be updated every two years.

"The result," said Sprague, "will be that program managers will no longer be concerned with providing hardware and software. By following the CANES roadmap, program managers will know when and what kind of hardware will be provided and can instruct their application developers to tailor applications to ride on that."

The CANES program team is also paying close attention to bandwidth consumption issues, especially with small fleet units that have traditionally been bandwidth disadvantaged. Wolborsky is working to ensure that the Automated Digital Networking System Increment III is aligned with the CANES program to make certain that the programs are cognitive of the bandwidth demand for the implementation of afloat core services and what these applications will need in the future.

"The challenge isn't going away, but over time we can significantly increase the amount of throughput with gapfiller satellites, expanded use of the Commercial Broadband Satellite Program and other initiatives that PEO C4I is taking on," Wolborsky said.

SAN DIEGO, Calif. (March 10, 2009) Fran White, left, a civil service employee at Space and Naval Warfare Systems Center Atlantic, and Clayton Bush, a Tactical Networks Program Office (PMW 160) contractor, work with Information Systems Technician 2nd Class James Rago to troubleshoot the video teleconference system of a video information exchange system aboard the aircraft carrier USS Ronald Reagan (CVN 76). PMW 160 and SPAWAR provide the Navy with network fabric and services used by multiple shipboard tactical and business applications and systems and routinely install, maintain and train crew members in operational and maintenance procedures. U.S. Navy photo by Rick Naystatt.

The Way Ahead

The CANES team has already begun coordination with the Navy's aviation and ship communities to ensure wider alignment with combat systems.

"We recently sent our team to Naval Air Systems Command so they could start conceptualizing how CANES could go on planes in the future. A number of aircraft applications could potentially be targeted, and we're working to determine how our core services can get out to the tactical edge more effectively."

Although PEO C4I is not typically involved in hull, mechanical and electrical networks, consolidation of these networks may be a requirement down the road.

"We do not field or support those networks today, but we are having detailed discussions with the folks that are responsible for doing that, the Ship Systems Engineering Station folks in Philadelphia, the Naval Sea Systems Command and the new construction folks. Even though there are complexities, they use the same technology from a networking perspective that we do," Wolborsky said.

The Navy's ultimate goal is to have one enterprise shipboard network, and the CANES team has been looking at work that has been done in the past to meet this objective, according to Wolborsky.

"We need to take a long, hard look at previous efforts and the lessons learned. We have a desired end-state in mind, but we need to do it." CHIPS

Sharon Anderson is the CHIPS senior editor, contact her at chips@navy.mil. For more information about CANES, contact the Space and Naval Warfare Systems Command public affairs office at (619) 524-3432.

Navy Prepares for Limited Delivery of Shipboard Wireless Networks

The Navy's PEO C4I announced in June that it will begin limited procurement and fielding of unclassified wireless networks on board Navy surface ships starting this summer. Once accomplished, shipboard wireless networks will allow Sailors greater mobility and enhance their ability to multitask and conduct shipboard business more efficiently.

While wireless networks are common in the commercial arena, until now, bringing the capability to the Navy has proven problematic based on the cost, the processes involved to meet the Navy's stringent security requirements, and the time it takes to develop, demonstrate and test a product within the minimum two-year acquisition cycle to rapidly deploy a capability.

The implementation of unclassified wireless networks capitalizes on commercial efforts and incorporates commercial best practices. The new capability will be delivered as part of ongoing installations to avoid the cost of installing network cables to the desktop.

Introducing wireless networks at sea will allow Sailors greater flexibility, enhanced mobility, and provide a foundation to allow new and innovative capabilities to be brought to the shipboard environment.

The shipboard network environment aboard Navy surface ships will use Institute of Electrical and Electronics Engineers 802.11 technology to provide Navy personnel with an unclassified wireless network interface. The wireless infrastructure will provide an extension of the unclassified Integrated Shipboard Network System.

Multiple Sailors will be able to share the capacity provided by a single wired network connection by using an unclassified wireless access point, into which the wired ISNS connection terminates. This eliminates the cost associated with providing wired network access to each Sailor.

Though the network will be unclassified, information assurance will remain a top priority. The system was designed to meet or exceed all DoD security standards for unclassified wireless technology, including defense-in-depth best practices and a Federal Information Process Standards 140-2 Level 2 accredited encryption module.

An authentication protocol will ensure the network is only accessible to valid wireless client devices and dual security layers will ensure that no unclassified wireless data can be captured and deciphered. In addition, a Wireless Intrusion Detection System will be included in the system design to identify invalid wireless activity and alert network administrators to the nature and location of the activity.

In a related effort, PEO C4I's Tactical Networks Program Office successfully leveraged the wireless network technology and effort to develop the Wireless Reachback System. The system provides a secure wireless link for the transmission of data supporting multiple mission sets. The system is currently employed by Visit, Board, Search, and Seizure teams to transmit biometric and intelligence data between vessels of interest and the on-scene commander during Expanded Maritime Intercept Operations, and to provide nongovernment officials Internet connectivity during disaster and humanitarian relief efforts. CHIPS

In Memoriam

John J. Lussier, Department of the Navy Principal Deputy Chief Information Officer, passed away on June 17, 2009. He leaves to mourn a wife and three young children. Also mourning his loss are his DON CIO family, his DON and Department of Defense colleagues, and a host of other family, friends and neighbors. John was diagnosed with pancreatic cancer in June 2008, but continued working while receiving treatment for his illness. During this difficult year, he maintained his professional demeanor, sense of humor and compassion.

John was selected by the Secretary of the Navy to serve as the DON Deputy CIO in May 2007. Previously, John was appointed Acting DON Deputy CIO in July 2006 and Acting DON CIO in November 2006. His appointments filled the void created when DON Deputy CIO Rob Carey was deployed to Iraq and DON CIO Dave Wennergren took a position as DoD Deputy CIO. With the top two positions in the DON CIO vacant, John was faced with what would have been a challenge to any leader.

However, he accepted this challenge with grace, and he managed the roles of Acting CIO and Deputy CIO, in addition to his responsibilities as Director of Operations, and Telecommunications, Wireless and Spectrum Team Leader.

As Deputy CIO, he managed and led the staff, providing the direction necessary to keep the DON CIO running a steady course. As the department's Senior Information Assurance Officer, he was responsible for the security of the DON's IT networks and applications to ensure information dominance on the battlefield and seamless operations for our Navy and Marine Corps forces.

The Computer Network Defense (CND) Roadmap he recently signed (included as an insert to this issue) charts the way ahead for CND in the department and will be extremely beneficial to the DON both in the present, and well into the future.

As the Director of Operations, he handled the responsibility for all personnel, budgetary, financial and contractual management for the DON CIO. As Telecommunications Team Leader, John succeeded in transitioning the department's telecommunications to an enterprise management model, which has influenced the way telecommunications is managed across the government.

The wireless LAN policy he formulated secures the wireless environment, which is most important to our Sailors and Marines deployed to locations where the use of wireless technology is critical.

John's leadership of the policy and strategic planning for electromagnetic spectrum has led to the assurance that DON and DoD equipment that uses the electromagnetic spectrum is protected.

John has represented the DON as the ranking official to national and international bodies, including the World Radiocommunication Conference, International Telecommunication Union, and the Federal Communications Commission.

John J. Lussier
27 July 1959 – 17 June 2009

John has positively influenced the work of the DON CIO, the department and the DoD, and his impact will be felt for years to come.

John was a great boss, an admirable leader and a vital part of the DON CIO family. He will be missed by all whose lives he touched. CHIPS

Communications Across the Joint Battlespace

By Mr. Dennis Bauman
Joint Program Executive Officer
Joint Tactical Radio System

In today's warfighting environment, it is essential that we, as Defense leaders, accelerate the delivery of advanced networking capabilities into the hands of our warfighters. The Department of Defense (DoD) has learned from the communications interoperability challenges observed during operations in Grenada, Panama and Desert Storm, and has sought to replace the multitude of non-interoperable, non-networked legacy radios in use throughout the services.

We must seek to not only replace legacy radio functionality, but to enable network-centric warfare across the joint battlespace through the use of advanced mobile, ad hoc network capable devices.

With its ability to deliver 10 to 100 times the bandwidth to the tactical edge, the Rifleman Radio represents an enormous increase in capability, technology and security for the Soldiers in forward operations. U.S. Army photo.

JTRS delivers interoperability to the tactical edge

In order for the U.S. military to be a truly superior fighting force, we must extend the power of the Global Information Grid (GIG) to the tactical edge to provide real-time battlefield awareness and enable timely decision-making. The Joint Tactical Radio System (JTRS) delivers this capability by building a powerful network of Soldiers, ground vehicles, sensors, ships and airborne platforms, enabling true networking and joint interoperability for the first time between all four DoD services across the tactical edge of the entire battlespace.

Using legacy systems, situational awareness stops at the command center, limiting the amount of information that can flow to or from the actual engagement. This lack of a networked information flow leads to latency in shared data, the inability of ground troops to expand their network vertically to receive cross-service air or maritime support and difficulty in tracking friendly versus enemy forces on the battlefield.

Additionally, capability upgrades have been arduous, as the radio industry paradigm has been a closed, proprietary model in which industry typically retains most software and hardware intellectual property rights. This model requires the services to continuously invest with an individual vendor for each capability upgrade. Furthermore, the services typically chose different radio vendors, diluting DoD's ability to leverage economies of scale.

Utilizing this model, the overall cost to innovate/upgrade and field in mass quantities was inflated, limiting the ability to effectively field new capability and constraining joint interoperability.

JTRS provides mobile, ad hoc networking

In order to combat this traditionally costly and disjointed system, the Joint Program Executive Office (JPEO) was formed in 2005 to provide joint oversight to the JTRS technology. The JPEO portfolio consolidates separate service-led and service-specific radio programs into a single, joint development effort and is comprised of five ACAT ID programs: Ground Mobile Radio (GMR); Airborne, Maritime and Fixed Station (AMF); Handheld Manpack, Small Form Fit (HMS); Multifunctional Information Distribution System-JTRS (MIDS JTRS); and Network Enterprise Domain (NED).

The GMR, AMF, HMS and MIDS JTRS programs leverage the waveform and network management capability provided by NED to develop and field the JTRS sets. The advanced networking capabilities are made possible by incorporating transformational waveforms, such as the Wideband Networking Waveform (WNW) and Soldier Radio Waveform (SRW), as well as legacy waveforms, such as Single Channel Ground and Airborne Radio System (SINCGARS), Enhanced Position Location Reporting System (EPLRS), Link 16, Ultra High Fre-

quency Satellite Communications (UHF SATCOM) and HF.

The incorporation of legacy waveforms, as well as the development of new waveforms, has allowed continued success across the JPEO enterprise in developing joint technology and furthering the goal of joint warfighting capability. The JPEO vision is focused on enabling network-centric warfare through the use of advanced mobile, ad hoc networking-capable JTRS devices.

JTRS systems are organic to tactical forces and not dependent on fixed infrastructure to move high-bandwidth data, dramatically improving decision superiority and battlespace flexibility. Unlike cellular and other mobile devices that require extensive arrays of fixed-site towers, relay stations or complex satellite constellations in order for users to communicate seamlessly while on the move, JTRS allows for those functions to be done within each radio device. This functionality is far beyond what a regular "radio" has ever had the ability to do and is critical to providing battlefield efficiency of the network as well as a common operational picture for the warfighter.

JTRS continues to make headway and drive forward with systems that are born joint and evolve to encompass changing technology without an unacceptable risk to joint/allied interoperability. As a result of the JTRS program, a joint tactical networking environment is within reach, in which all services can communicate in real time by video, chat, data or voice, in uncharted, uncertain terrain.

For the first time, these communications will encompass for warfighters high-bandwidth information (including sensor information from joint and national assets) over a single network, delivering true, interoperable, network capability at the tactical edge. JTRS connects the ground, air and maritime domains, not only with each other, but also with the GIG.

JTRS employs an innovative acquisition model

Facilitating this interoperable network is a software-defined architecture which enables the porting (or loading) and reuse of a standard suite of software products, including the waveforms used to transmit the data, on a wider variety of hardware configurations.

JTRS provides secure, high bandwidth networking waveforms, an intuitive network management capability, and software defined radio and networking technologies that make current and future platforms both more capable and flexible to meet today's and tomorrow's threat environment.

The ability to port and reuse standard software products allows JTRS sets to provide continued flexible technology insertion and product refresh without risk to interoperability, as well as the ability to expand to include coalition and allied fighting forces on the battlefield, further harnessing the power of the network as a true force multiplier.

Today, JTRS is demonstrating that success both in the testing and in the fielding of JTRS products. For example, the AMF program offers two different form factors [AMF-Maritime-Fixed (M-F) and AMF-Small Airborne (SA)] based on a single common architecture that is designed to meet the airborne and maritime-fixed station requirements for advanced networking capabilities (such as vertically extending the ground network). The Navy is currently planning to procure AMF-Maritime-Fixed radios for multiple platforms such as the CVN, DDG, SSN, SSBN, LHD and LPD, as well as the AMF Small Airborne radio for the E-2 aircraft.

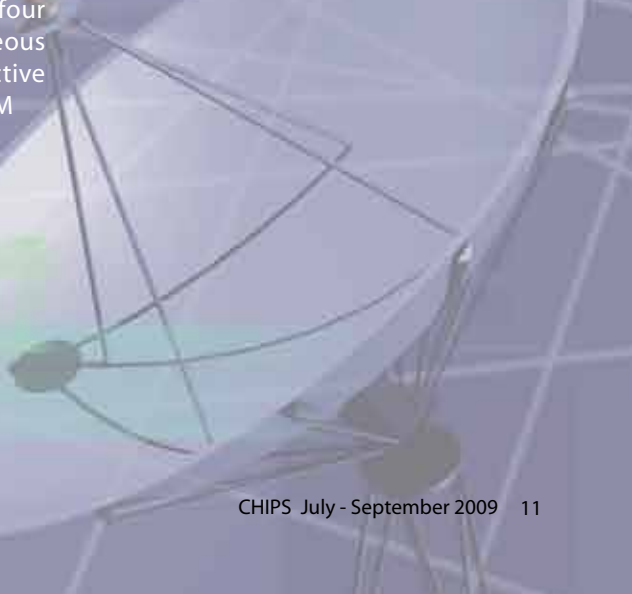
AMF JTRS is currently on contract for the Engineering and Manufacturing Development phase, and development is fully funded and on track to deliver EDMs meeting user need dates. Specifically, AMF offers the Navy a better solution than the DMR radio, providing four full duplex channels with simultaneous combinations of Mobile User Objective System (MUOS) and UHF SATCOM for the AMF-Maritime-Fixed, and two full duplex channels with simultaneous combinations of WNW, SRW, Link 16, MUOS and on the AMF-Small Airborne, offering one design with one waveform port and packaged for platform integration.

Additionally, the MIDS-JTRS program supports the airborne and maritime community by providing secure, jam resistant transmission/reception of Link 16 messages for joint/allied interoperability and situational awareness.

In demonstrating superior capability, MIDS-JTRS has completed nine successful tactical air navigation (TACAN) flights and three Link 16 flights to date.

Additionally, both HMS and GMR programs afford advanced support to the ground warfighter. HMS is currently developing small-form fit factors that provide tactical networking for soldier-carried handheld and manpack radios, specifically the Rifleman Radio, which is a single-channel, Type 2 encryption set with SRW and commercial GPS, delivering protected voice and situational awareness data.

JTRS Manpack and GMRs are designed to complement the Rifleman Radio, extending networking capability (via WNW and SRW) from the command post/vehicle to the squad leader. GMR supplies secure communications and enables simultaneous multimedia communications over independent channels to ground vehicle platforms like the Standard Integrated Command Post System Carrier,



Abrams Tank, Bradley Fighting Vehicle, High Mobility Multipurpose Wheeled Vehicle, Expeditionary Fighting Vehicle, and the Light Armored Vehicle. Both GMR and HMS have conducted multiple successful testing and field experimentations.

As JTRS demonstrates success and fielding of capabilities, the JPEO's business model and acquisition process have formed the foundation for affordable capability that can be delivered before the technology reaches commercial obsolescence.

The majority of our IT and networking infrastructure is software-based, which creates opportunities for new ways of thinking. This has afforded DoD the ability to establish open standards/open architecture approaches to create the necessary commonality for our systems.

JTRS promotes competition through a paradigm-busting business model

JTRS is applying several methodologies as part of an innovative Enterprise Business Model (EBM), including negotiation for Government Purpose Rights (GPR) for all JTRS software, promoting competition in production, and establishing a JTRS Information Repository (IR) to maintain and reuse this software for current and future capabilities.

Through this process, JTRS vendors provide GPR for their software and place the code in the IR. JPEO JTRS then controls access to the IR for capability improvement and enhancement.

Using this infrastructure process, JTRS has created a secure, Common Enterprise Architecture, as well as other standards, including application program interfaces (APIs), software architecture and key tags, to ensure that JTRS software is consistently applied across several hardware platforms.

The significance of this approach is in providing a foundation for increased software reuse and portability, which reduces life-cycle cost and maximizes communications/networking interoperability across multiple radio platforms. The Enterprise Business Model is a competitive approach, qualifying at least two sources of production for all JTRS products and competing buys in lots, maximizing competition in production to reduce unit costs. This allows DoD to take advantage of competition when real cost savings can be realized in production.

This model mirrors the U.S. Army's UAV Ground Control Station program and the U.S. Navy's Acoustic Rapid COTS Insertion (ARCI) model, which is leveraged by the submarine community, for open architecture approaches.

Since implementing this approach, JTRS has seen a significant return on investment. For example, the JPEO developed a Consolidated Single-Channel Handheld Radio (CSCHR) contract, a full and open competition for production of JTRS-approved single channel handhelds, and awarded contracts to two vendors.

The result was both an early delivery of JTRS capabilities and a cost savings for DoD of $428 million since contract award in June 2007. Clearly, this type of business approach not only provides competition and cost savings, but also provides a strategy for breaking the proprietary gridlock paradigm noted earlier.

Overall, the JTRS program is nearing completion of the core development activities necessary to field the full JTRS capability. Already there are more than 84,000 single-channel handheld JTRS radios that are either in the field or on order by the services. This is a significant achievement in replacing outdated and/or inferior legacy radios with more secure and higher-capability JTRS sets.

With thousands of units already in the field, and many more only months away, JTRS is delivering a business model that promotes not only efficiency in development, but overall value for the DoD and taxpayers.

JTRS connects the ground, air and maritime domains with each other and with the GIG

With the JTRS capability, the interoperable communications required during conflict engagements no longer stop at the command center, but now extend out to the warfighters on the move at the frontlines. As a result, our warfighters are being equipped with the necessary networking and communications capabilities to ensure their utmost safety and competitive advantage over their adversaries.

The JTRS concept of providing a truly joint, mobile, ad hoc, secure network that extends beyond the command center and to the tactical warfighting edge is a reality. In today's operating environment, with the U.S. military facing new tactical challenges and a more versatile and lethal enemy on the battlefield, it is critical that the DoD deploys cutting-edge technologies that not only begin and remain joint, but also evolve and improve over time.

JTRS reaches across the joint battlespace to enhance the efficacy and security of our warfighters, the United States and its allies. CHIPS

Mr. Dennis Bauman

Dennis Bauman was appointed the Joint Program Executive Officer of the Joint Tactical Radio Program in March 2005 granting him with dual responsibilities as the senior executive for C4I and Space and JTRS. In August 2006, he was assigned full-time duty as JPEO JTRS where he directs all waveform, radio and common ancillary equipment development; performance and design specifications; standards for operation of the system; and JTRS engineering. Additionally, Mr. Bauman oversees the cost, schedule and performance evaluation for all JTRS activities as well as the program at large.

For more information about the JTRS program, go to the JPEO JTRS Web site at http://jpeojtrs.mil.

Q&A *with* U.S. Marine Corps General James N. Mattis NATO Supreme Allied Commander Transformation Commander, U.S. Joint Forces Command

Gen. James N. Mattis

NATO Supreme Allied Commander Transformation and commander of U.S. Joint Forces Command Gen. James Mattis gave military, government and industry leaders his view of the future joint warfighting force and the challenges they will face at a major defense conference in Virginia Beach, Va., in May.

Mattis discussed current and future threats to national security and stressed the importance of a joint force able to conduct conventional warfare, as well as hybrid warfare, which could be a mix of peer-to-peer conflict, terrorism, criminal activity and cyber warfare.

The general said the U.S. armed forces needed to avoid the historic experience of one of our allies, using as an example Great Britain, which kept a watch on the cliffs of Dover for Napoleon 120 years after he was dead.

"We need to stop looking for Napoleon and start looking for current threats," Mattis said.

USJFCOM produced a document called the Joint Operating Environment (JOE) which examines trends and disruptions in the geopolitical and military landscape, such as: shifting demographics; globalization; economics; energy; food; water; climate change and natural disasters; pandemics; cyber; and space. These trends form the framework for exploring the following types of scenarios: competition and cooperation among conventional powers; potential challenges and threats; weak and failing states; the threats of unconventional power; proliferation of weapons of mass destruction; technology; the battle of narratives; and urbanization.

The JOE is meant to be read in conjunction with the Capstone Concept for Joint Operations (CCJO), which was signed by the Chairman of the Joint Chiefs of Staff (CJCS) Navy Adm. Mike Mullen Jan. 22, and developed with assistance by USJFCOM. Representatives from the Army, Navy, Air Force, Marine Corps and Coast Guard, as well as U.S. Special Operations Command and U.S. Strategic Command, also assisted in the JOE and CCJO development.

The JOE, currently under revision for 2009, "has influenced our Quadrennial Defense Review inputs, it has helped frame scenarios we are putting forward for what we may have to face in the future, it has helped reduce ambiguity so we have the fewest regrets … we can not get it perfect, but we can certainly reduce the scope of regrets we have," Mattis said.

After his opening address at the Joint Warfighting Conference, cosponsored by USJFCOM, the U.S. Naval Institute and AFCEA International, Gen. Mattis spoke with the media.

Q: From a military standpoint, what should the elements of [national] strategy be?

Mattis: We had a grand strategy during the Cold War against communism, called containment. We need a grand strategy today. Since the Berlin Wall came down we have gone into a very complex world, but the new administration is putting together their grand strategy, as I believe they must. We will nest the U.S. military strategy appropriately within that, and then I will know what kind of forces to deliver.

In the interim, we will keep modifying the military force to make sure it meets the grand strategy, the political strategy.

Q: You talked about military history and mentioned lessons learned from past conflicts, and you said there are things that we never should have forgotten. Were you referring to counterinsurgency doctrine that we used in Vietnam?

Mattis: Yes, but that doesn't mean it would have been adequate on its own. We have to adapt because each war has its own character. Certainly, there are timeless things that we should have carried forward. Part of the cost of Vietnam and the country's dismay was that we just wanted to leave all of it behind, not just by years, but also intellectually.

Unfortunately, an enemy will spot our weakness and work against us in that manner.

Q: You think lessons were discarded by military leadership after the Vietnam War because it didn't end as well as we would have liked?

Mattis: The reality is that Soldiers get condemned sometimes for fighting their last war. We were more focused on the future rather than bringing forward the lessons of counterinsurgency.

Q: If you don't want to fight a past war then do you have to plan for any possible contingency?

Mattis: We have to look at what is most likely. In recent conflicts, like Georgia, Russia, the 2006 Lebanon War, Chechnya, Iraq and Afghanistan, we can see how the enemy is adapting. Plus, the enemy often writes what they are going to do. I like to look at jihadist Web sites. They tell what they are going to do. They are going to make sure that no girls go to school. They are going to kill Americans. They are going to have sleeper cells. They tell all of their plans.

Q: You said something in your remarks about how the technology the troops are carrying right now makes them more vulnerable on the battlefield. What do you mean by that?

Mattis: I was talking about the radios. We have gotten so used to robust command and control networks that we think at higher headquarters that we can know all, see all. And, in fact, we have every reason to expect that in the future those networks will be broken down.

We have seen the enemy penetrating our networks, whether it be banking or stealing identities, and we have had Defense Department networks under attack. We know they can get inside, and we should anticipate that they will take these down.

I suggest we had better be ready to operate with degraded and, at times, no communications so that we don't have people waiting for orders. That's why I used the example of Admiral Nelson [before the Battle of Trafalgar] hoisting the flag and saying, England expects that every man will do his duty, because troops will have to take the lead sometimes.

Q. Has technology helped in the current fight?

Mattis: Absolutely, the technology has been an enormous help for us. We can pass information quickly and a lot faster than the enemy can. It has been a wonderful help, but we must not allow it to become our key vulnerability, which it could, if we overly rely on it and don't educate the troops to operate on their own initiative when, not if, those systems go down.

I know those systems are going to go down, so when they do, I want to have the troops say I know exactly what to do because I know what my commander wants done.

There will be opportunities on the battlefield that even today they can take advantage of much faster than technology can give them authority to do so. We are talking about unleashing initiatives, trust, harmony and those kinds of things more than pure technology as command and control.

Command and control is how do I make decisions as a commander and get troops to act on it with everybody working together. We have started believing that it is the number of data bits that we can put over a certain electronic pipe, that's not it. We are talking about unleashing command and feedback, not command and control.

Q: Could you connect the dots between the NATO Multiple Futures Project and the JOE?

Mattis: The JOE and the CCJO are focused on the operational level of war — how we mix Army, Navy, Air Force, Marines and civilians. When we get a national strategy, we will have to adapt operationally to that national strategy.

In my NATO hat, the Multiple Futures Project harvested good ideas from across Europe and America, the French White Paper [on defense and national security strategy], and from think tanks. We held roundtables in Berlin, Geneva and London. The Swiss military brought in nongovernmental organizations like the Red Cross and United Nations. We got these ideas together to help inform the strategic dialogue.

The JOE was an effort at the operational level, and the strategic dialogue is where I focus the Multiple Futures and NATO. The Secretary General of NATO has invited me to speak as he starts the strategic concept dialogue in July in Europe.

Q: Will these documents have an impact on the European Union?

Mattis: The EU and NATO draw from almost the same forces. I am a NATO officer, but in many, many, many cases, it is in NATO's best interest to work with the tightest possible collaboration with the EU. It will certainly reverberate there and since we drew ideas from the same nations that are part of the EU, I think that you will find a lot of commonality.

Q: You are linking up squads for joint ISR (intelligence, surveillance, reconnaissance) but then also taking command and control and breaking it down and giving commanders on the ground more control. Is there tension between squads being given more comms gear and then having it taken away?

Gen. James N. Mattis talking to members of the media at the Joint Warfighting Conference May 12, 2009, at the Virginia Beach Convention Center.

Mattis: There could be, but I don't think so. They carry the gear now. It is just a matter of translating and having the 'interware' that will allow the software to come down.

Once the Air Force came up with ROVER (Remote Operated Video Enhanced Receiver), suddenly every service could pull down every other services' UAV (unmanned aerial vehicle) feeds. There are ways to do this. This is technology and where technology works, it really works.

In the future, a troop will be able to switch from his satellite phone to his FM phone, to his AM phone. He can talk to an airplane, he can talk to his squad mates, or his commander, and when the whole thing goes down he will have other ways to communicate. They may be old-fashioned ways with colored air panels on the ground.

Because we know we are going to run into a challenge does not mean we are going to surrender the technological fight. We still fight it, but we are very cautious about relying on something we know that the enemy will eventually, just like we will, exploit.

Q: What makes this conference important to you and what do you hope to achieve here?

Mattis: We have to figure out what problems have to be solved and get the right people to try to solve them. The military can't solve them on their own. Industry can't, neither can universities and academia. Americans can't do it alone.

You will notice the number of foreign officers here. We get everyone in the room and there are all sorts of discussion and understanding and cross-fertilization on problem solving. This is very useful for us.

Q: Are you training commanders to accept [decision making at the troop level]? Is it difficult?

Mattis: I am responsible to train all one-star and three-star admirals and generals and new ones in the military when they come through. The primary message is that we bring their operation to the speed of trust.

We decentralize command and control and push it down. We train to this. It is happening across the military. Some services have cultures that permit it and accept it already, and others are going to have to adapt.

They can use the models from some of the other services. This is one of the values of having different service cultures. As technologies and the characters of wars change, then a different service's command and control that might not have looked right 20 years ago may be the one that we all gravitate to.

That is why I don't want a joint culture that subsumes the Army, Navy, Air Force and Marines. I want them each to have their own and for us to harvest the good out of all of them.

"The only thing harder than getting a bad idea out is getting a good idea in."

Q: But the responsibility that goes with command and control can't be delegated?

Mattis: No, it cannot. At the same time, understand that you can't regulate everything in war. War rubs the veneer of civilization off you and leaves bare the character underneath. Bad things happen sometimes in war. The enemy gets lucky sometimes. Young guys make mistakes. The fear can be paralyzing at times.

When you hold people accountable, I would just ask that before you judge somebody walk a mile in his moccasins. I would especially encourage members of the media to walk a mile in somebody else's moccasins before you condemn them.

The pressures on young commanders, whether it is a squad leader that is 20 years old with eight guys around him, with him as the oldest guy there, or a general in combat, understand that they are all trying to do their best, and we're not perfect.

Q: You have people that have been in war eight years making decisions; they come back into organizations with the normal chain of command. How do you improve training so they don't get bored?

Mattis: We have two services that take most of the casualties — the Army and Marines. They both have the highest reenlistment rates in their history right now so clearly something is resonating with them, and it is not just the economy because this was true three years ago as well.

You institutionalize what you have learned in these wars. By institutionalizing it, in the future, instead of the decision being made by a colonel, you will leave that to the captain or to the sergeant. There are ways you can build it into your daily routine. It is already happening in many of the services. Some of the services never had trouble with this. They have always sent captains off to sea.

The commander of the British forces going to Korea in 1950 to join the U.N. forces under U.S. command and control was given one order, 'Do what is in the best interest of the queen.' That was it. Then they sent him to do it. That's trust.

The reenlistment rate shows that they are not being turned off by it. They may complain about it at times. I complain too when I have too much command and control over me. Even four-star generals complain about that.

Q: Your memo on [the flawed nature] of Effects Based Operations last summer created a bit of controversy. It seemed to be welcomed by people with ground force experience in Iraq and Afghanistan but generally rejected by air power. Are you still getting push back?

Mattis: In my experience at Maxwell (Air Force Base), where I spoke with lieutenant colonels and majors, I did not get push back at all. I have had officers from various services say they support it 100 percent, but they wouldn't say so in public because it would ruin their careers.

… It's been overwhelmingly well received, and I was surprised by how little push back it got. I was shocked. The only thing harder than getting a bad idea out is getting a good idea in.

Q: How flexible are decision makers to change the players in the [acquisition] programs as well as the equipment that is being used?

Mattis: I think we are pretty good at it. If you look at a U.S. Soldier today, and a U.S. Soldier from six years ago, his combat gear doesn't even look like the same Army. There is nothing on him that is the same. His rifle is shorter; it has sensors that allow him to spot the enemy. They have different uniforms and different radios. The Personal Role Radio, the little radio in the ear, comes from a British company and was bought on short notice when we went into the fight in Iraq.

We have British airplanes and Harrier jets. If it is a good idea, I can just about guarantee you we are interested in exploring it. People are making MRAP (Mine Resistant Ambush Protected) trucks for us today that had never built one military vehicle.

Q: What steps are you taking to institutionalize knowledge gained?

Mattis: On the joint level, I look at what the joint needs are. If the Army is running a good course on ground advisers in Afghanistan, that includes how to get joint ISR, I endorse them and make sure that Army, Navy, Air Force and Marines all get to have that course.

We are opportunistic. Where it needs to be joint, it's joint. We are gathering this all up in a couple of places. We have a Joint Center for Operational Analysis. We also link with NATO Joint Analysis and Lessons Learned Center – JALLC, so NATO troops can get the advantage of the American lessons learned.

We have a tight bond between the Army, Navy, Air Force and Marines lessons learned people who pass it around inside their own network, and it gets out rapidly to the pre-deployment training sites.

There are a number of things the services have put out — Small Unit Leaders' Guide to Counterinsurgency and the Army/Marine Corps Counterinsurgency Field Manual. It is all out there; it is just a matter of if you have time to read it all. CHIPS

Hello, PACOM? Baghdad Calling

Roam Around the World – Securely with SME PED

By Mike Hernon

The Secure Mobile Environment – Portable Electronic Device (SME PED) will soon be operational across the Navy Marine Corps Intranet (NMCI) environment. The SME PED will significantly enhance the Department of the Navy's enterprise mobility efforts by providing mobile personnel with a more convenient and less expensive method to access secure voice and SIPRNET capabilities, as well as unclassified voice and NIPRNET access.

SME PEDs may also avoid the time and costs involved to install secure networking connections in quarters for personnel who require continuous access to the SIPRNET and secure voice.

What is it?

Approved use of the SME PED (pronounced "smee-ped") is the result of a partnership between industry and the National Security Agency. The Defense Information Systems Agency (DISA) led the integration efforts for the Defense Department network environment.

The SME PED is a mobile voice and data device that provides both secure and non-secure communications through two distinct hardware platforms in one case. Connectivity is provided through the use of commercial cellular networks. Depending on the type of traffic, the user either remains on the commercial network or is routed through to the appropriate DoD/DON voice and data networks.

The SME PED also provides all the standard PED functionality, including a calendar, Internet browsing and e-mail, making it a highly versatile traveling companion.

In secure mode, the SME PED provides SIPRNET data access up to Secret and supports voice communications up to Top Secret/Sensitive Compartmented Information (SCI).

For voice, the device determines the highest classification level common to the two parties, makes the connection at that classification level, and informs each user through the display so that the information discussed is kept to the appropriate classification level.

Operating in its unclassified mode, the SME PED operates as any DON-approved PED, such as a BlackBerry, including Common Access Card and Secure/Multipurpose Internet Mail Extensions (S/MIME) support for sending and receiving encrypted e-mail and using digital signatures.

Two versions of SME PEDs have been developed: General Dynamics' Sectéra Edge Smartphone and L-3 Communication Systems' L-3 Guardian. As of this writing only the Sectéra Edge device has been certified by the National Security Agency; certification for the L-3 Guardian is expected soon. The devices are marginally larger than a standard PED, or BlackBerry, in height and width, although about twice as thick.

SME PEDs are designed to be global devices, with interchangeable code division multiple access (CDMA) and Global System for Mobile communication (GSM) modules, able to provide cellular network access almost anywhere the proper cellular services are present. However, at this writing, the devices are incompatible with cellular networks in Japan and South Korea.

Intended Uses and Users

As a high-value device, with the potential to put classified data and communications at risk, assignment of SME PEDs will be carefully controlled. The SME PED is intended only for those personnel who have a bona fide requirement to process classified information outside of their normal workplace or who otherwise re-

quire the capability to process classified information in a mobile environment to accomplish their mission.

Potential users include personnel who have a statutory requirement for 24/7 access to secure communications or deployed personnel who are supporting combat, humanitarian or civil operations and require a mobile capability to process classified information.

To assist in determining user eligibility, the DON SME PED team developed the DON SME PED Concept of Employment, which is available as an attachment to the Department of the Navy policy on the Issuance, Use and Management of the Secure Mobile Environment – Portable Electronic Device.

Release of the Concept of Employment is imminent as of this writing, and it will be available on the DON CIO Web site at www.doncio.navy.mil.

Only those personnel who can demonstrate that they meet the user profile, qualifications and cellular coverage requirements, as described in the guidance, may be considered candidates for approval.

By using the eligibility process to assess and validate potential SME PED users, commands may avoid forwarding requirements for users that are not likely to receive approval.

L-3 Guardian
www.l-3com.com/smeped

Loose Lips Can Still Sink Ships

This expansion of secure communications access also carries with it increased risks. Technically, a SME PED user could initiate a classified phone call anywhere a cellular signal is present, such as on the street, or in a subway system, such as the Metro in the Washington, D.C., area. So, the old adage that "loose lips sink ships" is alive and well in the digital age!

As a result, the security posture of the SME PED relies to a great extent on user behavior to ensure that use of the device, particularly in classified mode, is limited to appropriate locations. To familiarize users with the device's operation and security requirements, users must complete scenario-based training before a SME PED can be activated.

General Dynamics Sectéra Edge
www.gdc4s.com/smeped

Procurement

The SME PED is classified as a Controlled Cryptographic Item (CCI) and is subject to the requirements validation process that covers all CCI devices. Potential users who think they require a SME PED should refer to the Concept of Employment to determine their eligibility and, if they qualify, forward their requirements through their chain of command. Procurement of the devices is funded by the requesting command and is limited to the existing NSA contracts.

The security posture of the SME PED relies to a great extent on user behavior to ensure that use of the device, particularly in classified mode, is limited to appropriate locations.

Future Use Cases

For now, SME PEDs only work when the proper commercial cellular network services and coverage are available. Three services are required: standard voice service, packet-switched data and circuit-switched data. This obviously limits their potential for shipboard use and other settings where the required cellular services are not available.

Future versions of the devices are expected to have wireless networking capabilities, such as WiFi or WiMAX, which, depending on how they are implemented, may facilitate the use of SME PEDs aboard ships or in forward deployed locations. This would potentially provide a smooth integration path for the devices into new environments, providing additional direct tactical warfighter support. CHIPS

For More Information

✓ Latest SME PED news and updates
www.doncio.navy.mil/telecommunications

✓ Device and ordering information
www.securephone.net

Mike Hernon is the former chief information officer for the City of Boston and currently serves as an independent consultant to the DON CIO on a variety of telecommunications topics.

Optimizing Telecom Usage While Cutting Costs

Telecommunications Expense Management in the DON

By Mike Hernon, Ken Brennan and Shirley Dolengo

The year was 1978 – the Bee Gees' "Night Fever" ruled the charts; "Mork and Mindy" first hit the airwaves; and it cost 15 cents to mail a letter, which people did a lot then because almost no one had e-mail.

That year also witnessed the drafting of a Department of the Navy (DON) telecommunications (telecom) policy that remains in effect today.

As you may imagine, policies from the 1970s regarding a technology as fast moving as telecommunications have lost their relevance over the intervening years. This disconnect between standing policy and reality is perhaps the best indicator that the telecommunications environment, which includes telephone and cellular services, as well as short haul data circuits, is ripe for improvement.

The environment serving the DON's Sailors and Marines, and those who support them, is a critical factor in mission success. As technology has continually advanced, the capabilities of the telecommunications devices and services used throughout the DON have dramatically improved as well; for example, compare today's mobile devices with those of just five years ago. As a result, the environment has become more diverse, more complex and more difficult to manage.

In response, the DON has developed a telecommunications optimization effort to ensure that these key assets meet mission requirements while being purchased, managed and utilized in a cost-effective and responsible manner.

Gaining Insight Through Automated Tools

Due to the complexity and volume of transactions that typify the DON's telecommunications environment, the use of automated telecommunications management tools is required for proper oversight and control.

Even with the existing tools in limited use, they are not consistently implemented, and they do not provide the end-to-end visibility, control and business intelligence required to support decision making, save money and deliver an optimized capability.

There are a wide variety of such tools available. Some provide day-to-day operational support by interfacing directly with telephone switches. Others are dedicated to expense management functions

such as invoice reconciliation. Still others deliver management information systems that provide analytical capabilities across multiple data sources to support a strategic analysis of the environment.

These tools are provided by a fairly large number of vendors and are available as single modules or in integrated suites. Unfortunately, there is not universal agreement among either the vendors or the users as to the precise definitions or desired capabilities of these tools.

From an enterprise standpoint, this lack of clarity raised the potential of multiple, uncoordinated tools being implemented that would not readily share information; would be expensive to support; and would still not provide the necessary insight into the telecom environment.

To avoid that scenario and best position the DON for the right suite of tools, the DON Chief Information Officer (CIO), in coordination with the Office of the Assistant Secretary of the Navy for Research, Development and Acquisition (ASN RDA), released guidance titled "Implementing Telecommunications Expense Management Tools in the Department of the Navy" on Jan. 28, 2009.

This guidance, in effect, instituted a strategic pause on the procurement of any automated tools until an enterprise strategy could be developed. While this guidance is in effect, the DON Telecommunications Working Group (DTWG) is developing a common set of definitions and capabilities for the DON.

The DTWG's work will provide input for updated guidance expected later this year. Thus the DON as an enterprise will be best positioned to gain the maximum benefits of these tools and make progress on its optimization goals.

Identifying Cost Savings

One of the primary benefits of implementing automated tracking tools is cost savings — money that can be freed up to provide more direct warfighter support.

Major cost drivers in the current environment are, in decreasing order, purchased equipment, personnel, connectivity charges and leased equipment.

The use of automated tools and the business intelligence they bring is expected to deliver savings across all these cost centers. Telecom industry studies show potential savings in the range of 12 to 30 percent for organizations that implement commercial off-the-shelf telecommunications management tools.

One good example of how an automated tool may identify opportunities to cut costs is with cellular phones and portable electronic devices such as BlackBerrys. A recent analysis conducted by ASN RDA showed that significant short-term cost savings could be garnered by optimizing the use of the available service plan options.

One indicator of this is the extremely low overage charges the DON incurs — less than 0.5 percent on average. Because the cost per minute for overages is relatively high, it is a common misperception that low overage charges represent effective cost control. In fact, the opposite is often the case due to overbuying minutes that are not used.

As shown in Figure 1, with a large surfeit of unused minutes there are no overage charges, but the funds expended are still twice as much as necessary. With more than 100,000 cellular lines billed every month across the DON, it is nearly impossible to recognize optimization opportunities like this without the support of automated tracking tools.

The DTWG Agenda

The DTWG's work will facilitate the availability of the right capabilities for the warfighter and the support structure while ensuring proper stewardship of public funds.

In addition to developing updated guidance on implementing automated management tools, the DTWG is evaluating the entire set of telecom polices — there are a number of policies 10 years old or more that are still in effect and have become outdated due to industry advances.

Other actions, such as drafting an updated governance framework; developing a Voice over Internet Protocol (VoIP) strategy; and aligning the enterprise with future Defense Department directions, among others, will support the delivery of an optimized and cost-effective telecom environment for the DON.

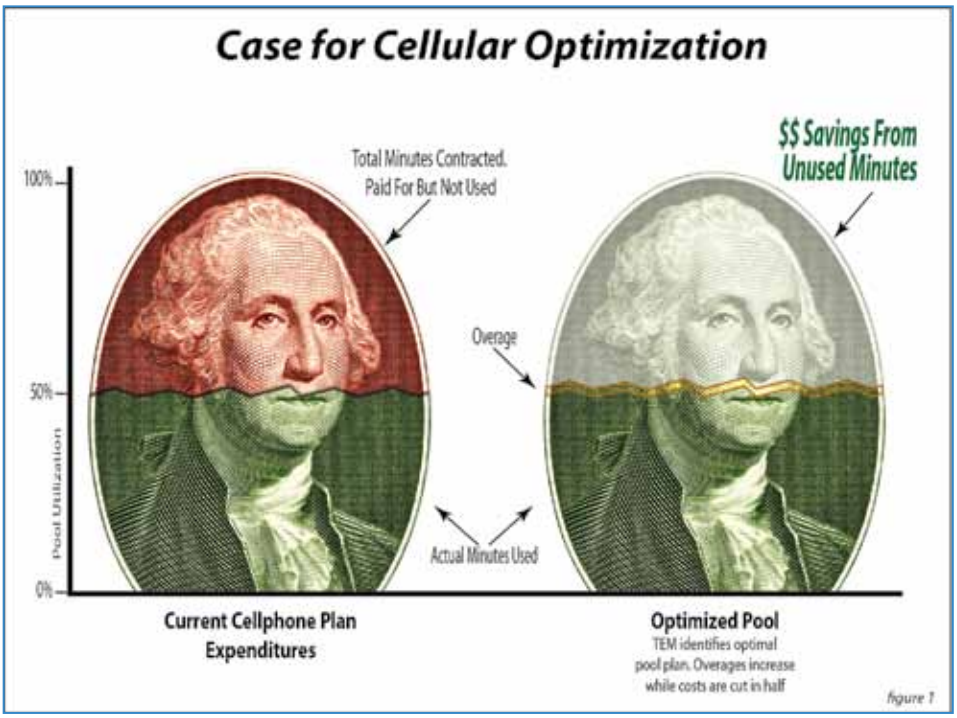
For the latest DON telecommunications news and policy updates visit: www.doncio.navy.mil/telecommunications. CHIPS

Mike Hernon is the former chief information officer for the City of Boston and currently serves as an independent consultant to the DON CIO on a variety of telecommunications topics.

Ken Brennan is an acquisition professional currently working Acquisition Program Assessment and Strategic Sourcing in the office of the Deputy Assistant Secretary of the Navy for Acquisition and Logistics Management (A&LM).

Shirley Dolengo is a retired Navy senior chief and the assistant program manager for the Navy's Shore Telephony Program.

Figure 1.



Q&A *with*

Vice Adm. Robert S. "Bob" Harward, Deputy Commander, U.S. Joint Forces Command
Rear Adm. Dan W. Davenport, Director, Joint Concept Development and Experimentation Directorate (J9), U.S. Joint Forces Command

Vice Adm. Robert S. "Bob" Harward

Deputy Commander U.S. Joint Forces Command Vice Adm. Robert S. "Bob" Harward and Rear Adm. Dan W. Davenport, director of the Joint Concept Development and Experimentation Directorate (J9) for USJFCOM, spoke to the media in a series of conversations about the Capstone Concept for Joint Operations (CCJO), a new warfighting concept prepared under direction of the Chairman of the Joint Chiefs of Staff and developed to describe the chairman's vision for how joint forces circa 2016-2028 will operate in response to a wide variety of security challenges forecasted in the Joint Operating Environment. The process to develop the CCJO was rigorous based on in-depth research of historical lessons learned, current operations and predictions outlined in the JOE.

JOE 2008 examines trends and disruptions in the geopolitical and military landscape, such as: shifting demographics; globalization; economics; scarce energy, food and water; climate change and natural disasters; pandemics; cyber threats; and the strategic importance of space.

Rear Adm. Dan W. Davenport

The concepts of the CCJO and JOE were tested in a series of seminar-style, joint-force war games held in McLean, Va. The war games began May 31 and concluded June 5. Results from the war games will be used to provide input into the Quadrennial Defense Review and also to shape future joint doctrine and training.

The war games look ahead to 2020 and feature scenarios that find U.S. joint forces up against three types of threats: a globally networked terrorist threat, a peer competitor, and a failed or failing state. Hybrid warfare, which includes a mix of warfare tactics, such as cyber threats, criminal activity and conventional warfare, is part of each scenario.

Participants in the war game series included former political leaders such as Newt Gingrich; multinational coalition members, such as British Army Lieutenant-General Graeme Lamb and Royal Australian Air Force Air Commodore John McGreely; retired combatant commanders such as U.S. Army General John Abizaid and U.S. Army General Gary Luck; five former ambassadors, such as Ambassador Robert Joseph; and current ones such as John E. Herbst, Coordinator for Reconstruction and Stabilization. Each of the services was represented by flag officers.

Interagency participation included the departments of State, Homeland Security, Justice, Commerce and Energy; Central Intelligence Agency; U.S. Coast Guard; Director of National Intelligence; National Security Agency; National Security Council; and the United States Agency for International Development.

The final conversation with the admirals took place about half way through the war game series.

Q: How do you know you have the right scenarios and are testing the right concepts?

Rear Adm. Davenport: We think the key to success in this war game is to have the right people involved and we do. First, you must have the breadth of experience and expertise and perspectives that you get from a collection of senior military officers, interagency senior leaders and multinational leaders. We have brought together a very select group to do this. Success will be based on the analytic foundation in development now to support the game.

Finally, we have a robust, dynamic, free-thinking regimen to make sure we really challenge ourselves, the ideas of the concept and solutions that the Blue Team is coming up with to make sure we are not too easy and really have the kind of debate we need for the concept itself.

We expect to have a final report developed by the end of July. The QDR is on a tight timeline, and we already are coordinating closely with the QDR. We are sharing information insights so that our war game is informed by the work that is already done. As soon as we get results, we will be able to feed that to the QDR folks as appropriate, so that we are able to help them along their timeline.

Q: What are you seeing midway through the game?

Vice Adm. Harward: There are four principles that we are hearing that are playing out significantly: major combat operations, security operations, engagement and reconstruction. In these scenarios, you may be limited to one reality or you may move through all four of those boxes. That is the significant difference; you are not going to be compartmentalized.

We have said that we are going to maintain our capabilities in major combat operations so this balance between that and our ability to deal with hybrid threats has to be incorporated into the force. The force needs to be prepared to deal with all those environments.

Q: I heard the word complexity frequently today concerning the national security environment and the various types of threats. How does that make your work more difficult?

Rear Adm. Davenport: The key is how that makes the joint forces task more difficult … We now have a hybrid threat. That is probably the most challenging one. It is a combination of conventional capabilities and an irregular adversary. We are dealing with a full spectrum of threats all at one time.

There is also the complexity of transitioning from conflict to stability to peacetime operations and back. All of those factors make up the complexity of the future environment.

Q: Do you think there may be a hurdle to clear in terms of trying to get all the services on board with your recommendations?

Rear Adm. Davenport: We think that the CCJO is a significant step forward in providing a foundation for joint concepts leading to joint doctrine that will allow the services to align their concepts and doctrine to the joint world. We are definitely moving in that direction.

The Army is already making progress in their capstone concept that is reflective of the CCJO. I think we will see real progress along that line.

All the services contributed and had a voice in the CCJO development. We think there is good buy-in. The service chiefs were all part of this discussion with the chairman, and it was formally vetted through that process. We have a solid foundation for all the services to align to.

Q: How is the war game going to take into account real-world complications such as multinational partners in the coalition having different rules of engagement and interagencies having different responsibilities and priorities?

Rear Adm. Davenport: I probably did not emphasize enough the participation of our interagencies and multinational partners because their perspectives and their realities are absolutely critical to the conduct of this war game. As the CCJO says, the military is just one instrument of national power; and, in many cases, it is not the preferred, depending on the challenge.

We recognize that the joint force is dependent on interagency and multinational success in order to generate the overall success we need. We realize that any solution we come up with has to include the interagency and multinational perspectives and their contribution to the solution set.

That piece of the participation group is particularly important. Our ROE (rules of engagement) differences and organizational differences will play out in the war game as the scenarios and the vignettes are presented to this group.

…The scenarios provide an environment where the players are allowed to identify the kinds of partnerships that they would need in order to effectively deal with the challenges.

Deputy Commander U.S. Joint Forces Command Vice Adm. Robert S. "Bob" Harward in a panel discussion at the Joint Warfighting Conference in Virginia Beach, Va., in May. USJFCOM leadership engaged in several media events to discuss the importance of the JOE and CCJO and symposium-style war games that followed in June to test the concepts outlined in the JOE and CCJO.

Q: Were there any requests from QDR folks about where they would like to see emphasis or any indication of what they want to see coming out of the war game?

Rear Adm. Davenport: The scenario timeframe is 2020 and that is in the middle of the window for CCJO. We have drawn from the scenario developers in the Pentagon and our own scenario developers to fill gaps not covered in the Pentagon scenario set. We have developed the Blue Force capabilities and the Red Force capabilities by drawing those from the services, the OSD (Office of the Secretary of Defense) and the Joint Staff experts in this field.

The specifics of the scenarios are less important than the challenges they represent. The collective challenges that these scenarios bring forth allow us to evaluate the CCJO and evaluate the joint force's ability to be versatile and to adapt as necessary to meet the variety of challenges.

Q: Does the media have a role in the war game?

Vice Adm. Harward: There is a recognition of how important it is to have that overarching blanket of Information Operations, both in the receive mode, in the transmit mode, proactively and reactively, being a major consideration in all of these operations.

… The 'battle of the narrative' is emphasized in the game and how we get that right is a major topic in most of the decisions and the discussions I am hearing through the war game.

Q: Gen. Mattis (USJFCOM commander) said that the joint force can't assume that there is going to be command and control in place everywhere in the future. Are you considering that in the war game?

Rear Adm. Davenport: We will be evaluating the command and control environment and cyber challenges, space challenges, and those things that take away our standard command and control capabilities. We have to be able to operate through those effectively.

Decentralization is a central theme to the CCJO and enabling our operators to take the [commander's] intent and operate. [The war game] is about the education and skill sets that are provided for our operators so they can effectively deal with these challenges with or without that large command and control structure.

Q: Are you making assumptions about what kind of technology will be available in 2020? Does technology have a role in the war game?

Rear Adm. Davenport: When you project out to the future, you are making assumptions. You look at what is planned in the program of record and what the services intend to develop and invest in over time and that becomes your foundation for the capability set for that timeframe. That's what we have been doing. Those databases developed in the Pentagon are our capability set.

Q: Both Defense Secretary Gates and General Mattis have said that where our dominance lies is in conventional warfare and the gaps and potential vulnerabilities are in irregular warfare. Could you talk a little bit about how General Mattis has spoken about how small units work in the concept?

Vice Adm. Harward: Sure. We've looked, especially as we deal with this hybrid threat, at the versatility, the flexibility, the connectivity of small units. What they allow us to do on the battlefield is a significant game changer. We have seen that from the onset of this conflict. Now, how do we codify that? How do we inculcate that in the general purpose forces? How do we train for that? I think a significant part of this is the training and education.

From the senior leaders, how you employ and work in that realm, how do you understand the flexibility down to your NCOs to make sure they get the education and commander's intent to be able to function in that realm when they lose communications. Do they have that right commander's intent?

Do they have that right understanding and the right authority and confidence in what they do to be able to function and deal with these threat environments? So I think that's the goal. I think there is a broad acknowledgement of what that brings to the battlespace. Now how do we drive that into the organizations and forces we have for the future?

Another example, which I know you are familiar with, is simulation. We have hundreds of millions of dollars in simulations for pilots to fly everything, and rightfully so. But have we done the same thing for those small units who are on the ground? Can we get them that same sort of corporate knowledge and experience before they are really in the battlespace?

A pilot has hundreds of hours of simulation before he actually flies. Can we get ground forces those hundreds of hours of combat experience in simulation before we place them in those environments? Those are some of the things we are going to do with our small unit program initiatives.

Q: Can you give some specific examples of the size of units you are talking about?

Vice Adm. Harward: We have not been that tactical in this realm. And we are leaving that up to the JTF commanders, to some extent, based on the capacity and capability. But it can be as small as one or two individuals forming joint fires, a JTAC, a joint terminal attack controller. Those sorts of elements and capabilities … medics, linguists, all those sorts of skills, we need in the battlespace, PRTs [Provincial Reconstruction Teams].

Do you give the PRTs the right sort of training and connectivity so they are now the supported element, not the supporting element in combat operations? So I think those are some examples. We haven't thrown those out in the vignettes just yet. We are leaving that to the JTF commanders to work through to determine what sort of skills and capabilities we need to meet the objectives of their scenario.

Q: What is happening when there is a lapse in C2?

Vice Adm. Harward: We are taking them off the net completely. We want to see what do you do then? Did you have the right education and training in place? The right commander's intent? Did you have those tools in place so they can still operate effectively and complete the mission when we lose those nets?

By the way, what are we doing when we lose the net? Do we develop that backbone of C2 so it's not just based on satellites — that you have an air leg, a ground leg, so that you have that triad of communications and command and control in place when you do lose the net. So all aspects of the scenarios take you through those three levels of effect.

Q: Which scenario is the toughest?

Vice Adm. Harward: I think they are all tough. When you are a joint task force commander and now it is all on your shoulders, you have to address all aspects of warfare. A lot of commanders have talked about deterrence. We have a great model for deterrence from the last 50 years — the Cold War. How does this deterrence work when we are dealing with non-state actors who are empowered with technology and weapons that have significant impact above the tactical and operational if not the strategic level?

Those are the challenges regardless of which scenario you face, especially as we see state actors using surrogates who have disavowed knowledge or connectivity and yet are empowered with assets that only a state actor can bring to bear.

Surrogates could be terrorist groups, but in some cases, not. For example, in cyber warfare, we know there are state actors, but there are also hackers, who are not terrorists, but surrogates in some cases.

Q: In addition to the C2 network that could go down, what other constraints are in the game?

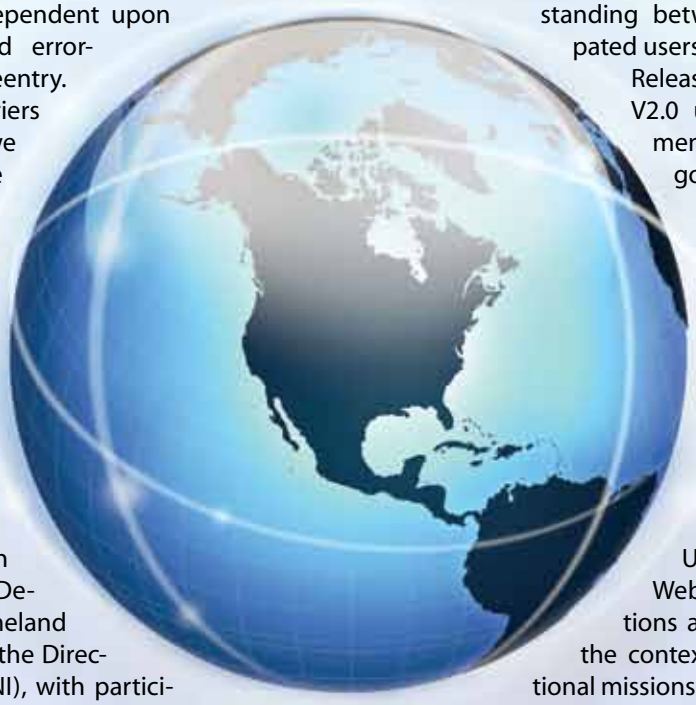
Rear Adm. Davenport: We can't get into specifics about the scenarios, but we can tell you that the cyber challenge is robust in each of the scenarios. It is forcing each of the Blue Teams to determine what kinds of capabilities they will need and how that may affect their operations and to push toward their ability to work in a network challenged environment. Decentralized operations with small units may be the only way you are effective. CHIPS

By Dan Green

Universal Core
Improving Information Sharing Across the Government

Uncertainty is the hallmark of 21st century national security. As proven time and again, no one organization or agency operates alone to address these challenges. It is through the efforts of many, both internal and external to government, that we find success. Partnerships may be predetermined, or completely unanticipated. To succeed, timely and trusted information must be accessible by the team and shared among mission partners. It is the sharing of information that lies at the heart of our future security.

The ability to share information remains hampered by data stovepipes and incompatible systems that cannot talk to each other. Sharing is highly dependent upon point-to-point connections, and error-prone manual data entry and reentry. What if we could break the barriers to information sharing? What if we could exchange basic data more effectively with our current infrastructure? How would we do that and what would it look like?



Historically, programs have defined their own vocabularies and information exchange schemas, limiting the amount of understandable information that can be shared outside of tightly coupled interfaces.

In 2007, the chief information officers from the departments of Defense (DoD), Justice (DoJ), Homeland Security (DHS) and the Office of the Director of National Intelligence (ODNI), with participation from the program manager for the Information Sharing Environment and the White House Office of Management and Budget, formed an Executive Steering Committee to address these issues. The committee was tasked to define requirements and develop an information exchange specification that could be used by all agencies and their information sharing partners. This specification is known as the Universal Core.

UCore V2.0 evolved from the successful information sharing efforts developed and adopted by UCore government partners and industry. The Navy accepted the role as DoD lead and has served as overall co-lead for the federal effort. The Space and Naval Warfare Systems Command is providing engineering leadership on behalf of the Navy. By leveraging lessons learned and reusing products and processes from various efforts, such as the National Information Exchange Model, Cursor on Target and Strike Community of Interest, the team kept costs low, maintained a demanding schedule and ensured UCore was compatible with existing infrastructures.

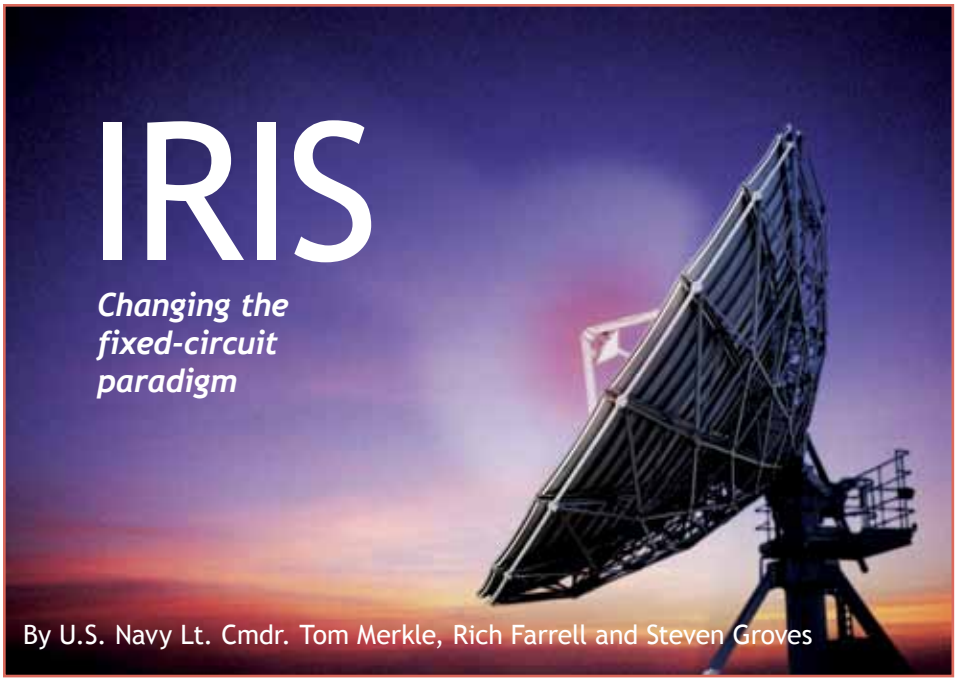
UCore enables information sharing by defining an implementation specification (XML Schema) that contains agreed upon representations for the most commonly shared and universally understood concepts of "who," "what," "when," and "where." UCore is simple to explain, understand and implement, containing a minimal set of objects with broad applicability across a wide range of domains. UCore is built on an extensible framework that permits users to build more detailed exchanges tailored to their mission or business requirements. The UCore validation processes and tools provide a means to consistently achieve definable levels of interoperability and promote machine understanding between anticipated and unanticipated users.

Released on March 31, 2009, UCore V2.0 ultimately involved almost 500 members from across the federal government and industry who contributed to its design, development, testing and evaluation over an 18-month period. This not only ensured the requirements from many stakeholders in the federal government were considered, but also significantly reduced risk and helped socialize the effort as it was being refined. Today there are more than 1,000 registered UCore users as noted on the UCore Web site, www.ucore.gov. Organizations are using or evaluating UCore in the context of a variety of important national missions including combating improvised explosive devices, ballistic missile defense, counterterrorism and maritime domain awareness.

UCore is breaking the barriers to information sharing both from a technical and an organizational standpoint. UCore has proven the ability of federal agencies to come together to solve complex information sharing issues despite organizational and financial boundaries.

In January 2009, DoD, DHS, DoJ and ODNI were honored by the Institute for Defense and Government Advancement for their collaborative work on UCore and its contribution to network-centric warfare. This is a tribute to the strong leadership provided by the federal CIOs, the commitment of the services and agencies in the partner departments, and the incredible technical talent that coalesced around this small but important effort from all levels of government and our industry partners. CHIPS

Dan Green is the DoD co-lead for UCore.



IRIS

Changing the fixed-circuit paradigm

By U.S. Navy Lt. Cmdr. Tom Merkle, Rich Farrell and Steven Groves

U.S. Navy and Marine Corps command, control, communications, computers and intelligence (C4I) communities face a major obstacle in fielding a true net-centric capability to the warfighter due to inadequate throughput to disadvantaged and remote users. But help is on the way.

Industry partners, in collaboration with the Defense Department, will launch and operate the Hosted Payload-Internet Routing in Space (IRIS) on Intelsat's IS-14 satellite scheduled for launch from Cape Canaveral in late summer 2009.

Since IRIS is a commercially owned and operated venture, the cost of the satellite, launch and payload are funded by a private sector group, led by Cisco Systems Inc. and Intelsat General Corp.

IRIS represents the next generation in telecommunications satellite services with an ability to reach into space. IRIS will cover Europe, Africa and the Americas from its 45-degree orbital slot over the Atlantic Ocean.

The IRIS payload will provide the ability to merge ground and space communications infrastructure with Internet Protocol (IP) — the common frame of reference between networks. Figure 1 illustrates the IRIS topology.

U.S. Strategic Command has tasked Army Space and Missile Defense Command Future Warfare Center (SMDC-FWC) in Colorado Springs, Colo., with determining if a commercial Internet hub in space would dramatically improve net-centricity for strategic, operational and tactical units of the DoD, and joint, interagency, intergovernmental and multinational (JIIM) partners.

To this end, experts from SMDC-FWC are monitoring, collecting and assessing data associated with the IRIS venture during pre-launch preparations. They will also conduct a final operational demonstration after the IRIS package is on orbit.

The IRIS Hosted Payload program was accepted by the Defense Department as a fiscal year 2007 Joint Capability Technology Demonstration (JCTD). The demonstration will examine the potential utility of augmenting joint, interagency, intergovernmental and multinational information transport with space-based IP routing and processing.

The IRIS JCTD represents a new model for government and industry collaboration. This relationship will allow the DoD to examine, demonstrate and assess the utility of IRIS' capability and potentially transition this capability to U.S. forces both at home and abroad.

The IRIS JCTD will provide an operational utility assessment and a recommendation to the Office of the Secretary of Defense regarding the operational impact of the IRIS venture. If IRIS has utility for the DoD and JIIM community, the JCTD will execute a contract mechanism for the Defense Information Systems Agency (DISA) to procure IRIS services.

On-orbit assessment of the IRIS payload begins fall 2009. The primary players for the on-orbit assessment are Joint Interagency Task Force (JIATF) South in Key West, Fla.; U.S. Southern Command in Miami, Fla., and elements of the Royal Netherlands Navy (RNLN), including Commander Task Group 4.4 in Curaçao, Netherlands Antilles.

Testing during counter-narcoterrorism operations in the JIATF South operations area is scheduled to be conducted both ashore and underway on the Royal Netherlands Navy warship HNLMS Amsterdam (A836).

The SATCOM Bottleneck

Much has been done to increase available bandwidth and throughput via military satellite communications (MILSATCOM); however, the gap between end-user requirements and available capacity is growing faster than anticipated.

No significant reduction in this gap is expected to begin until the next generation of MILSATCOM is available. In the meantime, military forces must either accept the disparity between requirements and existing MILSATCOM capacity, or shift throughput to commercial satellite providers.

Between 60 to 80 percent of all DoD satellite bandwidth in the beginning stages of Operations Iraqi Freedom and Enduring Freedom was provided by commercial satellite. COMSAT proved to be an important part of providing connectivity to the warfighter. However, the long-term cost of commercial satellite service remains prohibitive.

The COMSAT market has also become tighter in recent years because new users have emerged and companies and governments worldwide have increased their use of services at a faster pace than new capacity has been added.

In addition to the high cost, there is another constraint: Most COMSAT services are provided through a "bent-pipe" architecture. This means that data transmitted to the satellite is sent right back down like a bent pipe to fixed gateways to the Global Information Grid (GIG) on the ground. The only processing done by the satellite is to retransmit the signal. The gateway architecture creates throughput problems because different sized military units use

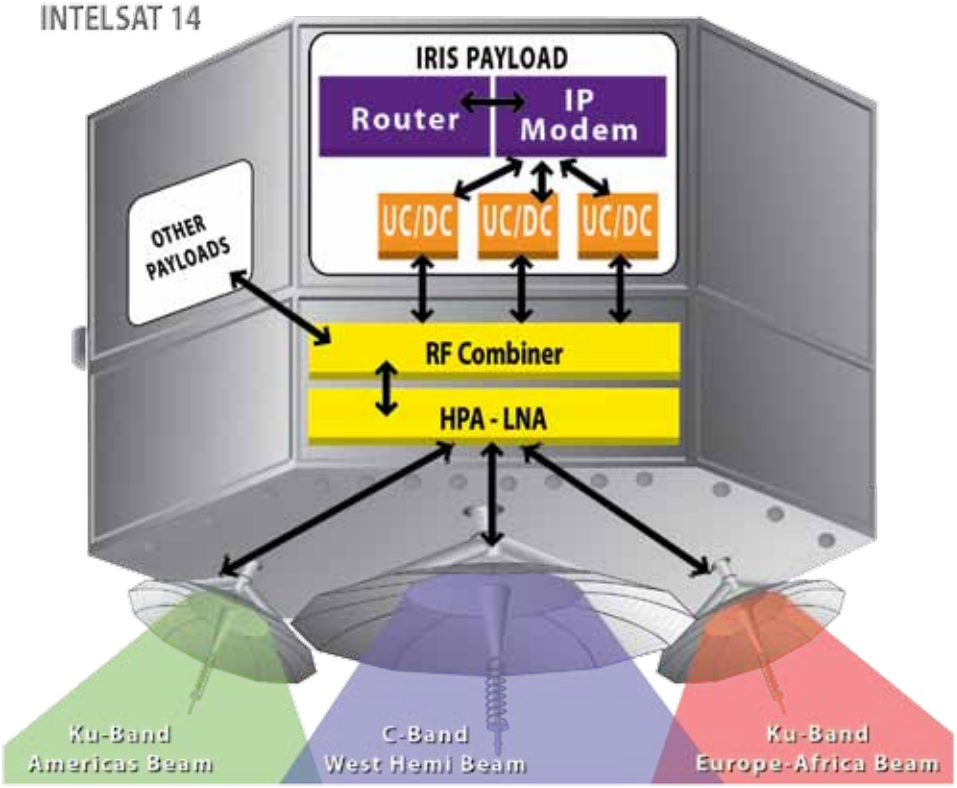


Figure 1.

varying satellite systems, frequencies and gateways to access the GIG.

This smorgasbord of systems requires multiple frequency conversions, digital processing, routing via terrestrial networks and additional satellite links between distant ends. The result is that IP-based network traffic between a flagship and a destroyer just a few miles away may require multiple hops through different satellites and ground networks prior to arriving at its destination.

Each of the steps adds delay and latency and lowers effective throughput, especially to small disadvantaged units.

Bottlenecks Affect Missions

The resulting low throughput makes it difficult to provide shore-based networks and network enclaves, such as the classified SIPRNET, to the small maritime unit. The DoD has been able to overcome some aspects of this problem via Web-based tools such as Collaboration at Sea.

CAS is based on the IBM/Lotus collaboration toolset and is used mostly to support operations with coalition partners. CAS and other network traffic reduction methods have helped to integrate the small unit into the networked battle. However, there is no solution for high throughput requirements at the heart of net-centric operations, including transmission of high-resolution imagery, full-motion video and video teleconferencing for telemedicine.

This C4I bottleneck is daunting enough for traditional U.S. command and control networks, but it intensifies when integrating multinational organizations and governments, interagency partners, and military coalitions and allies of varied technological and financial resources.

In general, multinational organizations and coalition partners cannot afford to devote sparse satellite bandwidth to multilateral networks such as the Combined Enterprise Regional Information Exchange System (CENTRIXS.)

This makes tasks that are taken for granted at a land-based headquarters insurmountable for deployed ships and small units. For example, simply e-mailing a photo of a suspect vessel to a coalition warship on patrol may be impossible or so delayed that tactical value is lost.

The Fixed-Circuit Paradigm

There are two main reasons why small and disadvantaged units experience low throughput: a rigid satellite subscription fee structure and large antenna size. The bent pipe architecture requires a continuous, fixed satellite link between the gateway on shore and the forward-deployed unit when the circuit is connected.

Since the frequencies, channels and power amplification that a single COMSAT can support are fixed at launch, the cost of the satellite and launch is recovered in the access fees paid over the life of the satellite. The architecture also generally requires large, bulky antennas and even multiple antennas for multiple bands.

Bent pipe communication channels must be reserved ahead of time and cost the same regardless of the amount of data passed over the transponders. Whether a unit uses 90 or 10 percent of the licensed throughput, the full channel is reserved.

Even mobile systems, such as Inmarsat B, require that the circuit be dialed in and fully "on charges" to be connected. This results in a high cost of doing business for deployed units, ships, combatant commanders and the shore-based communication providers that support them.

To keep the cost and antenna size to an acceptable level for various commercial and government customers, the COMSAT industry provides the minimum acceptable throughput for the majority of its customer base. For example, Inmarsat B provides voice services, telex services, medium speed fax and data services at 9.6 kilobits per second (Kbps) and high speed data services at 56, 64 or 128 Kbps.

To minimize cost, combatant commanders and communications planners provide COMSAT access only to the tactical units that are deployed on a day-to-day basis. However, network throughput requirements can vary dramatically over the course of a day and even over the course of an hour. During a crisis or surge period, a narrow channel presents the same slow response time and the same low throughput regardless of need.

Meanwhile at low demand times, the full channel is being maintained but underutilized — at the same high price. Another complication arises in preparing for a surge or contingency requirement. The lead time for commercial satellite service provisioning is considerable. It can range from several months to several years in advance.

In the event of a critical requirement, there may not be sufficient channel availability in the crisis area to provide services to deployed ships and units.

Communications architectures using IRIS have the potential to overcome many of these issues. By providing digital processing on orbit and multiple bands of service, the IRIS payload can reduce antenna size requirements, particularly for maritime units.

But, the most important IRIS capability lies in the promise of dramatically better flexibility for requirements planning, lower overall cost per bit and a higher throughput to the disadvantaged unit.

If the IRIS payload is able to deliver on these promises, the result would be improved connectivity, more affordable bandwidth and more flexibility in operations with JIIM partners.

Changing the Paradigm

Lack of flexibility is a problem with fixed-circuit paradigms, whether satellite or land-based, and it has a major effect on the cost of bandwidth. For a comparison with land telephony, consider the difference in cost between an Internet service provided T1 line versus a 1.5 megabits per second (Mbps) digital subscriber line.

Whereas the T1 line averages $500 to $600 in cost per month, DSL from the same company averages $50 to $60 per month for the same throughput.

The difference in price is primarily due to oversubscription which allows underutilized bandwidth to be shared among users. Since not all customers require the full 1.5 Mbps throughput at all times, a telecommunications provider can provision much less total throughput on the back-end than a fixed circuit would require.

When applied to satellite services, under the current fixed-circuit paradigm, providing services for 40 satellite customers at the relatively low rate of 128 Kbps requires 40 different channels for a total satellite throughput of 5.12 Mbps.

On the other hand, with modest oversubscription ratios of 5-to-1 or 8-to-1, that same 5.12 Mbps of satellite capacity would allow 10 512 Kbps channels, which can support between 50 to 80 customers, and yet each customer would effectively experience the higher rate of 512 Kbps.

More customers can be serviced at a far higher throughput. In addition, since customers use the system on demand rather than continuously, they can be charged on the basis of actual data services used, rather than access fees.

This concept has been difficult to implement for traditional bent pipe satellite services due to the high latency between the distant end and gateway and the larger antenna size that a higher bandwidth connection requires. By reducing antenna size and harnessing the inherent flexibility of IP routing, a COMSAT with IRIS capability could eliminate the resourcing and scheduling difficulties of provisioning adequate throughput for contingency and surge requirements.

IRIS Operational Demonstrations

The IRIS JCTD has already performed two of four planned operational demonstrations. Because OD 1 occurred prior to satellite launch, it focused on characterizing space router performance, which was emulated at MIT's Lincoln Laboratories in July 2007.

In preparation for the maritime and terrestrial nodes required for demonstration, SMDC-FWC and the U.S. Coast Guard Pacific Area conducted OD 2 in September 2008. USCGC Sherman (WHEC-720) used existing domestic Ku-band satellite services and simulated the IRIS payload on land at a San Diego teleport. The simulation effectively quadrupled the available throughput using the same size antennas the Sherman uses with its existing legacy SATCOM service.

The Sherman became the first cutter to perform a high-quality video teleconference between ship and shore, including a live video interrogation of an individual of interest on the ship by an interpreter based on shore.

The critical lesson learned was that linguists could be based anywhere in the world and conduct a real-time interview of a suspect in custody on an underway vessel.

The ship was also able to rapidly upload and download multiple large PowerPoint files, images and documents, which required huge amounts of bandwidth, proving that the increased throughput could improve operational planning and communications.

The final demonstration is scheduled for fall 2009. It will test the performance of on-orbit IRIS services and the operational impact of an Internet hub in space for secure and multilateral IP-based networks. The test will involve communications between multiple land sites across the Caribbean and aboard HNLMS Amsterdam.

The key land nodes are JIATF South, USSOUTHCOM and Commander Task Group 4.4 headquarters. The demonstration will include providing tactical data and services to the HNLMS Amsterdam that are currently available only to shore-based sites.

The tactical data are expected to enhance the capability of the HNLMS Amsterdam to support counter-narcoterrorism operations in the JIATF South area of operations. Capabilities include coalition encrypted CENTRIXS, a live video broadcast of the daily situation briefing, video teleconferencing, Voice over IP, and transfers of daily operations briefs and images usually only available to shore-based networks. The Amsterdam crew will also enjoy robust Internet access at sea.

Without reliable, robust bandwidth, simply e-mailing a photo of a suspect vessel to a coalition warship on patrol may be impossible or so delayed that tactical value is lost.

The Road Ahead

As Internet and networking technology continues to proliferate on a global scale, commercial Internet hubs in space like IRIS will likely become commonplace.

Once IP routers are deployed on geostationary commercial satellites, a truly net-centric capability may be available to the disadvantaged and small maritime unit for the first time. CHIPS

Lt. Cmdr. Tom Merkle is the chief for C4I systems engineering for JIATF South.

Mr. Rich Farrell is a senior analyst with Camber Corp. providing support to SMDC-FWC.

Mr. Steven Groves is a lead scientist with Camber Corp. providing support to SMDC-FWC.

GOING MOBILE

The Choice Between Wired and Wireless

By Tom Kidd, Department of the Navy, Director of Strategic Spectrum and Wireless Policy

Whether wireless voice, video or data, the number of wireless applications is increasing. Wireless capabilities can be as simple as a wireless doorbell system or as complex as a naval unmanned aerial system providing real-time intelligence to forward-deployed Marines and Sailors.

While the use of wireless systems is certainly advantageous for mobile requirements, wired systems retain a number of inherent benefits for non-mobile, transportable or nomadic requirements.

Both wired and wireless connectivity have advantages and disadvantages that should be evaluated whenever new capabilities are considered. "One Size Fits All" is not a solution for every Navy or Marine Corps requirement.

Wired and wireless solutions each possess inherent risks and benefits that should be considered whenever a transmission medium is selected. And while some risks and benefits are obvious, others are not immediately apparent until a thorough comparison of capabilities, benefits, risks and rewards is made.

Cost. Cost benefits associated with wired and wireless transmissions were often dramatically different a decade or more ago. A copper "wired" solution was generally less expensive than many wireless capabilities, while fiber optic and its associated equipment were generally more expensive than wireless systems.

However, these broad rules of thumb no longer apply. Recent technological developments and production capabilities have significantly reduced the cost of wireless and fiber optic equipment.

Determining the "best buy" for wired or wireless systems now requires consideration of installation requirements and associated costs, as well as maintenance requirements and technology refresh costs.

Accordingly, the total cost of ownership must be developed to determine the most economical transmission media to support connectivity requirements.

Security. Security risks must be an upfront driver for determining wired or wireless use. Security considerations include cryptographic requirements and information assurance (IA) requirements.

Additionally, physical security requirements, including access to transmission lines or transmission points, such as towers, antennas and associated equipment, must be considered.

Depending on the capability requirement, security issues may be complex. Wired and wireless transmission media have previously been chosen with little if any security considerations.

However, today's digital capabilities generally necessitate layered security measures to ensure networks and standalone systems are protected from physical, as well as internal and operational damage.

Potential information compromise must also be considered when addressing security issues. It may not be easy to determine the best alternative between wired and wireless due to unique security issues among voice, video and data transmissions.

Wireless operations are generally thought to have greater security concerns than wired operations due to radio propagation characteristics; however, both mediums are susceptible to intrusion if security issues are not adequately addressed.

Reliability. All Department of the Navy voice, video and data requirements include mandates for reliable solutions that minimize downtime. Downtime not only results in service loss to users but also increases maintenance and reinitiation activities.

A number of factors affect system reliability including environmental, electrical and maintenance issues, in addition to other considerations. Reliability, in many ways, is similar to system security; reliability can be impacted by issues that appear insignificant or are overlooked.

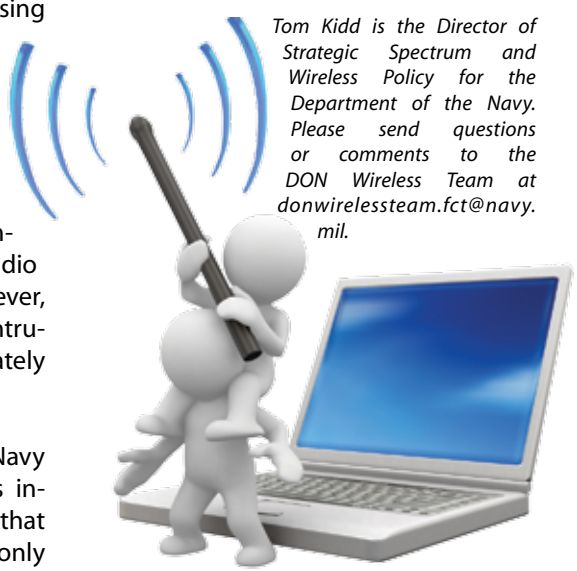
While wired systems may seem to offer the greatest reliability, they are subject to vulnerabilities that wireless systems are not. Some common issues that often impact the reliability of wired systems are severe weather conditions, which can destroy cables, or digging equipment and tracked vehicles, which can cut cables.

Wireless systems have intentional and unintentional radio frequency interference vulnerabilities as well as signal coverage challenges.

The Navy and Marine Corps will continue to use both wired and wireless systems for communications, intelligence and other naval requirements.

The choice between wired and wireless, given the option, is not an easy or obvious decision. CHIPS

Tom Kidd is the Director of Strategic Spectrum and Wireless Policy for the Department of the Navy. Please send questions or comments to the DON Wireless Team at donwirelessteam.fct@navy.mil.



Full Spectrum

By Tom Kidd, Department of the Navy, Director of Strategic Spectrum and Wireless Policy

New rules create sharing between federal and non-federal radio systems

The National Telecommunications and Information Administration (NTIA) Interdepartment Radio Advisory Committee (IRAC) recently approved an addition to the Manual of Regulations and Procedures for Federal Radio Frequency Management. The new paragraph, 8.2.47, enables federal and non-federal agencies to share radio systems. Navy and Marine Corps first responders may have an opportunity to dramatically expand their geographic coverage without the prohibitive cost of building additional infrastructure. This change in governance charts a new course away from federal and non-federal agencies jealously guarding their allotted spectrum. Before this change, sharing among federal and non-federal radio systems was extremely difficult and as a result, rare.

The electromagnetic spectrum, which these radio systems utilize, is a sovereign resource of every nation to manage as they see fit. The United States manages spectrum usage under two sets of rules, one for federal government agencies, such as the departments of the Navy, Justice and Homeland Security, and one for non-federal agencies, including state, local and tribal police; fire and ambulance services; business radio; broadcast television and radio; and more.

United States Code further separates portions of the radio spectrum into frequency bands for exclusive use among federal users, and other bands for exclusive use among non-federal users. Even though there may be no operational restriction to sharing frequency resources, these regulatory limitations made it difficult, if not impossible, to share radio systems between federal and non-federal users.

The Department of the Navy Chief Information Officer (DON CIO) will lead a push to expand Navy and Marine Corps systems to take full advantage of this new opportunity. All Land Mobile Radio System (LMRS) operators are encouraged to evaluate their current service area and determine if their system coverage and capabilities may be expanded under the new rules. Many systems may be able to expand their service area with minimal or no new equipment. Navy and Marine Corps land mobile radios may already be capable of taking advantage of non-federal frequency bands.

Sharing among federal and non-federal radio systems involves a three-step process. First, the federal and non-federal users must agree to share. This agreement is then coordinated with the IRAC to ensure it adequately addresses the needs of the government, including the return of federal frequencies if all federal users withdraw from the system or if the federal frequencies are no longer available for non-federal use.

Second, the federal user must submit technical information about the non-federal system to the IRAC to certify that it is in compliance with other rules governing federal radio systems. And lastly, the federal user requests the federal equivalent to a radio frequency license in the non-federal frequency band.

The exact process and procedures, in paragraph 8.2.47 of the NTIA Manual, are reprinted in the text box on the next page. However, as of press time, the NTIA Web site had not been updated with the newly approved paragraph.

State, local and tribal radio system operators are also encouraged to explore how they will share in this new opportunity.

Sharing spectrum is an alternative to spectrum reallocation. Over past decades various actions have been taken to reallocate spectrum among federal and non-federal users. The process of migrating operations out of one frequency band and into another requires considerable time and resources.

Spectrum is critical to our nation's economy and security. Sharing empowers all users to efficiently and effectively execute their careful stewardship over this finite resource. CHIPS

Tom Kidd is the Director of Strategic Spectrum and Wireless Policy for the Department of the Navy. In addition to "Full Spectrum" (formerly called "Can you hear me now?"), he also authors the recurring CHIPS magazine series "Going Mobile" which focuses on enterprise mobility and the DON Wireless Working Group.

8.2.47 Shared Federal / Non-Federal Radio Systems

The term "shared system" as used in this section means a radio system using one or more frequencies authorized by the NTIA and one or more frequencies licensed by the FCC. "Agreement" or "Agreements," as specified in this section refer to Memorandums or Letters of Understanding or Agreement between federal agencies and non-federal partners. Shared systems may be authorized under the following conditions (Operations conducted under Section 7.3.6 or Part 7.12 of the Manual, which allow a federal radio station to utilize any frequency authorized to a non-federal radio station under specified conditions, are exempt from this policy.). The federal agencies signing the Agreement shall:

a. prior to signing any Agreement, submit to the IRAC, for information and planning purposes, a copy of any Agreement which has been coordinated between the parties to the Agreement. The Agreement shall state that it is contingent on NTIA's approval of any supporting certifications, authorizations, or modifications. The Agreement shall contain conditions for the return of frequencies authorized by NTIA in the event that NTIA determines that: the frequencies can no longer be made available for non-federal use, all federal participants withdraw from the shared system, or the return is required for convenience of the government.

b. obtain spectrum certification from NTIA prior to requesting authorization for frequency assignments from NTIA.

c. in accordance with the procedures specified in Chapter 10, submit a request for system review to the Spectrum Planning Subcommittee (SPS) for the proposed shared system and obtain NTIA Certification of Spectrum Support. The following information shall be submitted to the SPS: In accordance with Section 10.1.3 of the NTIA Manual, a request for certification of spectrum support for the proposed system; a frequency plan for federal spectrum access requirements; and a copy of the signed Agreement between the requesting federal agency and the non-federal system partner. If equipment to be used by the federal agencies has already been certified, it is sufficient to provide the SPS numbers of the certifications in lieu of detailed equipment characteristics. Upon receipt of NTIA certification, agencies may submit requests for permanent frequency assignments or modification to existing assignments to support the shared system.

d. apply for frequency authorizations in accordance with Chapter 9 of this Manual. In addition, federal agencies:
   (1) shall obtain authorizations from NTIA for all frequencies (regardless of the frequency band) that will be used by federal stations;
   (2) may request authorization for a band assignment vice discrete frequency assignments for spectrum used by the shared system and allocated for non-federal use, e.g., 150.8-162.0125 MHz;
   (3) shall make the non-federal partner aware that, in order to have access to spectrum allocated to the Federal Government, the non-federal partner must obtain an FCC license through the normal FCC licensing process (this application will be coordinated by the FCC through the Frequency Assignment Subcommittee); and
   (4) shall include in their proposals:
      (i) Remarks line that shows the joint operations by the agency, non-federal, and other agencies:
      Example: REM05 *JNT, I , NG ,J , A ,DHS
      (ii) Information in the supplementary details identifying the agreement reached between the federal agency(ies) and non-federal partners:
      Example: SUP01 DOl and Wyoming Agreement 6 Dec 2006
      (iii) Special Note S402:
      NTS01 S402
      (iv) *NTS, M015 entry with the IRAC and SPS document numbers for this system:
      Example: REM07 *NTS,M015,IRAC,XXXXX,SPSXXXXX
      (v) Paired frequency data referencing the system-wide FCC spectrum band assignment:
      Example: REM03 *PRD,M150.8000,I 080001
      (vi) Supplementary remarks listing each maritime frequency or two-digit maritime channel number used, if maritime frequencies are included in a band assignment:
      Example: SUP02 Marine Channel XX included in band assignment
      (vii) When a band assignment is used for spectrum allocated for non-federal use, the assignment must list the individual frequencies in the supplementary details or reference an FAS document that contains the individual frequencies in the circuit remarks MOOI entry:
      Examples:
      SUPOI FCC licensed frequencies in use, MXXX.XXXX,
      REM05 *NTS, MOOI,FAS,XXXXX

e. have (1) an assignment for each frequency which is allocated on a primary basis for federal use; and (2) individual assignments or a band assignment for operations allocated on a non-primary basis for federal use.

f. ensure that the non-federal partner has FCC licenses for operations on frequencies which are allocated on a primary basis for federal use.

Annex A
A.6 Special Notes
S402--This assignment has been made pursuant to Section 8.2.47 of the NTIA Manual for a shared federal/non-federal radio system.

Reprinted from NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management

Detecting Conventionally Powered Submarines

Team SPAWAR contributions to the DESI and Maritime Strategy

By Frank Bantell, José Carreño, George Galdorisi and Russell Grall

Since the end of the Cold War, the antisubmarine warfare challenge changed from one focused on prosecuting nuclear-powered submarines in deep oceans, to finding conventionally powered vessels operating in the shallow, littoral regions of the world. The need to train against this threat is palpable. The solution today is the Diesel Electric Submarine Initiative.

Begun in 2001, DESI grew out of a necessity for realistic antisubmarine warfare (ASW) training against the emerging threat of conventional submarines. Relatively inexpensive, conventional submarines constitute a threat entirely out of proportion to their cost and numbers. Once underway, the stealth capability of these assets requires an inordinate amount of resources dedicated to finding and prosecuting their threat.

To underscore this point, during the Falklands War, the Royal Navy committed a fair portion of its resources to finding the ARA San Luis (S-32), a Type 209 diesel-powered submarine of the Argentine Navy, known to be operating north of the Falklands. Despite considerable effort by the Royal Navy, the San Luis successfully evaded detection, returning safely to its homeport of Mar del Plata, Argentina.

Over the last several years, the number of conventionally powered submarines has proliferated, with more than 370 submarines spread across 39 countries, many of these in the Pacific Rim region, and many of them in the hands of nations who are potential rivals of the United States.

Following the dissolution of the Soviet Union, U.S. naval strategic thinking transitioned from blue water operations to power projection and the employment of naval forces from the sea to influence events in the littoral regions of the world.

The two Navy strategic documents are "From the Sea and Forward …" and "From the Sea." The notion of projecting power into the littorals was ultimately incorporated into the Navy's vision document, "Sea Power 21," issued in 2002.

Focused on "projecting decisive joint capabilities," Sea Power 21 would "continue the evolution of U.S. naval power from the blue water, war-at-sea focus of the 'Maritime Strategy' (1986), through the littoral emphasis to a broadened strategy in which naval forces are fully integrated into global joint operations against regional and transnational dangers."

Sea Power 21 remains the Navy's vision to this day, and the ways and means to achieve its ends are set forth in the nation's maritime strategy, "A Cooperative Strategy for 21st Century Seapower." Influencing events ashore therefore remains an overarching strategic imperative, and sea control into the littoral regions requires a robust ASW capability.

Organized under U.S. Fleet Forces Command, DESI provides the U.S. Navy's surface and subsurface assets with realistic training against conventionally powered submarines.

Unlike Soviet nuclear submarines that were relatively noisy and could be detected with passive sonar, modern diesel–electric submarines are much harder to detect, particularly in the littoral regions where sea life and merchant shipping can mask their presence.

Without diesel-electric submarines of its own, the U.S. Navy has turned to partner nations to provide a credible, realistic opposition force. The demand for training against these types of threats has grown and become a key element of strike group ASW training certification.

Conducted on both the U.S. East and West Coasts, DESI participants primarily include South American navies, such as Brazil, Chile, Colombia and Peru, with Argentina expected to participate in 2010.

Thus, aside from actual training, DESI promotes a key pillar of the Maritime Strategy, that of fostering international trust and cooperation. Specifically, the Maritime Strategy notes that "expanded cooperation with the maritime forces of other nations requires more interoperability with multinational partners possessing various levels of technology." A key part of this effort is the Global Maritime Partnership, an initiative intended

SAN DIEGO (April 30, 2009) The Peruvian Navy submarine BAP Arica (SS-36) prepares to moor to a pier at Naval Submarine Base Point Loma. Arica is the first Peruvian submarine to pull into San Diego Bay and is participating in the Diesel Electric Submarine Initiative (DESI). The DESI program is a U.S. Navy partnership with South American countries and supports their diesel-electric submarine operations and fleet readiness events in operating areas off the U.S. East and West Coasts. Participating DESI partners include Colombia, Peru, Chile and Brazil. U.S. Navy photo by Mass Communication Specialist 2nd Class Derek R. Sanchez.

to serve as a "catalyst for increased international interoperability."

Achieving interoperability constitutes not only a cornerstone of the Maritime Strategy, but a necessity for successful training engagements like DESI. In that regard, one of the biggest challenges has been that of communications between U.S. and South American assets while underway that goes beyond language barriers and into the technical realm.

To bridge this gap, DESI leveraged the Combined Enterprise Regional Information Exchange System (CENTRIXS), a coalition communications network, in support of 2008 and 2009 DESI events in San Diego. Team SPAWAR, Space and Naval Warfare Systems Command, implemented this vital communications component.

Shortly upon arrival to Naval Submarine Base in Point Loma, personnel from the Space and Naval Warfare Systems Center Pacific (SSC Pacific) successfully installed and trained CENTRIXS on the Type 209 Peruvian submarine, BAP Arica (SS-36), as well as at the Peruvian Navy's Submarine Headquarters in Callao, Peru. Each installation took approximately two days to complete, demonstrating both the mobility and flexibility with which the deployable systems used to connect partner nations to the CENTRIXS coalition network can be installed.

The team coordinated closely with U.S. Naval Forces Southern Command (NAVSO), Commander, Submarine Force U.S. Pacific Fleet (COMSUBPAC), and Commander, Submarine Squadron 11 prior to the installation to ensure operational objectives would be met.

For the past two months, the BAP Arica has been using CENTRIXS to communicate with Peruvian Submarine Headquarters as well as COMSUBPAC in Hawaii via secure chat and e-mail. Releasable security devices were used in both installations allowing the BAP Arica to sail without the need for U.S. Navy ship riders, thus saving U.S. naval resources.

This is the second time CENTRIXS has been used on a diesel-electric boat. The first was Chilean Submarine (CS) Simpson (SS-21) in September 2008 while Simpson was also participating in the DESI program. This year's efforts, however, mark the first partner nation submarine headquarters to be enabled with CENTRIXS.

The strength of CENTRIXS is in its ability to permit highly secure communications between the United States and partner nations. This capability is critical to all installations and has been a focus area of SSC Pacific for several years, involving close coordination with the fleet, combatant commanders and other agencies, to resolve technical issues and seek the appropriate approvals.

Services normally available for high bandwidth platforms include chat, e-mail, Web services, Common Operational Picture and Voice over Internet Protocol enabling real-time secure information exchange between units. However, for the DESI installs, extremely mobile, small footprint, low-bandwidth CENTRIXS Portable Operations Kits (CPOK) were used.

The CPOKs were developed by SSC Pacific, in conjunction with industry, and were first deployed in 2006 during the Southeast Asia Cooperation Against Terrorism (SEACAT) exercises.

CPOKs facilitated communications between smaller partner nation ships, achieving navy-to-navy communications between U.S. and four Southeast Asia partner nations.

As a result of the limited bandwidth, only chat, e-mail and a geographically filtered COP are normally deployed with a CPOK install. However, these three applications are the cornerstone of the collaboration toolsets allowing the ships to maintain 24/7 situational awareness with any other CENTRIXS enabled units. The appeal of using a CPOK comes from its ease of use and low up-front hardware costs of just under $10,000.

The CPOK is one of a variety of different fly-away kits that SSC Pacific provides to enable the fleet and partner nations to connect to CENTRIXS.

SSC Pacific, in conjunction with Commander, Pacific Fleet and other naval organizations, has managed and executed more than 50 installations and removals in each of the past three years. As noted in an article from the January-March 2008 issue of CHIPS, "Supporting a Cooperative Strategy for 21st Century Seapower through Interoperability" (www.chips.navy.mil/archives/08_jan/web_pages/Seapower.html), this effort represents one facet of Team SPAWAR's ongoing contribution to enabling the interoperability necessary to fully realize the Global Maritime Partnership.

With the program now in its eighth year, and its imminent expansion in 2010 with the expected participation of Argentina, DESI stands as an example of viable cooperation in the Americas. Expanding participation to other nations can broaden the span of cooperation, and provide U.S. forces with a more diverse set of submarines for honing their skills.

Widely exported throughout South America, German-built Type 209 submarines have been the primary asset employed during DESI. Exercises with other submarine designs, such as the Swedish Navy HMS Gotland, leased by the U.S Navy between 2005 and 2007, can only enhance the training regimen of U.S. Sailors.

With air-independent propulsion systems, these advanced submarines can remain submerged for significantly longer periods of time, with obvious implications for ASW efforts.

Enabling partner navies with interoperability with U.S. forces remains a critical imperative Team SPAWAR is well positioned to provide.

Through its contributions to DESI and the Global Maritime Partnership, SSC Pacific and Team SPAWAR have helped foster interoperability of U.S. and partner nations in support of a critical training component of U.S surface and subsurface forces against an emerging threat.

Enabling these kinds of exercises not only enhances the capability of U.S naval forces, but fosters the trust and cooperation prescribed in the nation's maritime strategy. CHIPS

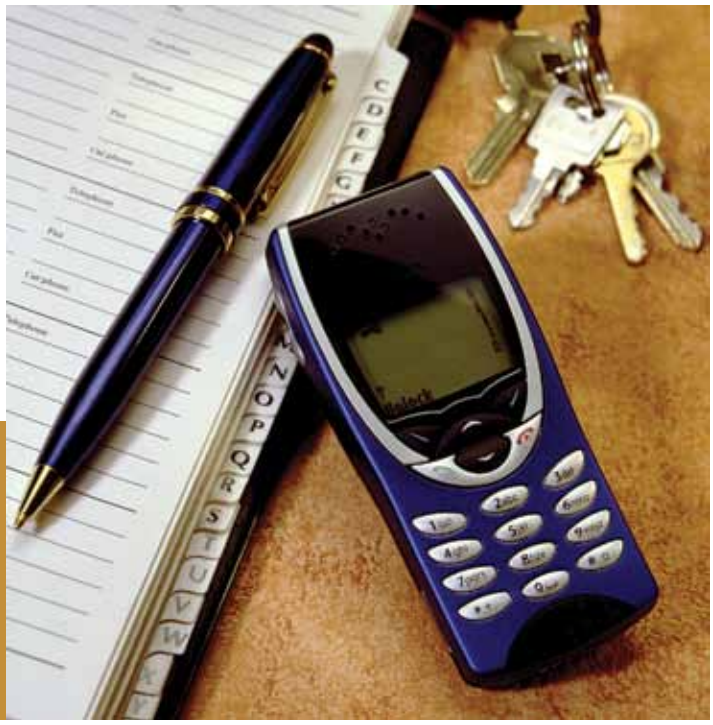
George Galdorisi is the director of the Corporate Strategy Group for SSC Pacific.

José Carreño is the branch head for Strategic and Business Planning at SSC Pacific.

Frank Bantell is the lead coalition communications engineer working for SSC Pacific in the Pacific C4ISR department group in direct support of the U.S. Pacific Fleet communications directorate.

Russell Grall is a senior project engineer who works in the SSC Pacific C4ISR department.

Defending Cell Phones and PDAs Against Attack



By DON CIO Privacy Team

As cell phones and personal digital assistants (PDAs) become more technologically advanced, attackers are finding new ways to target victims. By using text messaging or e-mail, an attacker could lure you to a malicious site or convince you to install malicious code on your portable device.

What unique risks do cell phones and PDAs present?

Most current cell phones have the ability to send and receive text messages. Some cell phones and PDAs also offer the ability to connect to the Internet. Although you may find these features useful and convenient, attackers may try to take advantage of them. As a result, an attacker may be able to trick you into revealing personally identifiable information (PII) or using your service by the following methods.

❑ Abuse your service. Most cell phone plans limit the number of text messages you can send and receive. If an attacker spams you with text messages, you may be charged additional fees. Attackers may also be able to infect your phone or PDA with malicious code that will allow them to use your service. Because the contract is in your name, you will be responsible for the charges.

❑ Lure you to a malicious Web site. PDAs and cell phones that provide access to e-mail are targets for standard phishing attacks; attackers are now sending text messages to cell phones. These messages, supposedly from a legitimate company, may try to convince you to visit a malicious site by claiming that there is a problem with your account or stating that you have been subscribed to a service. Once you visit the site, you may be lured into providing PII or downloading a malicious file.

❑ Use your cell phone or PDA in an attack. Attackers who can gain control of your service may use your cell phone or PDA to attack others. Not only does this hide the real attacker's identity, it allows the attacker to increase the number of targets.

❑ Gain access to private account information. In some areas, cell phones are becoming capable of performing certain transactions from paying for parking or groceries, to conducting larger financial transactions. An attacker who can gain access to a phone that is used for these types of transactions may be able to discover your account information and use or sell it.

What can you do to protect yourself?

❑ Follow general guidelines for protecting portable devices. Take precautions to secure your cell phone and PDA the same way you should secure your computer.

❑ Be careful about posting your personal cell phone number and e-mail address. Attackers often use software that browses Web sites for e-mail addresses. These addresses then become targets for attacks and spam. Cell phone numbers can be collected automatically, too. By limiting the number of people who have access to your information, you limit your risk of becoming a victim.

❑ Do not follow links sent in e-mail or text messages. Be suspicious of URLs sent in unsolicited e-mail or text messages. While the links may appear to be legitimate, they may actually direct you to a malicious Web site.

❑ Be wary of downloadable software. There are many sites that offer games and other software you can download onto your cell phone or PDA. This software could include malicious code. Avoid downloading files from sites that you do not trust. If you are getting the files from a supposedly secure site, look for a Web site certificate. If you do download a file from a Web site, consider saving it to your desktop and manually scanning it for viruses before opening it.

❑ Evaluate your security settings. Make sure that you take advantage of the security features offered on your device. Attackers may take advantage of Bluetooth connections to access or download information on your device. Disable Bluetooth when you are not using it to avoid unauthorized access.

Originally produced by Mindi McDowell, United States Computer Emergency Readiness Team (US-CERT). CHIPS

USS Truman Readies for Operational Testing of Key Data Integration

DCGS-N allows ashore and afloat ISR and IO sharing

By Michael Pobat

Training has intensified for Sailors aboard USS Harry S. Truman (CVN 75) as crew members learn to operate and maintain the Navy's newest intelligence, surveillance, reconnaissance and targeting (ISR&T) system.

USS Truman became the first ship in the fleet to receive the Distributed Common Ground System – Navy (DCGS–N) in January 2009. The accelerated training is in preparation for a series of upcoming test events that will culminate in August 2009 with an operational evaluation (OPEVAL) conducted by Commander Operational Test and Evaluation Force. Upon completion of OPEVAL, USS Truman will deploy overseas as the first operational unit to feature DCGS-N.

The DCGS-N is the fleet variant of the Defense Department's DCGS family of systems that provides integration of ISR&T support capabilities previously accessed from a variety of stand-alone systems. The system allows USS Truman Sailors to produce and share actionable intelligence products that adhere to intelligence community standards within the family of systems and with other DoD customers.

"Our fleet users continually ask for increased interoperability and ease of use with regard to C4I products," said Chris Miller, the Program Executive Officer for Command, Control, Communications, Computers and Intelligence (PEO C4I). "The introduction of DCGS-N to the fleet satisfies both criteria and will significantly improve the Navy's ability to share the actionable intelligence needed to identify and destroy targets."

Initial feedback on the system is extremely positive. Sailors like the improved capability of launching the Generic Area Limitation Environment signals intelligence application; the Integrated Imagery and Intelligence analyst application; the Common Geospatial-Intelligence System; and SHARP Display System (for rapid screening of digital tactical image data from a live datalink) from all DCGS-N workstations.

This multi-mission, multi-workspace flexibility allows users to tailor their tools and situational picture for virtually any mission and any workcenter, saving time and streamlining operations. Sailors are also pleased that DCGS-N operational reliability and stable software allow the system to operate for long periods of time without the need to reboot.

Cmdr. Eric Law, USS Truman's intelligence department head, indicated he was glad to finally see DCGS-N come to fruition.

"It had been a long road with a few bumps, but it is important to get all the intelligence systems bundled and to the fleet in a usable format," he said. "DCGS-N has the ability to transform the way we do intelligence business in the fleet."

Law said DCGS-N is user-friendly and provides a significant improvement in imagery processing and geocoordinate point mensuration. He also gave credit to the installation team.

"System installations can sometimes be difficult and complex. This install was relatively smooth and the team aggressively worked at mitigating any problems," he said.

PEO C4I's Battlespace Awareness and Information Operations Program Office is responsible for managing the program and training the USS Truman's intelligence team to effectively employ DCGS-N in an operational environment.

Training began during an at-sea period in February 2009 and has been augmented by additional training at the SPAWAR Systems Center Atlantic Charleston, S.C., facility.

Intelligence specialists and cryptologic technicians are receiving in-depth instruction in the geospatial intelligence, imagery intelligence, signals intelligence and operational intelligence disciplines required to effectively operate the DCGS-N system.

Additionally, the ship's electronic technicians will receive instruction on hardware and software maintenance to ensure the system is kept up and running.

With DCGS-N, USS Truman has the capability to develop new naval intelligence concepts of operations and access intelligence software applications that were previously found only on stand-alone workstations in specified shipboard workcenters, for example, Multi-Sensor Interpretation, Strike Intelligence Analysis Center, Ship Signal Exploitation Space and Supplementary Plot. These software applications are now conveniently available as icons on all DCGS-N workstations in the ship's intelligence spaces.

DCGS-N was designed to leverage commercial off-the-shelf and mature government off-the-shelf software, tools and standards to provide a scalable, modular and extensible multi-source capability that operates at the general service and Sensitive Compartmented Information security levels.

DCGS-N uses an ashore Enterprise Point of Presence, accessible to all users via a Web interface, to facilitate sharing and receiving information with mission partners in a Web-enabled, network-centric, joint-interoperable enterprise. This improvement also significantly reduces the stress on already limited bandwidth in the DCGS-N afloat configuration.

The DoD DCGS family of systems access and ingest data from spaceborne, airborne, afloat ISR collection assets, intelligence databases and intelligence producers. Data is shared across the joint enterprise using DCGS Integration Backbone and Net-Centric Enterprise Services standards to optimize timeliness, quality and multi-service integration of ISR information. CHIPS

Michael Pobat works in the PEO C4I Battlespace Awareness and Information Operations Program Office. For more information, contact the Space and Naval Warfare Systems Command public affairs office at (619) 524-3432.

Above: May 2, 2009 – The aircraft carrier USS Harry S. Truman (CVN 75) transits the Atlantic Ocean during a Tailored Ships Training Availability and Final Evaluation Phase. U.S. Navy photo by Mass Communication Specialist 3rd Class Justin M. Smelley.

SPAWAR Systems Center Pacific offers guaranteed education, technical training and jobs

Get SMART –Get Ahead – Get Paid

By SSC Pacific Public Affairs

Space and Naval Warfare Systems Center Pacific (SSC Pacific) recently announced a new scholarship program that targets local community college students and provides continued mentorship to prepare students for guaranteed laboratory positions at SSC Pacific as scientists and engineers upon graduation.

"For years, the lab has reached out to local four-year universities to provide a significant percentage of the 100-plus scientist and engineering graduates hired each year. What's new is we are now able to reach students attending local community colleges by offering three-year scholarships, summer internships and assured job placement," said Carmela Keeney, technical director for SSC Pacific.

"Historically, community colleges have not been on our radar since we require BS and BE degrees to even be considered for education programs and employment," Keeney said. "We can now tap into a much larger and diverse population of students who are motivated and demonstrate academic acumen and tenacity."

On April 16, SSC Pacific welcomed Miguel Rodriguez and Jessica Daniels from Southwestern Community College to celebrate the new Science, Mathematics, and Research for Transformation (SMART) Scholarship community college pilot.

Left to right, back row, Shannon Bake, Diana Arceo, Anjum Gupta, Narek Pezeshkian, Deborah Shifflett, Daniel Kichura. Front row, Jessica Daniels, Ayax Ramirez, Miguel Rodriguez and Jim Rohr, outreach coordinator.

SMART is a Defense Department-sponsored civilian scholarship for service program designed to fill critical workforce requirements in the science and engineering disciplines to recruit the technology leaders of the future.

The SMART program offers full tuition, full-time salary, or stipend, while in school, health insurance, textbook allowance and paid summer internships. The program is extremely competitive, with only a few hundred SMART fellows selected annually from thousands of applicants nationwide.

SSC Pacific has been participating in the SMART Scholarship program since 2005 and has already hired five scholars with more than a dozen ready to start when they finish their degrees.

"This is the first time that the SMART program has had a dedicated and organized effort for community college students," said Deborah Shifflett, SMART program manager at the Naval Postgraduate School.

Rodriguez and Daniels are the first two college sophomores to be accepted by SSC Pacific in the new SMART program. Traditionally, SMART fellows are recent college graduates and are hired after completing a four-year degree.

During their visit to SSC Pacific, Rodriguez and Daniels were introduced to their mentors, Ayax Ramirez, a photonics researcher, and Narek Pezeshkian, a robotics researcher. Rodriguez and Daniels also met the five other 2009 SMART fellows currently working at the center.

Rodriguez has an impressive military background, having served three tours in Iraq. An avid student with near-perfect grades, he has a passion for science and technology. Rodriguez is highly motivated and is currently pursuing an Associate of Science degree in physics. He plans to transfer to the University of California, Berkeley, and complete his degree in physics by 2012.

"I really enjoy studying physics, and I look forward to working with Mr. Ramirez," Rodriguez said. "I am excited about the opportunity to contribute to the work currently being done in photonics and lasers."

Daniels, a full-time student, balances a full-time work schedule and still manages to volunteer; she is currently the acting president of Southwestern Community College's Computer Science Club. With a background in business administration, Daniels is seeking to challenge herself and gain experience in computing and programming.

Daniels is pursuing an Associate of Arts degree in computer science and plans to transfer to San Diego State University (SDSU) to complete her Bachelor of Science degree in computer science by 2012.

"I feel so lucky to be selected into the SMART program. I never even thought I would be able to get my bachelor's degree, I feel so fortunate to be given this opportunity," Daniels said. "My goal is to transfer to SDSU, graduate in 2012, and join the SPAWAR team!"

SMART scholarship students are required to sign a service agreement that requires a DoD civilian employment com-

mitment. For each year of academic funding, SMART fellows are required to work for a DoD agency for one year.

After receiving a degree through the SMART program, students are awarded full federal government employee benefits, competitive post-graduation starting salaries, and a unique opportunity to contribute to their country in exciting careers in advanced technology.

SSC Pacific is the nation's only full spectrum C4ISR (command, control, communications, computers, intelligence, surveillance and reconnaissance) laboratory providing research, development, acquisition, test and evaluation and full life-cycle support across systems that integrate the military's sensors, networks, command and control, and weapons into a fully netted combat force with full spectrum dominance. CHIPS

For more information about SSC Pacific, go to the SPAWAR Web site: http://enterprise.spawar.navy.mil/.

For more information about the SMART Scholarship, go to www.asee.org/fellowships/smart/.

DON CIO releases the latest in its podcast series with the Next Generation Enterprise Network podcast

In this podcast, Rear Adm. Bill Goodwin, Assistant Chief of Naval Operations for the Next Generation Enterprise Network (NGEN) System Program Office, sits down with Rob Carey, the Department of the Navy CIO, to discuss NGEN and plans to ensure continuity of services during the transition from the Navy Marine Corps Intranet to NGEN.

With the evolution from NMCI to NGEN, Carey and Goodwin discuss plans to create a first-of-its-kind fully integrated enterprise-wide Naval Networking Environment that will make data and services available to all users from any CAC-enabled computing device.

To listen to and download the podcast, visit: www.doncio.navy.mil/ContentView.aspx?ID=1149. CHIPS

NMCI Links to Other Defense Branches Via JEDS

By NMCI Public Affairs Office

00The Navy Marine Corps Intranet (NMCI) has now reached a new level of interoperability and integration for its users, simply by connecting them with their counterparts across the Department of Defense. A new Enterprise Global Address List (GAL) allows NMCI users to find people in the other branches of the military from their desktops.

In the spring, NMCI rolled out a new GAL that synchronizes NMCI with the Defense Information Systems Agency's (DISA) Joint Enterprise Directory Services. JEDS houses the contact information for personnel in the Army, Air Force, Coast Guard, Marine Corps, Navy Bureau of Medicine and Surgery (BUMED), the Integrated Shipboard Network System (IT-21/ISNS), as well as other Defense agencies.

From Microsoft Outlook, users will be able to search all DoD address books, or narrow their search by selecting a specific agency's address book. Once a contact is found, users will be able to easily add that individual to their contacts.

"The addition of this service reflects a new level of interoperability for NMCI users," said Capt. Scott Weller, program manager for NMCI, which is part of the program portfolio of the Program Executive Office for Enterprise Information Systems (PEO EIS). "This new GAL will allow for greater collaboration between our enterprises and the DoD community, a key component of the DON's Maritime Strategy."

Current DoD directory services do not support interoperability between services, which makes e-mail and contact information in those directories inaccessible to the larger DoD community. Per DoD Directive 8500.1, the services were instructed to become net-centric by integrating all DoD information directory services. NMCI is the first defense IT network to meet the requirements of the DoD directive.

The roll-out of the new GAL will reach all NMCI users by the end of the summer. Users will receive a user alert approximately two days prior to their scheduled installation.

To receive the new GAL, users must be logged onto their computer, but not necessarily Outlook. If users are logged into their Outlook inbox, they will receive a warning requiring them to close Microsoft Outlook. Once closed, Microsoft Outlook will briefly launch and close twice, taking about a minute to complete.

Following implementation, users can go to "Tools: Address Book: Show names from the:" to see the additional directories listed in their Windows Address Book .

The immediate benefit will be greater access to information in all DoD branches. Users will be able to search for contacts, in all DoD address books, or narrow their search by selecting a specific agency's directory. Once a contact is found, users will be able to easily copy that individual to their contacts list. CHIPS

About NMCI

The Navy Marine Corps Intranet (NMCI) is the Department of the Navy's shore-based enterprise network in the United States and Okinawa and is part of the program portfolio of the Program Executive Office for Enterprise Information Systems (PEO EIS). NMCI provides a single, integrated IT environment for reliable, stable information transfer.

Team SPAWAR's Fiber-Optic Technology Helps Nereus Reach Deepest Part of the Ocean

By Media Relations, Woods Hole Oceanographic Institution and SPAWAR Public Affairs

A new type of deep-sea robotic vehicle called Nereus has successfully reached the deepest part of the world's ocean, thanks in part to fiber-optic technology developed by Team SPAWAR's Space and Naval Warfare Systems Center (SSC) Pacific scientists. The dive to 10,902 meters (6.8 miles) occurred May 31, 2009, in the deepest part of the world's oceans, Challenger Deep, in the Mariana Trench in the western Pacific Ocean, according to a team of U.S. engineers and scientists aboard the research vessel Kilo Moana.

The unique hybrid-vehicle design of Nereus makes it ideally suited to explore the ocean's last frontiers. The unmanned vehicle is remotely operated by pilots aboard a surface ship via a lightweight, micro-thin, fiber-optic tether that allows Nereus to dive deep and be highly maneuverable.

The tethering system presented one of the greatest challenges in developing a cost-effective remotely operated vehicle (ROV) capable of reaching these depths. Traditional robotic systems use steel-reinforced cables containing copper wires to power the vehicle and optical fibers to enable information to be passed between the ship and the vehicle. If such a cable were used to reach the seafloor in the Mariana Trench, it would snap under its own weight.

Solving the Challenge

To solve the challenge, the Nereus team adapted fiber-optic technology developed by SSC Pacific to carry real-time video and other data between the Nereus and the surface crew. Similar in diameter to a human hair and with a breaking strength of only 4 kilograms (8.8 pounds), the tether is composed of glass fiber core with a very thin protective jacket of plastic.

Nereus brings approximately 40 kilometers (25 miles) of cable in two canisters the size of large coffee cans that spool out the fiber as needed. By using this very slender tether, instead of a large cable, the team was able to decrease the size, weight, complexity and cost of the vehicle.

To reach the trench, Nereus dove nearly twice as deep as research submarines are capable of and had to withstand pressures 1,000 times of that at Earth's surface — crushing forces similar to those on the surface of Venus. Only two other vehicles have succeeded in reaching the trench: the U.S. Navy-built bathyscaphe Trieste, which carried Jacques Piccard and Don Walsh there in 1960, and the Japanese-built robot Kaiko, which made three unmanned expeditions to the trench between 1995 and 1998.

Neither of these is presently available to the scientific community. Trieste was retired in 1966, and Kaiko was lost at sea in 2003.

Unique Design

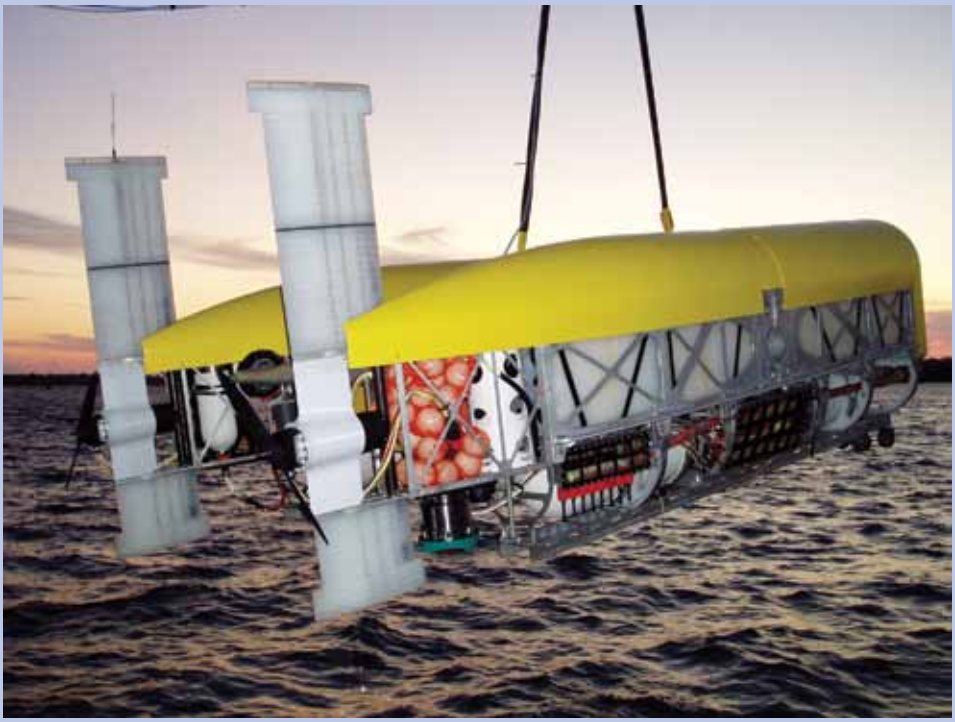
The Nereus engineering team knew that to reach these depths, a tethered robot using traditional technologies would be prohibitively expensive to build and operate. So they used unique technologies and innovative methods to strike a balance between size, weight, materials cost and functionality. Building on previous experience in developing tethered robots and autonomous underwater vehicles (AUVs), the team fused the two approaches together to develop a hybrid vehicle that could fly like an aircraft to survey and map broad areas and then be converted at sea into a tethered ROV that can hover like a helicopter near the seafloor to conduct experiments or to collect biological or rock samples under real-time human control.

The present trials of Nereus are being conducted in this tethered ROV mode of operation. Nereus can also be switched into a free-swimming, autonomous vehicle.

Reaching the bottom

On its dive to the Challenger Deep, Nereus spent more than 10 hours on

HROV/Nereus testing off Kilo Moana. Photo by Matthew Heinzt, Woods Hole Oceanographic Institution.



Closeup of HROV/Nereus out of the water. Photo by Christopher Griner, Woods Hole Oceanographic Institution.

Top, WHOI biologist Tim Shank (at right) and Patty Fryer (left), a geologist with the University of Hawaii, examine the samples retrieved from the Mariana Trench by the vehicle. WHOI summer student fellow Eleanor Bors examines a sea cucumber collected during Nereus's first dive to the Mariana Trench. Photos by Barbara Fletcher, SPAWAR Systems Center Pacific.

The Nereus team adapted fiber-optic technology developed by SSC Pacific to carry real-time video and other data between the Nereus and the surface crew

the bottom, sending live video back to the ship through its fiber-optic tether and collecting geological and biological samples with its manipulator arm. It also placed a marker on the seafloor signed by those aboard the surface ship.

"We couldn't be prouder of the stunning accomplishments of this dedicated and talented team," said Susan Avery, president and director of Woods Hole Oceanographic Institution.

"With this engineering trial successfully behind us, we're eager for Nereus to become widely used to explore the most inaccessible reaches of the ocean. With no part of the deep seafloor beyond our reach, it's exciting to think of the discoveries that await."

The dive makes Nereus the world's deepest-diving vehicle and the first vehicle to explore the Mariana Trench since 1998. CHIPS

A specialized manipulator arm of the newly built hybrid remotely operated vehicle (HROV)/Nereus samples sediment from the deepest part of the world's ocean, the Mariana Trench. Photo by Woods Hole Oceanographic Institution.

For more information, go to the SPAWAR Web site: http://enterprise.spawar.navy.mil/.

Woods Hole Oceanographic Institution is a private, independent organization in Falmouth, Mass., dedicated to marine research, engineering and higher education. Established in 1930 on a recommendation from the National Academy of Sciences, its primary mission is to understand the oceans and their interaction with the Earth as a whole, and to communicate a basic understanding of the oceans' role in the changing global environment.

Hold Your Breaches!

By Steve Muck

The following is a recently reported compromise of personally identifiable information (PII) involving the improper disposal of human resources documents. 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 DON CIO Privacy Office.

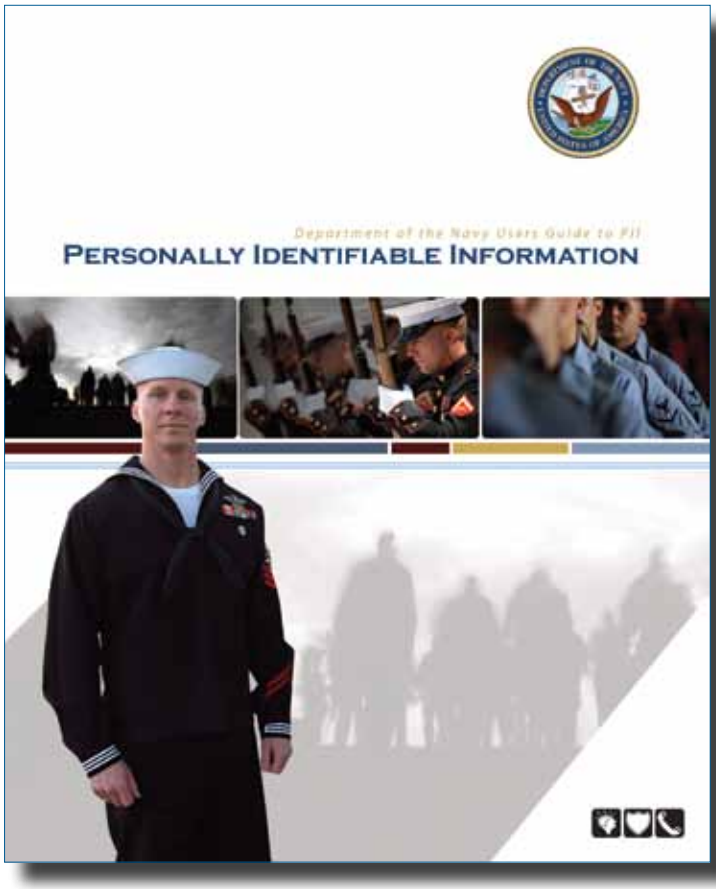
The Incident

Some time between late February 2009 and mid-March 2009, three boxes were discovered in a recently vacated office. The office had been completely stripped of all furniture, supplies and equipment in preparation for another office code to move in. The empty office was unlocked and probably remained so until the movers arrived with the new office equipment. The boxes contained more than 240 employee records, with Social Security numbers, home addresses and other personal information dating back to the early 1980s. All personnel in the building were questioned, but no one claimed to have any knowledge of how the boxes appeared in the empty office.

This incident is a privacy official's worst nightmare: *Old records containing high-risk PII in an unlocked office that no one could account for.* Like most PII breaches, this one could have easily been prevented.

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

Steve Muck is the DON CIO privacy team lead.



A new PII brochure is available with protective measures you can take to help you understand PII and its hazards.

Lessons Learned

- ❑ Office moves are common and present unique challenges when moving paper and electronic records. The command privacy official should ensure that all personnel involved in an office move take extra precautions when packing, shipping and relocating records that contain PII.
- ❑ Develop a moving plan and ensure PII safeguard considerations are factored in.
- ❑ Human resources, law enforcement, medical, administrative, legal and financial offices are especially vulnerable to this type of PII compromise/loss due to the personal records that these offices maintain.
- ❑ All vacated offices should be locked.
- ❑ Remember that PII has a very long shelf life and can be used fraudulently even after a person is deceased. Commands should develop and implement a document destruction policy following guidelines issued in the DON Records Management Manual (SECNAV M-5210.1) available from the DON CIO Web site, www.doncio.navy.mil, under the Policy and Guidance tab.
- ❑ Most documents can be destroyed after five years.

THE FEDERAL TRADE COMMISSION ESTIMATES THAT AS MANY AS 9 MILLION AMERICANS HAVE THEIR IDENTITY STOLEN EACH YEAR

COBRA: ONE STEP CLOSER TO EXPEDITIONARY WARFARE USERS

Mine detection system passes critical Milestone "C" Decision for low-rate initial production

By Jacqui Barker

Sailors and Marines are one step closer to receiving a new mine detection system called Coastal Battlefield Reconnaissance and Analysis. COBRA received Milestone C decision approval within the Department of Defense (DoD) acquisition process on March 31. Milestone C signifies that the design is mature enough to enter the production phase of development.

According to assistant program manager for assault breaching systems (ABS), Lt. Col. Tim McLaughlin, this is a significant step toward delivering viable 21st century mine detection capabilities to Littoral Combat Ships (LCS).

COBRA was designed to support U.S. Marine Corps amphibious assault breaching operations. The Program Executive Office for Littoral and Mine Warfare, Mine Warfare Program Office, part of Naval Sea Systems Command, is responsible for ABS. "This is a great capability … an important first step in delivering this system of systems," McLaughlin said.

ABS, as an integrated system of systems, provides Department of the Navy forces with a method to access beachheads via littoral areas without being operationally impeded. COBRA is the intelligence, surveillance and reconnaissance technology component of the ABS, making it one piece in a system of systems. COBRA detects and precisely locates minefields and obstacles. Other systems within ABS are then used to guide service members and their equipment safely ashore.

Naval Surface Warfare Center Panama City Division (NSWC PCD), a field activity of NAVSEA, serves as the technical design agent for the COBRA system. NSWC PCD and its industry partners developed COBRA Block I to determine the presence or absence of minefields and obstacles on the beach and further inland.

COBRA is designed to be used as a modular capability as part of the mine countermeasures mission package on the LCS. The COBRA airborne payload will be flown as one of the missions assigned to the MQ-8B Fire Scout vertical takeoff and landing tactical unmanned aerial vehicle (VTUAV). Fire Scout provides unprecedented situational awareness and precision targeting support for U.S. forces.

"This system is paving the way for integrated and interoperable mine identification and neutralization efforts," said NSWC PCD ABS branch head Dave Bucher. "More than simply overseeing design and development, performance in-service is our goal and responsibility.

"I'm a former mining and in-service engineering agent. It may sound cavalier, but I've had the opinion that mines could easily defeat countermine forces. COBRA has convinced me otherwise because it works, and it works well," Bucher said. "It identifies patterns and other characteristics from the air, processes them through sophisticated software and presents the results to a Sailor or Marine for a gut-check by an experienced interpreter and planner. It's been exciting for me to see."

The capability demonstration was so impressive that the sponsor wants to have production systems ready for the fleet right away. The next steps for COBRA Block I are to determine the best way to provide the units to the fleet and to put a Block I production contract in place for additional units. CHIPS

Jacqui Barker is the NSWC PCD public affairs officer.

The Coastal Battlefield Reconnaissance and Analysis system's gimbal, the visible part of the airborne component of the COBRA system. Other system components include a post-mission analysis station and the ground control station for the vertical takeoff and landing tactical unmanned aerial vehicle. U.S. Navy photo. For more information about Naval Surface Warfare Center Panama City Division, visit http://nswcpc.navsea.navy.mil/.

By Christy Crimmins

Use of Web 2.0 Tools for DON IM/IT Policy Development

Over the past few years, the use of Web 2.0 tools has increased in the Department of the Navy. Many of these tools present both opportunities and challenges. This column will focus on educating readers about the myriad tools available for use within the DON, Department of Defense, and federal government, as well as the challenges they present. Topics will range from new applications to safe use and cultural changes that occur as a result of Web 2.0 collaboration. In the interactive spirit of Web 2.0, your comments and suggestions are encouraged.

The office of the DON Chief Information Officer (DON CIO) has begun to pilot the use of Intelink, home to Intellipedia, "the U.S. Government's unclassified wiki," developed by the Intelligence Community Enterprise Services (ICES) within the Office of the Director of National Intelligence.

The DON CIO is using Intelink to develop and refine existing policy. 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 and instant messenger — in all classification domains — and a Web-based document management system called Intelink Inteldocs. An outline of these services, as well as information on ICES, can be found on Intellipedia at https://www.intelink.gov/wiki/ICES_Services.

On April 29, 2009, Secretary of the Navy Instruction (SECNAVINST) 5000.36A, the department's policy on information technology applications and data management, was posted to Intellipedia for community comments and editing. The policy will remain open for editing for approximately three months. In the near future, the DON CIO plans to post additional DON information management/information technology (IM/IT) policies for community editing.

"A challenge faced by the DON is to develop and promulgate effective IM/IT policy," said DON CIO Chief Technology Officer Michael Jacobs. "Effective policy does more than simply identify the 'rules' that must be followed; it guides the department toward achieving its critical goals and strategic objectives."

The DON CIO hopes that by opening policies for community editing, members of the department will be encouraged to review, provide input and make changes during the policy development phase.

"We hope to foster a collaborative environment where everyone has the opportunity to comment while the posted policies are taking shape, not just as a final step before they get signed," Jacobs said.

In addition to providing a space for collaboration on existing policy, the page also includes space for the identification of policy gaps. Like the policies posted to the site, this page is open to anyone in the department with suggestions for future DON IM/IT policy development.

To access DON IM/IT policies open for community comments and editing, as well as the space dedicated to identification of IM/IT policy gaps, please visit: https://www.intelink.gov/wiki/DON_information_management_and_information_technology_policy.

Users will need to register for a user name and password to access the site.

The development of DON policy is a For Official Use Only (FOUO) activity. Access to Intellipedia is limited to government employees; active duty and ready reserve members of the U.S. military; active members of the U.S. National Guard; contractors or other individuals sponsored by a U.S. government agency; state, local or tribal government employees; Foreign Nationals sponsored by a U.S. government agency; and members of the U.S. academic community sponsored by a U.S. government agency.

Intellipedia has more than 23,000 registered users and 126,000 pages. There are 1,100 unclassified blogs with more than 8,900 posts. Users who register for accounts are able to create their own blogs and post comments to many others.

Jacobs has started a blog (https://www.intelink.gov/blogs/michael.b.jacobs/) to discuss emerging IT issues relevant to the DON, as well as their use, implementation and adoption. CHIPS

Christy Crimmins provides communications support to the Department of the Navy Chief Information Officer.

Today's Plan for Tomorrow's Cybersecurity Workforce

Using Metrics to Ensure Compliance

By Mary Purdy

A primary challenge for the Department of the Navy Chief Information Officer (DON CIO) is planning and preparing for future workforce roles and training. As stealthy assaults on DON systems and networks multiply, much is expected of the cybersecurity workforce (aka Information Assurance and Computer Network Defense Service Provider (CND SP)).

Therefore, it is essential that IA professionals be equipped with the skills they need to be successful. From the IA systems architect, to the system administrator, to the computer network defense analyst and incident responder, the team must work together across cyberspace in the development, operation, defense and security of information systems.

The teams must be given time to prepare and do their work with the tools to accomplish the mission, the training to enhance their skills, and the technical information to do well in their jobs.

To standardize and improve cybersecurity workforce skills, the Defense Department directed the services to implement DoD 8570.01-M, "Information Assurance Workforce Improvement Program (IA WIP)." The program requires the DON to identify IA positions, identify the IA workforce (IAWF) and ensure members are appropriately trained and commercially certified to fulfill their job functions.

In addition to the DoD IAWF improvement mandate, service IAWF commercial certification status must be reported to Congress each year in compliance with the Federal Information Security Management Act (FISMA).

Recently deceased DON Senior Information Assurance Officer, Mr. John Lussier, chartered the IAWF Management Oversight and Compliance Council (IAWF MOCC) to ensure compliance with DoD 8570.01-M and FISMA. Led by an executive board, all Echelon I and II and major subordinate command IAWF managers and stakeholders are invited to participate as we work collaboratively to bring IA, CND SP and Information Assurance System Architecture and Engineering (IASAE) certification and training requirements into compliance. In its oversight role the MOCC membership will:

✓ Sustain discipline in IAWF management implementation plans, processes and procedures;

✓ Review Budget Submitting Office manpower requirements to ensure the enterprise is resourced to effectively deliver the cybersecurity mission;

✓ Oversee the health of the IAWF and support improved hiring practices that allow the services to hire the best personnel;

✓ Develop career path recommendations to include enhanced training and rotational plans for developing leaders in cybersecurity; and

✓ Ensure FISMA compliance.

Services are required to meet certain implementation milestones over the next two years with full sustainment by 2011. Access to accurate IAWF electronic data is critical to ensuring the workforce is appropriately trained, mentored and commercially certified. User friendly workforce management tools will not only free personnel from annual hand counts, but also validate command self-reported implementation status.

To accomplish stringent oversight and compliance capability, the MOCC uses metrics tools such as compliance checklists, IAWF management assist visits, audits, inspections, red and blue team visits, the Defense Readiness Reporting System (DRRS) and a total workforce management dashboard.

The workforce management system pulls data from authoritative sources and displays military, civilian and contractor information in one view. These management tools allow leadership to clearly view IAWF status and enable better analysis for future workforce needs.

As George Bieber, from the Defense-wide Information Assurance Program (DIAP) office recently stated, "I applaud the DON for standing up the MOCC. Its oversight capability and compliance authority is a major step that will ensure its IAWF, as a whole, can achieve the cybersecurity mission, and that each individual has the opportunity to achieve his or her personal growth leading to a successful IT career. This is especially important because once the IAWF improvement program is fully implemented, personnel will require certification if they are to continue doing their job, and this applies equally to uniformed personnel, government civilians and contractors."

The DON's vision of a highly skilled cybersecurity workforce is attainable. Through command visits and electronic data transparency, the IAWF MOCC will have a clear understanding of the IA workforce skill level and will be able to shape workforce modernization.

The MOCC governing board will initiate an ongoing conversation with Navy and Marine Corps command information officers and IA managers about the commercial certification status of their individual IAWF members. This two-way communication will be very important as we all work to ensure Information Assurance Workforce Improvement Program compliance. CHIPS

Mary Purdy supports the DON CIO as the IAWF MOCC facilitator.

For more information, go to the DON CIO Web site: www.doncio.navy.mil.

Joint and coalition warfighters test new and emerging technological solutions for combatant commanders at CWID 2009

By John J. Joyce

More than 430 visitors observed U.S. and coalition warfighters judge new and emerging technologies in simulated military missions and national emergency scenarios during Coalition Warrior Interoperability Demonstration (CWID) 2009 at the Naval Surface Warfare Center (NSWC) Dahlgren Division conducted from June 15-25.

"The visitors toured CWID's Dahlgren site to watch 114 warfighters — including 36 foreign military members — evaluate 31 interoperability trials, such as mapping programs and tracking systems," said NSWC Dahlgren Division Commander Capt. Sheila Patterson. "Warfighter appraisals determine whether or not a trial truly improves interoperability and is ready for deployment to our joint and coalition forces."

This is the 10th year NSWC Dahlgren hosted U.S. forces and coalition partners to evaluate new solutions. Warfighters from New Zealand to Norway tested 42 trials — cutting-edge information technologies — designed to fill capability gaps and requirements defined by combatant commanders.

"Interoperability trials continue to develop complex solutions to meet the technology needs of warfighters on the frontlines," said NSWC Dahlgren Division CWID Site Manager Dennis Warne. "This year, CWID's complexity featured multiple domain networks running simultaneously, multiple warfighting scenarios, and several ITs attempting far reaching technologies."

The demonstration took place out of five network locations across the United States and with more than 20 coalition partners around the world.

The Chairman of the Joint Chiefs of Staff annual event enables U.S. combatant commands, the services, agencies and international partners to investigate technologies that enhance interoperability and C4ISR (command, control, communications, computers, intelligence, surveillance and reconnaissance) capability.

"Our operating environments are complex," said Marine Corps CWID lead Col. Jim Bacchus. "For example, in Afghanistan multiple nations and nongovernmental organizations are providing reconstruction, stability and security. Connecting and sending data effectively among partners is challenging, especially in the rapidly changing world of information technology."

The forum is the only Defense Department hosted event that brings together new and emerging information technologies into a global network environment with interagency and multinational partners.

"CWID is all about identifying and fixing interoperability issues before you find them on the battlefield," Bacchus said.

The warfighters' assessment of technologies includes how well the interoperability trials performed, ease of use, compatibility and interoperability among existing systems and other test technologies.

Interoperability trial technologies receive one or more of three assessment types during execution. Assessment types are: warfighter/operator utility and technical performance; interoperability/technical ability to exchange usable data; and information assurance — the capability to identify threats and enforce policies.

U.S. Joint Forces Command (USJFCOM), in its role as the leader of joint capability development, coordinates assessment results to determine which CWID trials meet defined requirements and have the potential to fill identified capability gaps. Assessments will be compiled in a final report published later in 2009.

Although U.S. CWID is not an acquisition venue, the assessments support the acquisition process and support system life-cycle milestone decisions to efficiently invest in needed capabilities and save services, agencies and stakeholders precious resources.

Some developers choose to demonstrate limited versions of their capabilities just for the broad exposure CWID provides — these technologies are not formally assessed.

CWID brought hundreds of technology representatives together with military and government experts from around the world.

The process begins each year with a Federal Business Opportunity (FBO) publication in April (www.fedbizopps.gov) and ends 14 months later at the conclusion of the operational-scenario-driven demonstration every June.

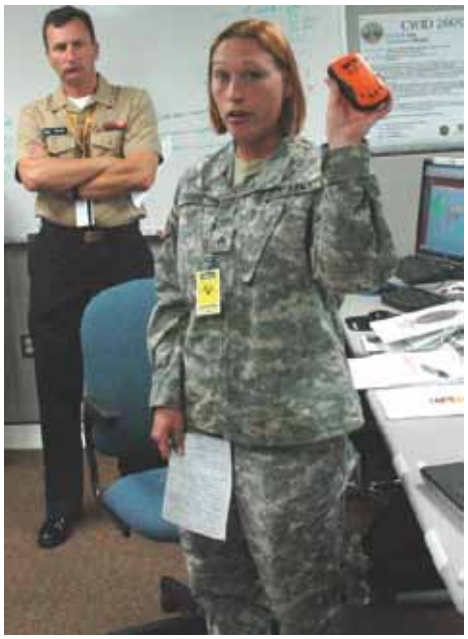
CWID provides focus on promising solutions to specific warfighter and responder requirements through a final report to DoD, government agencies and first responders published by October every year. This report will be made available on the CWID Web site (www.cwid.js.mil).

CWID 2010 is already underway with the FBO announcement now available. You can also access the FedBizOps link on the CWID Web site.

NSWC Dahlgren will serve as the primary site for the U.S. Marine Corps and U.S. Army, along with supporting forces from the National Guard Bureau, U.S. Navy and U.S. Coast Guard in 2010. CHIPS

www.cwid.js.mil

John J. Joyce is with NSWC Dahlgren Division Corporate Communications.



DAHLGREN, Va. (June 24, 2009) -- An Army specialist at the Coalition Warrior Interoperability Demonstration (CWID) demonstrates a location device that can attach to a belt and interface with Google Earth on a standard PC or Mac computer so a warfighter's exact location can be tracked. U.S. Navy photo by Doug Davant.

TW09/OLC2: Sea Trial Experimentation of Critical Maritime Technologies

By Holly Quick

Speeding cyberspace technology to the warfighter is the theme of Trident Warrior 09, the Navy's major annual FORCEnet Sea Trial experiment. TW09, sponsored by Commander, Second Fleet and directed by Naval Network Warfare Command (NNWC), consisted of experimentation and analysis of more than 90 FORCEnet technologies with participation from five countries including Australia, Canada, New Zealand, the United Kingdom and the United States.

Execution took place June 15 – July 3 off the Virginia Coast with 60 U.S. ships and 19 coalition ships. With more than 1,600 events executed in just 23 days, each ship received a detailed hour-by-hour schedule to keep events on track.

Capt. Carl Conti, director of innovation and experimentation for NNWC, explained that Trident Warrior serves to, "accelerate technologies and get them to the warfighter — technologies that will save money, save time, and save lives."

Conti observed the Autonomous Maritime Navigation unmanned surface vessel (USV) demonstration, from the deck of the USS Nassau (LHA 4) which was docked at Norfolk Naval Base. The USV, from the Naval Sea Systems Command Combatant Craft Division, and Nassau, participated in a force protection trial consisting of a boat posing as a rogue vessel attempting to harass the Nassau. The USV was able to detect, track, report and intercept the boat, using high-tech software similar to the software used by the Mars Rover.

"The USV has a digital monitor in charge of its brain, so it knows where the channels are, it knows where the markers are, it knows where the buoys are, and because there are objects out here moving around, it has obstacle avoidance on it," said Rick Simon, director of Spatial Integrated Systems Inc., who conducted the demonstration.

"The USV has a number of sensors, lasers, and radars and electro-optical sensors to give it perception, eyes and ears, to allow it to make decisions based on that perception, and based on the behaviors we teach it, allow it to do the mission," Conti said.

For the exercise the USV was in autonomous mode; however, there was an operator aboard for safety reasons and a technician to collect data. "[The USV] thinks on its own, it makes corrections on its own, and it knows where all the hazards to navigation are," said Trident Warrior director, Cmdr. David Varnes. Varnes said the USV publishes its data to the Maritime Domain Awareness (MDA) data sharing (DS) community of interest (COI).

Kevin Kurtz, TW focus area lead for MDA, explained that the MDA DS COI is interested in sharing maritime data, specifically vessel positional data, in an unclassified but secure environment. He demonstrated how the MDA DS COI and the USV technologies work together.

"Just like using Google maps, you can zoom in and zoom out; you click on different vessels for extended data. It tells the course, speed, latitude, longitude and call sign for the vessel," Kurtz said.

The data source is the Nationwide Automatic Identification System which is a combination of Navy and Coast Guard data. The USV sends photos of the rogue vessel to the MDA DS COI common operational picture, as well as standard contact reports.

Norfolk, Va. - The Autonomous Maritime Navigation USV intercepts a rogue vessel during a TW09 Sea Trial experiment.

Operational Level Command and Control (OLC2) is a 2nd Fleet-hosted experiment running concurrently with Trident Warrior 09. The OLC2 series of experiments is supported by the Navy Warfare Development Command. The primary goal of OLC2 is to improve maritime security between U.S. and multinational partners. OLC2 leveraged the capabilities of a global maritime partnership, along with emerging tools, processes and procedures. OLC2 experimentation took place June 22 – July 2 at the newly dedicated Mitscher Center located on Norfolk Naval Base.

The four components of the OLC2 included Maritime Situational Awareness (MSA), Information Operations (IO), MOC-to-MOC and Coalition, and Seabasing. The experiments of TW09/OLC2 were designed to examine technologies and refine, develop, test and explore capabilities to close gaps in the MOC-to-MOC core operational level of development.

"[The experiment] is trying to use technology to facilitate collaboration, communication," said Second Fleet MOC director, Capt. Richard Henderson. "Another part of this experiment that we are running, OLC2 09, is to test the equipment, the networks, the systems, and evaluate, as part of the experiment, how well the equipment and systems are working."

Dr. Tom Forbes, Second Fleet science advisor, emphasized the importance of coalition collaboration across domains, from one classification system to another. OLC2 features a global network of maritime headquarters among U.S. and national partners, including Second and Fourth Fleets, as well as the U.S. Coast Guard. There is also multinational participation from Canada, the United Kingdom, the NATO MOC in the U.K. and Portugal.

"The Cross Domain Collaborative Information Environment allows us to virtually tie two networks together in different domains. The interesting feature is that it has a language translation tool built into it so the Portuguese can collaborate in a chat room in Portuguese, and we will see it here in English, and vice versa," Forbes said.

The TW09/OLC2 Main Experiment proved to be a great success. Forbes said he was pleased with the brisk pace of its execution.

"This experiment has gone more smoothly than any experiment I have been involved in before. It has just been stable. It's been available." CHIPS

Holly Quick is an operations research analyst working for SSC Atlantic and a contributor to CHIPS.

ONR Partners with Car Industry to Test Energy-Efficient Vehicles

By the Office of Naval Research Corporate Strategic Communications

The Office of Naval Research teamed with an automobile industry leader to explore energy-efficient, environmentally-friendly viable transportation alternatives; the cutting-edge General Motors Chevrolet Equinox fuel cell vehicle (FCV) is the result of the partnership.

As the global automobile industry considers alternative energy sources to replace the traditional internal combustion engine, Jessie Pacheco, a mail clerk at Camp Pendleton, makes his rounds in a FCV. ONR has sponsored GM FCVs at Camp Pendleton since 2006, with two more scheduled to arrive later this year.

"These vehicles are the future," Pacheco said. "It's great to see people drive by me, giving me the thumb's up, and asking, 'Where can I get one?'"

"Fuel cell vehicle research is clearly a case where the Navy and Marine Corps needs are propelling advanced technology that also has potential benefit to the public," said Rear Adm. Nevin Carr, chief of naval research.

Within the Navy-Marine Corps team, ONR has researched power and energy technology for decades. Often the improvements to power generation and fuel efficiency for ships, aircraft, vehicles and installations have direct application for public benefit as well.

"There is not a drop of oil in it," explained Shad Balch, a GM representative at Camp Pendleton. "The electric motor provides maximum instant torque right from the get-go."

The efficiency of a hydrogen-powered fuel cell may prove to be twice that of an internal combustion engine, if not greater, Balch added.

From an operational perspective, the fuel cell vehicle is quiet yet powerful, emits only water vapor, uses fewer moving parts compared to a combustion engine and offers an alternative to the logistics chain associated with current military vehicles.

The addition of fuel cell vehicles to Camp Pendleton provides a glimpse into the future of advanced transportation technology which reduces reliance on petroleum products and affords environmental stewardship benefits, such as reduced air pollution and a smaller carbon footprint, for Navy and Marine Corps bases.

"Partnering with the military gives us critical feedback from a truly unique application. This will help us as we engineer our next generation of fuel cell vehicles," Balch said.

Technology underwrites solutions for both national and naval energy needs. As an ONR program officer in the 1990s, Richard Carlin, Ph.D., recognized the potential of alternative fuel research to help meet the energy challenges of the future. Today, as ONR's director of power and energy research, Carlin is pleased to see the positive reaction to the fuel cell vehicle research program.

"This is an example of where the value of investment in science and technology can really pay off," Carlin said. "Besides the potential energy savings and increased power potential of fuel cell technology, the research and testing we are doing will address challenges like hydrogen production and delivery, durability and reliability, on-board hydrogen storage and overall cost."

For example, through its testing, ONR has made advances in storage capacity necessary for achieving greater range in fuel cell automobiles.

Dave Shifler, the program manager for alternative fuels initiatives at ONR, emphasized that partnerships are essential when bringing a new technology forward.

"With the right partnerships, you can accomplish almost anything," Shifler said. "We have teamed with the Army from the beginning on this research, sharing technical support, contracting support and usage of the GM fuel cell vehicle."

ONR fuel cell research has not been limited to vehicles; it spans the operational spectrum, from ground vehicles to unmanned aerial vehicles (UAVs), to man-portable power for Marines and afloat units. Hydrogen-powered fuel cell technology is one of many programs at ONR in the power and energy research field that is helping the Navy meet the energy needs of the warfighter — and the public.

ONR's partnerships in fuel cell vehicle research include: Headquarters Marine Corps; the Marine Corps Garrison Mobile Equipment office; Southwest Region Force Transportation; Naval Facilities Engineering Service Center, Port Hueneme; Department of Energy (Energy Efficiency and Renewable Energy); South Coast Air Quality Management District; California Air Resources Board; California Fuel Cell Partnership; Defense Energy Support Center, General Motors; Naval Surface Warfare Center, Carderock Division; U.S. Fuel Cell Council; U.S. Army Tank Automotive Research, Development and Engnieering Command/National Automotive Center (TARDEC/NAC), and Deputy Assistant Secretary of the Navy (Environment).

Through its affiliates, ONR is a leader in S&T with engagement in 50 states, 70 countries, 1,035 institutions of higher learning and 914 industry partners. ONR employs approximately 1,400 people, comprised of uniformed, civilian and contract personnel. CHIPS

For more information, contact the ONR public affairs office at onrpao@onr.navy.mil or (703) 696-5031.

INDIVIDUAL AUGMENTEE SAILORS PREPARE FOR AFGHANISTAN MISSION

Since 9/11, more than 73,000 Sailors have served on IA tours in support of "enduring conflicts."

By Army Staff Sgt. Raheem Lay

Reserve and active-duty Sailors from all over the country form a united front in support of Operation Enduring Freedom. This year, Sailors from Navy Group 2 will conduct a detainee operations mission in Afghanistan. Knowing how critical this mission will be, the 177th Armored Brigade is dedicated to ensuring that these Sailors have the necessary tools and guidance to make their mission a success.

"We have been training nonstop here at Camp Shelby," said Senior Chief Petty Officer Mike Luong. "Although we have a week to go before entering the detainee operations training facility, the field training exercises have kept our motivation and confidence level high. Our Soldiers are dedicated to the training and to the mission we stand to face in theater."

The Sailors are being trained on the most recent detainee operational procedures and warfighting tactics executed in theater. Veteran Soldiers, who have just returned from battle, act as controllers/trainers working with Sailors on the Operation Warrior Trainer (OWT) under the 177th Armored Brigade at Camp Shelby Joint Forces Training Center.

Lt. Cmdr. Brett Tittle said he appreciates the input from the trainers who have recently deployed to theater. "It gives us more confidence with the preparation we have received thus far. Knowing that we are being educated with the most recent intel raises our levels of understanding and awareness of our mission in combat."

So far, the Sailors have undergone an extensive amount of training in basic military precision and warfighting. Training, in urban operations, mounted combat patrol and countering improvised explosive devices (IED), has already begun to shape the minds and attitudes of the Sailors in preparation for combat.

After field training, Navy Group 2 will move into detainee simulated facility training. While there, the Sailors will be directed on proper procedures for a detention facility. The Sailors will be evaluated on proper execution to different scenarios that may occur while in country.

Tittle said his Sailors are taking full advantage of their training. While 95 percent of the Sailors are volunteers and many have never been in ground combat before, he said the Sailors' level of concentration and preparation has been "off the charts."

"They understand that they have a critical mission overseas," Tittle said. "Each of them has made significant contributions towards helping one another in developing a team effort environment."

With almost five years since its establishment, the 177th Armored Brigade has successfully trained nearly 75,000 National Guard and Reserve troops for combat. Its willingness to adapt to changes, which have occurred since the beginning of the war, has made Camp Shelby Joint Forces Training Center one of the most prolific mobilization training sites in the country.

"We are amazed with the training and preparation regimen of the 177th Armored Brigade staff," Luong said. "Every day sets a new challenge for all of us. We continue to learn about our mission and most importantly ourselves. I am certain that the training groundwork we discover here at Camp Shelby will carry us through to our mission in theater." CHIPS

Staff Sgt. Raheem Lay is with the 177th Armored Brigade public affairs office located at Camp Shelby in Hattiesburg, Miss.

Sailors from Navy Group 2 are training for deployment as individual augmentees to Operation Enduring Freedom. They will be conducting detainee operations in Afghanistan later on this year. U.S. Army photos by Staff Sgt. Raheem Lay/177th Armored Brigade.

SSC Pacific Guam facility at the forefront of strategic military buildup efforts

The relocation of 14,000 military personnel to Guam requires massive improvements to C4ISR capabilities

By Tom LaPuzza

There is an old saying about how to assess the value of real estate: "Location, Location, Location," and this adage works well to describe the value of the partnership between the island of Guam and the Space and Naval Warfare Systems Center (SSC) Pacific facility located there.

The island is small, about 208 square miles with approximately 171,000 inhabitants (compared to 600 square miles and 875,000 inhabitants on the Hawaiian island of Oahu).

The SSC Pacific facility is similarly small, with a workforce of about 40 compared to the center's total workforce of around 4,000, with most working in San Diego, Calif. Nevertheless, over the next six to eight years, both the island of Guam and the center's far western Pacific facility are poised to make a big impact on a major shift of Defense Department resources.

"Guam is the westernmost sovereign U.S. territory," said SSC Pacific engineer Adrian Gogue. "As such, it represents a unique resource for staging U.S. military forces; no foreign ally, experiencing a change of heart, can take away air fields, or ports, or links in the supply chain required to project American presence to the Far East and the Middle East."

The joint decision by the United States and Japan in October 2005 to move 8,000 U.S. Marines from Okinawa and relocate them to Guam, about 1,800 miles to the southeast, placed the tiny island in the spotlight.

Guam is an integral part of DoD's logistical support system and serves as an important forward operational hub for a mix of military mission requirements, according to an April 2009 report by the Government Accountability Office (GAO), which reported to the Congress on the island's military buildup and its potential challenges.

According to DoD, "Guam provides strategic flexibility, freedom of action, and prompt global action for the global war on terrorism, peace and wartime engagement and crisis response."

Guam also provides solid ground on which to build, which is DoD's plan for the island between now and about 2014. During that timeframe, plans are being developed to establish a $13 billion infrastructure needed to support thousands of U.S. service personnel who will be living on the island.

It is a daunting plan based on figures provided by Adrian Gogue.

"In addition to the 8,000 personnel of the III Marine Expeditionary Force, there will be 2,000 more Marines assigned to transient units on the island," Gogue said. "The Navy will bring in high speed vessels, littoral combat ships and 1,650 more personnel. New carrier berthing will be added to the naval base in Apra Harbor."

The Air Force will transfer one or two Global Hawk unmanned aerial vehicle squadrons and more than 2,500 personnel. The Army will bring in 630 personnel to staff an air defense battery.

The nearly 14,000 military members moving to the island will be accompanied by more than 11,000 family members, according to Gogue, who agreed with the GAO's conclusion that the massive influx of personnel and family members offered some substantial challenges.

For example, GAO cited lack of local construction capacity and commercial development required to build offices, training facilities and residential units. Highways and roads for transporting supplies and for travel to work, schools, shopping and recreation are inadequate with the anticipated population growth. Utilities — the electric grid, water and solid-waste facilities — may not be able to handle the expected 25 percent increase in demand.

But the Department of the Interior's Interagency Group on Insular Areas and DoD's Joint Guam Program Office, and a Navy field office, directed to facilitate, manage and execute requirements associated with rebasing Marine Corps assets from Okinawa to Guam, are working aggressively to address the potential resource shortfall.

Public infrastructure is not the only requirement for the Guam buildup. The move of thousands of active-duty personnel will require barracks, training ranges, pier facilities and hangars. Most critically, the troops will require communication channels including landlines, cell phone towers, e-mail and data networks.

It is in several of these areas that SSC Pacific personnel, already working on the island, and those anticipated to be recruited over the next several years, will be most essential. Work has already begun for the Guam Joint Military Master Plan (GJMMP). In mid 2008, SSC Pacific personnel conducted a six-month preliminary study of the III MEF's information systems, and in October, they revisited Okinawa to determine the electronic and network resources that must be replicated or modernized as the force moves to Guam.

An electromagnetic interference survey of Guam followed in December 2008 which led to the ongoing site survey of proposed Marine Corps training ranges planned for several islands

to the north of Guam in the Commonwealth of the Northern Mariana Islands.

As a result of the studies and subsequent analysis, the SSC Pacific Guam team has identified the requirements for a robust synchronous optical network (SONET) expanded backbone which will require redundancy and bandwidth upgrades to the current Guam backbone; 8,000 network connections (6,000 garrison and 2,000 tactical); and four "battle cabin" command and control centers, one for each Marine general officer of the III MEF.

Additional requirements determined by the study include upgrades to the Joint Worldwide Intelligence Communications System (JWICS); 100 data connections; two Marine Air-Ground Task Force Network Operations Centers; tactical support centers; and training centers.

The team has a C4ISR planning study in progress providing information for military construction (MILCON) documentation and for analyzing electromagnetic radiation for the Guam Build-up Environmental Impact Statement and GJMMP development on both existing and proposed communication systems. Deliverables include creating a preliminary cable distribution system to support information technology service and conducting Hazardous Electromagnetic Radiation to Ordnance (HERO), Facility (HERF) and Personnel (HERP) testing on the planned radio frequency footprint.

The proposed evolution of the Guam network infrastructure, intended to provide common mission and business applications for users, involves progressing from stand-alone networks for each of the four services and the joint command environment to connecting the four service networks to a joint backbone (Phase 1) and then integrating the networks while maintaining their individual integrity (Phase 2).

One of the major efforts required for the successful move of the Marines is their transition from the Navy Marine Corps Intranet (NMCI) to the U.S. OCONUS Navy enterprise network called ONE-NET.

ONE-NET provides centralized control authority for Navy and Marine shore installation users from Europe to the Far East. The Marines coming from Okinawa will transition to ONE-NET, and then later to its planned successor, the Next Generation Enterprise Network (NGEN).

The SSC Pacific Guam facility is responsible for the Marines' transition to ONE-NET and subsequently to NGEN. As information technology advances to an approved Joint Information Environment-Marianas (JIE-M) infrastructure under the Global Information Grid (GIG) 2.0 construct, the long-term end state for all the services in Guam will be a fully implemented Joint Base Network.

Guam facility engineer Regie Pablo spent five months last year upgrading 57 buildings across the island to ONE-NET standards, pulling new cable and installing equipment racks. SSC Pacific's Guam personnel handled infrastructure design and installation. Pablo will eventually take the IT portions of all the installation design plans and further develop them in sufficient detail so that they can be provided to a contractor for the IT installations.

Judy Flores is an IT specialist and program manager working on ONE-NET infrastructure upgrades for other command-funded projects. She is responsible for the ONE-NET installation of the NIPRNET and SIPRNET Protected Distribution System, the physical environment for security. She researches and documents requirements and then helps other commands meet them by coordinating with the local Naval Facilities Engineering Command office, providing site surveys for customers and then planning the installations with contractor support.

There are many other SSC Pacific team members who are working on the Guam buildup efforts. They include: Michael Castro, heading the region's Enhanced Land Mobile Network; Jeffrey LeCureux, heading the Anti-Terrorism/Force Protection Smartgate installations for the region; Klyte Mills, working on the Joint Region Marianas Headquarters C4ISR effort; and Mathew Paco, engaged in creating

SSC Pacific personnel supporting the Guam military buildup include Klyte Mills, Judy Flores, Adrian Gogue, Regie Pablo and Robin Hecita. Below, the USS New Orleans (LPD 18) at the U.S. Naval Base Guam. The Navy is substantially increasing the platforms and personnel assigned to the base. This will require significant network upgrades, many of which are being managed by SSC Pacific personnel.

the initial Marine Corps C4ISR capabilities footprint in the newly renovated Marine Forces Pacific Forward Guam Office.

Frank Salas and Bert Salonga, branch heads in the SSC Pacific Guam facility, are also both leading efforts to increase SPAWAR's presence in C4ISR planning in the Commander, Submarine Squadron 15 headquarters, the new naval hospital, and other long-term planning efforts with the Joint Region Marianas chief information officer staff.

Bill Naputi, managing director of the Guam facility, discussed the changes as the facility works to meet its assigned responsibilities for the buildup, as well as traditional tasking.

"We have grown in the recent past from 22 personnel to 38, with more to come. Our workload, represented by funding, has grown from $3 million to $20 million. We anticipate a large amount of additional work in the 2010-2014 timeframe.

"We do want to avoid growing too large to sustain the civil service population after the buildup winds down, so we will rely substantially on contractors after we grow our in-house workforce to the appropriate level.

"The submarine force will be growing over the next few years, with Ohio and Virginia-class boats coming. We will build up to support them, but cross-train our people because the workload is not always sustainable for the submarine work," Naputi said.

Capt. Miguel San Pedro, Officer in Charge of SSC Pacific's Pacific C4ISR department based in Hawaii, added his thoughts.

"The Guam military buildup is a unique opportunity to provide proven C4ISR capabilities to the joint warfighter in the Asian-Pacific theater. To succeed in this role, however, will require that SSC Pacific has the personnel resources in place to meet the challenge. We already have a talented team in Guam to support the technical network requirements of the buildup. What we lack are the numbers to complete the tasking before us."

George McCarty, a department manager in Hawaii and former head of the submarine communications division at SSC Pacific headquarters in San Diego, is spearheading the recruiting effort.

"Realizing the engineers we have in Guam are working overtime to meet the increased demand, we're actively soliciting SSC Pacific and SSC Atlantic personnel to work with them," he said. "Now is a good time to make the transition, since the major military moves have not yet started and there are still reasonable accommodations available on the island."

An F-22 Raptor and a B-2 Spirit bomber on the flight line at Andersen Air Force Base. A major buildup of military personnel on Guam will include new UAV units at Andersen. Right, the USS Ohio (SSGN 726) moored at the newly renovated Bravo Wharf in Apra Harbor. The Ohio is one of a number of new submarines assigned to Guam. SSC Pacific personnel on the island provide substantial C4ISR support to the submarine force there.

McCarty said the tour requirement is two years, but hopes those interested will stay three or four years to take time to get settled and up-to-speed before the crunch occurs, thus enabling substantial contributions to the buildup effort.

"We theoretically will need 75 government personnel there in three years," he said. "Our primary shortages, and so our prime recruitments, are for engineers, but we are also considering technicians. Although the focus is preparation for the buildup, we are supporting other requirements. Due to Guam's unique position as a gateway to Asia, there are many opportunities in the region for our workforce, such as tasks in Singapore, Diego Garcia, Okinawa and other Asian settings populated with joint/naval activities."

The significance of the Guam buildup was highlighted during a visit April 28 by then-Acting Secretary of the Navy, the Honorable BJ Penn at the Guam Industry Forum. The forum provided private industry representatives an opportunity to understand the requirements for the buildup so they can better support it. In his opening remarks for the forum, Mr. Penn emphatically made the case for the strategic importance of Guam and the military requirements there.

"Indeed, it's not just a matter of national security — the stability of the entire Pacific region depends upon this successful mission," Penn said. "Let me repeat that — it's not just a matter of national security — the stability of the entire Pacific region depends upon this successful mission."

So, for the several dozen SSC Pacific personnel in Guam, and for this small island in the vastness of the western Pacific Ocean, there are large challenges and larger opportunities looming on the horizon. CHIPS

Go to the SPAWAR Web site for more information: http://enterprise.spawar.navy.mil/.

Tom LaPuzza is with the SSC Pacific public affairs office.

DON IM/IT Conference Provides Venue for Feedback

DON CIO leadership asks for input on important policy issues

By Sharon Anderson

The semiannual Department of the Navy Information Management/Information Technology Conference continues to be an important communications tool for the IT workforce and IT users, but communications are meant to be a two-way channel between department leadership and the workforce, said the DON Chief Information Officer team, which hosted the conference. At each session, speakers encouraged audience participation and were eager to hear what the DON workforce and industry partners had to say.

The DON IM/IT Conference was conveniently held at the same time and location as the Joint Warfighting Conference, cosponsored by U.S. Joint Forces Command, the U.S. Naval Institute and AFCEA International. Running from May 11 to 14, the DON IM/IT Conference offered sessions covering many topics, including enterprise architecture, electromagnetic spectrum, strategic sourcing, privacy, asset management, software buying, and DON critical infrastructure protection.

Tom Kidd, the DON director for strategic spectrum and wireless policy, conducted one of the most lively sessions with a number of subject matter experts speaking on naval telecommunications challenges and solutions. Kidd invited command telecommunications managers — as well as the average user — to comment on the department's draft telecommunications policy which is currently under revision.

The Next Generation Enterprise Network (NGEN) session, led by retired Navy Capt. Bob Whitkop, executive director to the Assistant Chief of Naval Operations NGEN System Program Office, drew a large crowd consisting of industry partners and the naval workforce. While industry partners were impatient to gain more insight on the requirements for the network that will replace the historic Navy Marine Corps Intranet, the naval workforce was curious about the improvements NGEN will bring in collaboration tools, applications, bandwidth capacity and security.

Whitkop explained that many organizations, such as the Office of the Chief of Naval Operations, Deputy Chief of Naval Operations for Communication Networks (OPNAV N6), Headquarters Marine Corps C4, the DON CIO, Naval Network Warfare Command and the Program Executive Office for Enterprise Information Systems (PEO EIS) are among others across the department, working to make NGEN a fully integrated enterprise-wide networking environment — a true extension of the warfighting domain.

The IM/IT workforce sessions are always well attended, but perhaps the DON IT Community Town Hall with DON CIO Rob Carey is the most popular. Mr. Carey is the DON IT Workforce Community Leader and he provided his perspective for enhancing warfighter effectiveness through the efforts of the IT workforce. He also provided an overview of IT workforce trends and remarked on the multigenerational nature of the workforce with baby boomers, Generation X and Millennials all working together.

One of the surprises in forecasting workforce trends is that baby boomers have not retired in the large numbers that were originally predicted by the Office of Personnel Management, Mr. Carey said. Still, recruiting a talented, diverse multicultural workforce and enhancing the skills of the current multigenerational workforce to meet the cybersecurity challenges and technologies of the future are ongoing initiatives within the DON, he said.

One of my favorite sessions is the Knowledge Management track always held on the first afternoon of the conference. Jim Knox, the DON KM leader, always has an enthusiastic slate of speakers.

Presenters from Pacific Fleet; Commander, Second Fleet; Multi-National Force-Iraq; Naval Special Warfare Command; and the Virginia Department of Transportation, talked about the challenges and successes of institutionalizing KM in their organizations. They, along with Jim Knox, offered to assist any command or agency in starting a KM program.

The KM community of interest (COI), accessible at https://www.fleetforces.navy.mil/Communities/KMWG/default.aspx, contains a plethora of information on how to begin and sustain KM practices in an organization.

Jim Knox, Department of the Navy Knowledge Management leader, and Tom Kidd, DON director for strategic spectrum and wireless policy, led sessions at the DON IM/IT Conference.

The DON CIO exhibit was busy with DON IM/IT personnel seeking assistance from DON CIO staff.

The DON CIO team also hosted an exhibit at the Joint Warfighting Conference. At the exhibit booth, DON CIO staff provided information about department programs and some of the essential products created by the DON CIO, such as the Computer Network Defense Roadmap 2009, which is included as an insert in this issue, and the Workforce Competency and Career Planning toolkit.

There are so many opportunities for sharing information, networking with colleagues and participating in forums at a DON IM/IT Conference that you can't do it all — but you can try — at the next DON IM/IT Conference, to be held Feb. 1-4, 2010, at the San Diego Convention Center. CHIPS

To request conference presentations and provide feedback for DON policies and future DON IM/IT Conferences, go to the DON CIO Web site: www.doncio.navy.mil.

What does it take to change the world? A few things come to mind: the discovery of fire, the wheel … and a realization that the universe is a much bigger place than we originally thought.

However, since CHIPS is an information technology magazine, we will limit our discussion here to the disruptive information technologies that have transformed cultural models, social structures, economic systems and living conditions in unexpected ways.

Disruptive technologies have four primary characteristics.

✔ They change the environment, usually in multiple areas simultaneously: personally, socially, at work, at home, and with rippling unexpected side effects.

✔ Their environmental changes generate changes in behavior, which may be conscious or unconscious, in a growing fraction of the population.

✔ The combination of environmental and behavioral changes creates new paths of least resistance that turn a disruptive technology into an essential technology used by a majority of the target population.

✔ The unintended side effects of disruptive technologies are frequently more disruptive than the effects associated with their primary purpose. Truly disruptive technologies generally cause changes well beyond the boundaries of their original purpose.

Disruptive IT — the First 5,000 Years

To give us a frame of reference, we will start by looking at information technologies that disrupted the world long before computers.

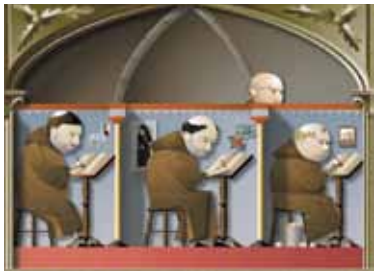
The earliest form of IT began with the advent of writing around 3100 B.C. Painting pictures on cave walls was also a milestone, but pictures of early humans hunting are considered illustrations, whereas, writing is the representation of language in a textual medium through the use of a set of signs or symbols.

Two subsequent disruptive technologies were both more efficient ways of producing written language: the printing press in about 1440 and improvements to the typewriter in the mid-1880s.

The printing press automated, to a degree, the process of reproducing copies of religious and literary works. Before the printing press, the most literate group in Europe were clergymen who were the foremost copyists of the day. The printing press took book copying out of the hands of the clergy, which contributed to changes in the political and religious landscape by making it much harder for anyone in authority to control or censor what was being written.

As use of the printing press spread across Europe, thousands of written works became available to the population writ large, generating a tremendous rise in literacy. This explosion of mass literacy gave European nations an enormous competitive advantage and facilitated their colonization and conquest of much of the rest of the world, since, historically; highly literate nations are able to prevail over nations with low rates of literacy.

Other side effects of the invention of the printing press were the development of copyright laws and the importance of authorship and intellectual capital.



While the typewriter originally created just one copy at a time, it allowed faster personal creation of standardized, legible documents, filling a niche not quite covered by the printing press.

The wired telegraph, invented by Samuel Morse in 1835, was the most significant advance in long-distance communications for one simple reason: It was the first time we had a reliable means of communication that traveled faster than we did.

Before the telegraph, it would take days or weeks to send a message across the United States. With the telegraph, it took mere minutes, and once trans-Atlantic cables were laid and the first telegrams were exchanged between America and England in 1858, telecommunications began to "shrink" the world.

As the 19th century ended, the telephone, invented in 1876, and the radio, invented in 1891, completed the basic telecommunications framework that would dominate information technology for many decades.

The telephone was disruptive because, unlike the telegraph, you did not need special training or to learn Morse code to use it. The telephone opened up communications technology for long-distance social and business contact.

In business offices, the telephone, together with the typewriter and adding machine, speeded productivity and simplified the handling of increasing correspondence and records. Improved communications in the early 1900s pervaded American life and led to the expansion of social and intellectual activities. Progress led to a thirst for knowledge and better way of life throughout the entire country.

Radios were one of the first important hybrid technologies, an advance that combined two or more earlier technologies in a single device with a newer, enabling technology. In the case of the radio, it combined aspects of the telegraph (Morse code) and telephone (analog voice transmission) with wireless transmission for portability. Interestingly, the popularity of radio was a huge blow to newspapers. Not only did the radio provide news

and entertainment, but many advertisers migrated to this new medium.

The last great mass advance in analog IT was the television, displacing the radio in popularity, and yet another hybrid that added the transmission of moving pictures with sound. The analog age of IT was soon overtaken by a technology that also evolved from the telegraph on a different path: the digital computer.

The Digital Age

About the same time that the television was becoming a household staple during the 1950s, the first digital computers arrived on the scene. While the computer took a long time to influence the daily life of the average person, its effects have been far-reaching and life-altering for everyone around the globe.

Computers spawned the development of networks, personal computing, and all the various applications that dominate our current work environment and many of our social interactions. As we have previously covered a brief history of personal computing in CHIPS (four articles in the Summer 2002 through Spring 2003 issues), we will not spend a lot of time on those details. What we will do, though, is examine some of the migration paths and relationships between disruptive digital technologies and their analog predecessors.

Virtually every influential technology we use today is derived in some way from previous technologies or processes. Personal computers are hybrids that include the typewriter, television and calculator. The cellular phone is a hybrid of the radio and the telephone. The photocopier is a hybrid of the camera and printer.

There is also a functional relationship between the Internet and the postal service. At its core, a postal service is essentially a structured packet network, though with physical packets and manual transportation. While the Internet operates billions of times faster than snail mail, in many ways, the basic model for the Internet resembles the model used by Benjamin Franklin when he established the U.S. Postal Service in the 18th century.

The end result of this evolution are devices like the BlackBerry and iPhone that include the most common modern IT functions in a single, portable device, albeit with some trade-offs associated with screen size, ergonomics and battery life.

Unintended Consequences

Are the Internet and the World Wide Web the modern equivalents of writing and the printing press, revolutionizing phenomena for the masses giving those who employ them competitive advantage? It would seem so. The last 20 years of business history is littered with the remains of companies and other organizations that either underestimated or overestimated the power and influence of computers and networks. But those effects are a direct result of the application of the technology. Disruptive digital technology has also had some important side effects.

For example, migrating document preparation from typewriters to word processors resulted in a change in expectations. The task of creating a document with a pen or typewriter was a single event. Corrections were laborious and could require retyping the entire document. Word processors, on the other hand, made changes easier.

E-mail generated disruptions on several levels. Initially, some people saw e-mail as a potential replacement for postal mail. While it has arguably cut into the post office's revenue, it has not put the U.S. Postal Service out of business. What e-mail did, in combination with the computer, was give people a much more prolific way to exchange a larger volume of informal communications.

The most radical effect of e-mail was on organizational power structures. Before e-mail, power and knowledge in most organizations were held exclusively by executives who worked face-to-face or over the telephone. Written communications were highly structured and tightly controlled. E-mail shifted that balance of power by giving people at lower levels an easy way to communicate without regard to location or distance.

Another unintended technology side effect is 24/7 access made possible by the pager, cell phone and, subsequently, the BlackBerry. Yes, we now have 24/7 access to information, but the other side of the equation is that other people expect to have 24/7 access to us. This has radically changed the work and life dynamic for a lot of people.

Turning the Tide

We still have the opportunity to learn lessons from previous examples of disruptive technology to try and turn new ones into controllable tools for shaping our environment, instead of uncontrollable waves of change that drag us into their undertows and riptides.

There are some new technologies entering the IT environment that may offer us some relief from the excesses of our past and present. Before we discuss them, we should have a framework for how to assess their potential.

When considering a new technology, start with its output. What specifically does it produce, and what relationship does its products have with things you are already producing? To use e-mail as an example, at a basic level, it produces correspondence.

When we know the outputs, we can then try to predict outcomes by comparing how the new technology functions with how the old technology functions in five key areas: cost, speed, quality, adaptability and satisfaction.

The first four can be compared quantitatively. Does the new technology cost more or less? Does it produce results faster? Do the products differ in content, longevity, accessibility or usability? Does the new system replace more than one old technology?

Most importantly: What can the new technology eliminate? If we do not discard something when we add something, we may only compound our problems.

Satisfaction can be a funny thing to pin down. Why will people buy designer products that do not measure up when compared with ordinary items? I will, for example, never understand why anyone would buy a collar for a dog that costs more than my car. Satisfaction based on function I can understand. Satisfaction based primarily on status is a delusion that only the wealthy or a wannabe can indulge.

The Next Wave

So, what is on the disruptive technology horizon? Here are my current three picks for technologies that will lead the next wave of change.

First on my list is public key infrastructure, also known as PKI. This is not a new technology; however, people have been trying to figure out how to implement PKI on a large scale to establish digital identity for more than 15 years. There are some applications in use today, but no common standard that would allow establishment of a single digital identity to replace the current de facto standard for uniquely identifying a citizen of the United States: the Social Security number.

Social Security numbers were never intended to be used as a universal identification number, but became one due to the absence of any other identifier. Someone will eventually develop a digital alternative, and it will change the world.

Second is another old favorite in a new wrapper: thin client applications. We moved from mainframe-based systems to desktop office automation software decades ago because we saw personal computers as a less expensive alternative. Early attempts at Web-based office applications that tried to duplicate thin client functionality were unsatisfying on a variety of levels, so we still use thick client software that can be expensive to license and keep up-to-date.

However, Google Docs may finally be the harbinger of Web-based office software that breaks the "everything on the workstation" paradigm. Google Docs is a Web-based set of applications for word processing, presentation and spreadsheets.

My daughter and her 8th grade classmates do all of their homework in Google Docs. It does not matter where they are, what computer they are using, or what browser they use. They work on the same document while collaborating in real time without having to buy and use the same software or cluttering their hard drives with multiple versions of the same project.

Do Google Docs applications have all the functionality of the office software most of us use? No.

Do Google Docs applications have the functionality people need for most tasks? So far, they appear to work for my daughter and her friends — and do most of what I need, too.

Google Docs, and similar applications, can reduce storage requirements, facilitate collaborative work and, until someone starts charging for the service, eliminate the cost of buying and maintaining software applications. However, I do not see government agencies using these commercial applications any time soon because there is no guarantee of continued service or support, and there are understandable security concerns.

However, if the opportunity arose to license similar, supported Web-based applications within organizational networks, it could revolutionize information management for organizations that adopt this paradigm.

Also, bear in mind that in 20 years my daughter's generation will have brought the work habits they are developing in school into the mainstream of the workplace. If we do not make the move to thin-client applications, they likely will.

Thin client applications may be a major building block that allows another new technology to take hold: the netbook. Netbooks are inexpensive, bare bones portable computers that are larger and more ergonomically friendly than a BlackBerry but smaller and more portable than a full-sized laptop.

If you want a small, lightweight portable computer that connects wirelessly to networks for e-mail, Web browsing and simple document preparation, Google Docs could be one of the capabilities that makes the netbook a viable alternative. Add Voice over IP telephone service and now you have a device that can challenge the current crop of computers and smartphones.

The last technologies to keep an eye on are social media: Facebook and Twitter. Both are rooted in established social processes but are being accelerated by the same forces that made e-mail the juggernaut it is today.

Facebook helps maintain relationships, reinforcing and strengthening both virtual communities of practice and social networks. It is only at the beginning of its evolution, and it will be interesting to see where it goes over the next five years.

Twitter, on the other hand, just seems like a way to send short electronic postcards to everyone subscribed to your "tweets." Yes, it is possible to use it like a mass paging system to pass time-sensitive pieces of useful information to a large number of people. I just have trouble taking a technology seriously when a million people apparently subscribe so they can read what someone ate for breakfast.

Twitter may also contribute to "bullet-point syndrome," a state where people eventually lose the ability to write complete paragraphs consisting of grammatically correct full sentences because they spend most of their time writing short bullet points or computerese slang.

Final Thoughts

In the end, the path of least resistance usually determines which technologies win. However, this does not always mean that the "better" technology will win.

As an example, I offer the Dvorak keyboard designed to be more ergonomically friendly and allow faster typing than the familiar QWERTY keyboard. Why do we still use the QWERTY which was intentionally designed to slow down typists to keep them from jamming the keys on manual typewriters? Because by the time the Dvorak keyboard came along, QWERTY was too well-established to be displaced, even by a superior keyboard layout. The path of least resistance was to stick with what everyone knew.

Sometimes, it pays to hold on to what works and watch other people suffer on the "bleeding edge." Sometimes, however, clinging to the familiar only makes the transition that much more wrenching when a new technology changes the world around us. *The trick is being able to recognize the difference.* CHIPS

Until next time – Happy Networking!

Long is a retired Air Force communications officer who has written regularly 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.

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 500.2 in May 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 May 09 (Please call for extension information.)

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

Carahsoft

Opsware Asset Management – Provides software, maintenance and services.

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

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

Ordering Expires: 19 Nov 09

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

DLT

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

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

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

Ordering Expires: 01 Apr 13

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

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 SmartBUY 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)

Ordering Expires: Upon depletion of Army Small Computer Program (ASCP) 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.gsaweblink.com/esi-dod/boa/

www.it-umbrella.navy.mil

Mercury

Mercury Software - Provides software licenses, training, technical support and maintenance for Mercury Performance Center, Mercury Quality Center, Mercury IT Governance Center and Mercury Availability Center.

Contractor: ***Spectrum Systems, Inc.*** (SP4700-05-A-0002)

Ordering Expires: 21 Feb 09 (New agreement to be awarded. Please call for information.)

Web Link: http://www.spectrum-systems.com/contracts/esi-hp.htm

Database Management Tools
Microsoft Products

Microsoft Database Products - See information under Office Systems on page 57.

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); (757) 284-6570

TKC Integration Services, LLC (W91QUZ-09-A-0001); (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 SmartBUY contract and is open for ordering by all U.S. federal agencies, DoD components and authorized contractors.

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

Special Note to Navy Users: 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 Bill Huber, NAVICP Mechanicsburg contracting officer at (717) 605-3210 or e-mail William.Huber@navy.mil, 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 benefits including substantial cost avoidance for the Department. It facilitates the goal of net-centric operations by allowing authorized users to access Oracle databases for Navy internal operations and permits sharing of authoritative data across the Navy enterprise.

Programs and activities covered by this license agreement shall not enter into separate Oracle database licenses outside this central agreement whenever Oracle is selected as the database. This prohibition includes software and software maintenance that is acquired:

a. as part of a system or system upgrade, including Application Specific Full Use (ASFU) licenses;
b. under a service contract;
c. under a contract or agreement administered by another agency, such as an interagency agreement;
d. under a Federal Supply Service (FSS) Schedule contract or blanket purchase agreement established in accordance with FAR 8.404(b)(4); or
e. by a contractor that is authorized to order from a Government supply source pursuant to FAR 51.101.

This policy has been coordinated with the Office of the Assistant Secretary of the Navy (Financial Management and Comptroller), Office of Budget.

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/deal/Oracle/oracle.shtml

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: 30 Sep 09 (Please call for extension information.)

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

Web Link: https://chess.army.mil/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: JES Identity Management Suite; JES Communications Suite; JES Availability Suite; and JES Web Infrastructure Suite. 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; (301) 731-8105

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: 26 Jun 09 (Please call for extension information.)

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); (800) 645-3042

Ordering Expires: 22 Sep 09

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: 30 Sep 09 (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) 776-8283

Ordering Expires: 31 Mar 10

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: 5 May 09 (Please call for extension information.)

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

Planet Associates BPA - NEW!

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: 1 Jun 14

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

ProSight

ProSight - Provides software licenses, maintenance, training and installation services for enterprise portfolio management software. The software product provides the enterprise with a suite of solution specific applications for Capital Planning and Investment Control (CPIC) Budgeting (OMB 300/53); CPIC Process (Select/Control/Evaluate); IT Governance; FISMA (Federal Information Security Management Act) and Privacy Compliance; Project Portfolio Management; Application Rationalization; Research and Development (R&D) and Product Development; Asset Management; Grants Management; Vendor and Service Level Agreement Management; and Regulatory Compliance. ProSight products have been designated as a DoD ESI and GSA SmartBUY. The BPA award has been determined to be the best value to the government and; therefore, competition is not required for software purchases. Discount range for software is from 8 to 39 percent off GSA pricing, which is inclusive of software accumulation discounts. For maintenance, training and installation services, discount range is 3 to 10 percent off GSA pricing. Credit card orders are accepted.

Contractor: ***ProSight, Inc.*** (W91QUZ-05-A-0014); (503) 889-4813

Ordering Expires: 19 Sep 11

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

Quest Products

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

Contractors:

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

DLT Solutions (W91QUZ-06-A-0004); (703) 709-7172

Ordering Expires:

Quest: 14 Aug 10

DLT: 01 Apr 13

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

Telelogic Products

Telelogic Products - Offers development tools and solutions which assist the user in automation in the development life cycle. The major products include DOORS, SYNERGY and TAU Generation. Licenses, maintenance, training and services are available.

Contractors:

Bay State Computers, Inc. (N00104-07-A-ZF48); Small Business Disadvantaged; (301) 352-7878, ext. 116

Spectrum Systems, Inc. (N00104-07-A-ZF46); Small Business0; (703) 591-7400

Ordering Expires:

Bay State Computers, Inc.: 4 Aug 10

Spectrum Systems, Inc.: 31 Jul 10

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/telelogic/telelogic.shtml

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) 719-1836

Ordering Expires: Effective for term of the GSA FSS Schedule

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

Enterprise Resource Planning

Oracle

Oracle – *See information provided under Database Management Tools on page 54.*

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 currently 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, Army and Air Force will be releasing service-specific DAR guidance for their personnel to follow. Go to the ESI Web site at www.esi.mil for more information.

Guidance Available for Navy Employees!

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.

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

Enterprise BPA for Navy DAR Users:

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: 12 Dec 09

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 over 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

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
http://www.it-umbrella.navy.mil/contract/enterprise/iGrafx/softchoice/index.shtml
Softmart
http://www.it-umbrella.navy.mil/contract/enterprise/iGrafx/softmart/index.shtml
SHI
http://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:

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:

Dell Marketing L.P. *(formerly ASAP)* (N00104-02-A-ZE78); (800) 248-2727, ext. 5303

CDW-G (N00104-02-A-ZE85); (877) 890-1330

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

GTSI (N00104-02-A-ZE79); Small Business; (800) 999-GTSI ext. 2071

Hewlett-Packard (N00104-02-A-ZE80); (978) 399-9818

Softchoice (N00104-02-A-ZE81); Small Business; (877) 333-7638

Softmart (N00104-02-A-ZE84); (800) 628-9091 ext. 6928

SHI (N00104-02-A-ZE86); (732) 868-5926

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

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 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 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/services/gcss-j.html

Contractor: ***August Schell Enterprises*** (www.augustschell.com)
Download Site: http://redhat.augustschell.com
Ordering Expires: 14 Mar 10
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: 9 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 SmartBUY contract and is open for ordering by all U.S. federal agencies, DoD components and authorized contractors.
Ordering Expires: 27 Sep 09 (Please call for extension 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 53Software 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.ditco.disa.mil/hq/contracts/sstewchar.asp

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: http://www.it-umbrella.navy.mil/contract/r&a/gartner/gartner.shtml

DON IT umbrella program

www.it-umbrella.navy.mil
www.esi.mil

Visit our e-commerce site:
www.itec-direct.navy.mil

Page intentionally left blank

Plan to Be There

West Coast DON IM/IT Conference

Feb 1-4, 2010

DEPARTMENT OF THE NAVY
COMMANDING OFFICER
SPAWARSYSCEN ATLANTIC
CHIPS MAGAZINE
9456 FOURTH AVE
NORFOLK, VA 23511 - 2130
OFFICIAL BUSINESS

PERIODICAL POSTAGE PAGE
AND ADDITIONAL FEES PAID
NORFOLK, VA AND
ADDITIONAL MAILING OFFICE
SSC ATLANTIC
CHIPS MAGAZINE
USPS 757-910
ISSN 1047-9988