

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](mailto: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](mailto:chips@navy.mil); Web: [www.chips.navy.mil](http://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](mailto:chips@navy.mil) or phone (757) 443-0905, DSN 646.*



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

## 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*

## FEATURES

**6** CANES  
Delivering C4ISR to the fleet as an enterprise system

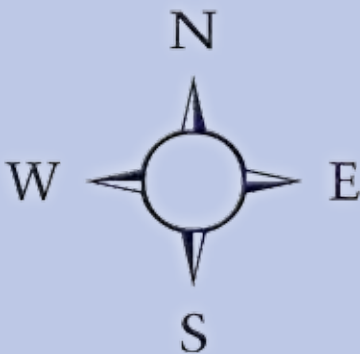
**10** Communications Across the Joint Battlespace  
JPEO for JTRS Dennis Bauman

**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



# 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 USJF-COM 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](http://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.

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.

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 poten-



Mr. Robert J. Carey

tially 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

w w w . d o n c i o . n a v y . m i l

# 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 sub-programs: 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](mailto: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 Radio-



John J. Lussier  
27 July 1959 - 17 June 2009



communication Conference, International Telecommunication Union, and the Federal Communications Commission.

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.

## 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



**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.**

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

**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.**

used to transmit the data, on a wider variety of hardware configurations.

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 Multi purpose 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**

*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.*



**Mr. Dennis Bauman**

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,*



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

*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?*

**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

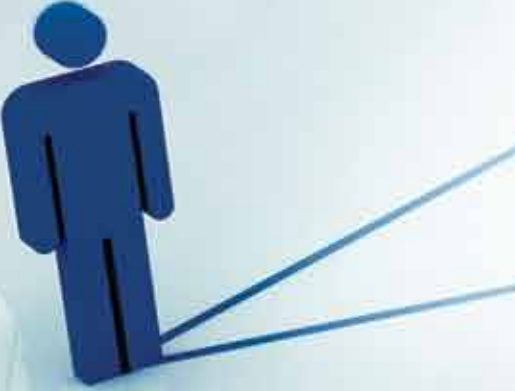
By Mike Hernon



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' Sectera Edge Smartphone and L-3 Communication Systems' L-3 Guardian. As of this writing only the Sectera 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-