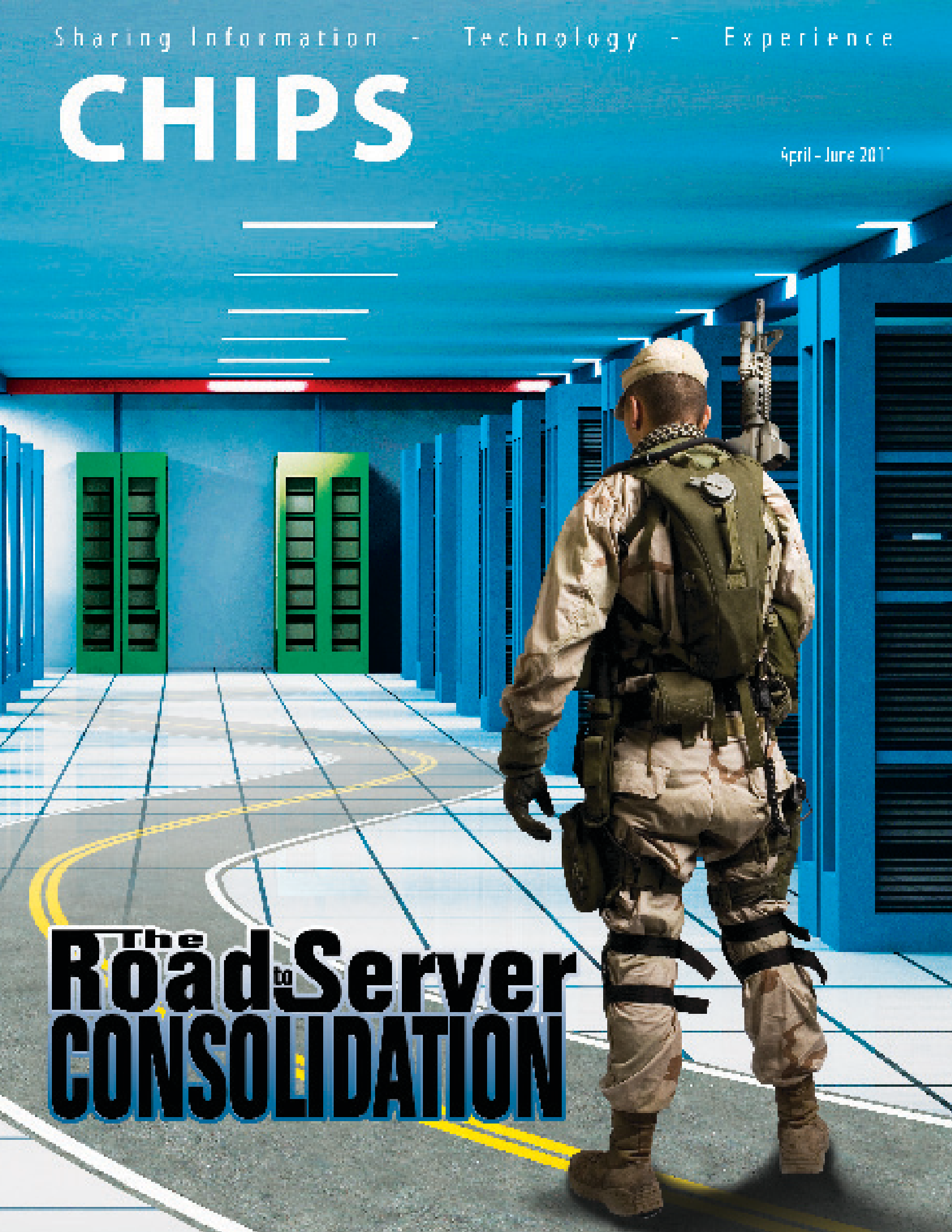
Sharing Information - Technology - Experience

CHIPS

April - June 2017



The Road to Server CONSOLIDATION

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
CHIPS	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department Of The Navy,Norfolk,VA,22511**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
CHIPS April - June 2011,Volume XXIX, Issue II

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**69**	

CHIPS April – June 2011 | Volume XXIX Issue II

Department of the Navy Chief Information Officer
Mr. Terry A. Halvorsen

Department of the Navy
Deputy Chief Information Officer (Navy)
Vice Adm. David J. "Jack" Dorsett

Department of the Navy
Deputy Chief Information Officer (Marine Corps)
Brig. Gen. Kevin J. Nally

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

Space & Naval Warfare Systems Center Atlantic
Commanding Officer Capt. Bruce Urbon

Space & Naval Warfare Systems Center Pacific
Commanding Officer Capt. Joseph J. Beel

Senior Editor and Layout and Design
Sharon Anderson

Assistant Editor
Nancy Reasor

Web Support
Minh Quach, SPAWARSYSCEN Atlantic

Columnists
Tracy Allison, Sharon Anderson, Capt. Josh Dixon, John Gibson, Terry Halvorsen, Norman Jones, Tom Kidd, Steve Muck, R. Ramnarayan, Mark Rossow

---

Contributors
Lynda Pierce, DON Enterprise IT Communications
Holly Quick, SPAWARSYSCEN Atlantic

CHIPS is sponsored by the Department of the Navy Chief Information Officer (DON CIO), the DoD Enterprise Software Initiative and the DON's ESI software product manager team at SPAWARSYSCEN Pacific. CHIPS is published quarterly by SPAWARSYSCEN Atlantic. USPS 757-910 Periodical postage paid at Norfolk, VA and at an additional mailing office. POSTMASTER: Send changes to CHIPS, SSC Atlantic, 9456 Fourth Ave., Norfolk, VA 23511-2130.

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

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

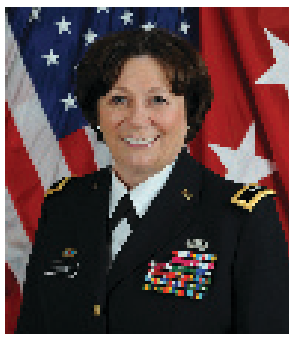
Disclaimer: The views and opinions contained in CHIPS are not necessarily the official views of the Department of Defense or the Department of the Navy. These views do not constitute endorsement or approval by the DON CIO, Enterprise Software Initiative or SPAWAR Systems Centers Atlantic and Pacific.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

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

Online ISSN 2154-1779: www.chips.navy.mil.

Cover

The Under Secretary of the Navy's memo, "DON Information Technology/ Cyberspace Efficiency Initiatives and Realignment," issued Dec. 3, 2010, underscores the challenge by the Secretary of Defense to think about the DON's approach to IT initiatives and to centralize and consolidate efforts where it makes sense. The memo directs DON CIO Terry Halvorsen to take the lead for the department to ensure a common, enterprise approach to IM/IT/cyberspace and IRM activities.



Navigation

More Interviews with

Highlights

In Every Issue

From the DON CIO Special Series on DON IT/Cyberspace Efficiency Initiatives & Realignment

From Around the Fleet and Program Offices

PACIFIC OCEAN (March 29, 2011) A CH-53E Sea Stallion helicopter, assigned to Marine Medium Helicopter Squadron (HMM) 262, takes off from the forward deployed USS Essex (LHD 2) to deliver humanitarian and disaster relief supplies. Essex, with the embarked 31st Marine Expeditionary Unit (31st MEU), is operating off the coast of Kesennuma in northeastern Japan to support Operation Tomodachi. U.S. Navy photo by Mass Communication Specialist 2nd Class Casey H. Kyhl.

Editor's Notebook

In this issue, we look at the efficiencies that can be achieved through improved information technology planning in interviews with top leadership in the information dominance domain, Rear Adm. Michael Broadway, deputy director, concepts and strategies for OPNAV N2/N6, and Mr. Dave Weddel, assistant deputy Chief of Naval Operations for Information Dominance. From the Program Executive Office for C4I, Mr. J. Terry Simpson, principal deputy for intelligence, discusses unmanned vehicles and their importance and challenges in regard to IT planning.

Experts from the DON CIO discuss their subject areas with an eye focused on achieving efficiencies, as directed by the Under Secretary of the Navy in a memo from Dec. 3, 2010, "Department of the Navy (DON) Information Technology (IT)/Cyberspace Efficiency Initiatives and Realignment."

To this end, the DON CIO is engaging with top commercial IT providers in DON desktop services, desktop/laptop operating systems and productivity software, database software, and network technologies to obtain their insight and lessons learned. The DON CIO posed IT strategy questions to Cisco, HP Enterprise Services, Microsoft and Oracle, and you will find their answers in this issue. The industry discussion will continue at the East Coast DON IT Conference in May, where these commercial IT providers will participate in a panel session.

In celebration of the Centennial of Naval Aviation (CoNA), commemorating 100 years of progress and achievement in naval aviation, we are featuring two interviews with Navy pilots: Rear Adm. Wendi Carpenter, Commander, Navy Warfare Development Command, and Capt. Sara Joyner, the first woman carrier air wing commander, who discusses the high-tech systems onboard Navy aircraft. They are emblematic of the pioneer spirit of naval aviation, and there are many others in addition to pilots, including aircrew, maintenance personnel and air traffic controllers.

CHIPS salutes the Navy, Marine Corps and Coast Guard aviation community. The Navy site for CoNA is www.public.navy.mil/airfor/centennial/pages/welcome.aspx, featuring events and historical information.

We are also pleased to feature an interview with the new Army CIO/G-6 Lt. Gen. Susan Lawrence.

In January, CHIPS staff participated in the West Coast DON IT Conference in San Diego, Calif., where we caught up with the dedicated members of the DoD Enterprise Software Initiative team, one of CHIPS' sponsors. At the same time, we exhibited CHIPS with SPAWAR at the West conference.

Welcome new subscribers!

Sharon Anderson

San Diego, Calif. DON IT Conference. The hardworking members of the DoD Enterprise Software Initiative, including the DON's ESI software product manager team and Naval Inventory Control Point Mechanicsburg contracting officers. Front row, from left, Henry Ingorvate, Robert Harden, James Clausen, Floyd Groce and Jim Cecil. Middle row, Chris Panaro, Susan Ellison, Linda Greenwade, Nina Diep, Jeffrey Ho, Thao Vu, Marissa Jackson and Sylvia Neidig. Back row, John Zetter, Bruce Whiteman, Clark Hendrickson, Renée Rothlein, Terri Baxter, Jonnice Medley and Rachel Cadarella.

SPAWAR Commander Rear Adm. Patrick Brady addresses conference attendees at West 2011, cosponsored by AFCEA International and the U.S. Naval Institute. Brady spoke about the Navy's information dominance goals and how SPAWAR's mission aligns with the Chief of Naval Operations' vision for information dominance. Photo by Rick Naystatt/SPAWAR A/V specialist.

A MESSAGE FROM THE

DON CIO

Why IT Efficiencies?

Why is the Department of the Navy aggressively pursuing information technology efficiencies? There are a number of contributing factors that led to the recent focus on efficiencies, but the primary catalyst is the realization by Department of Defense and DON leadership that from a fiscal perspective we cannot continue to do business the same old way, or it will adversely affect our ability to direct necessary resources to the "tip of the spear."

Additionally, striving to implement efficiencies in all areas of our business is always the right thing to do as the stewards of taxpayer money and to most effectively contribute to the nation's defense. If done right, implementing IT efficiencies will lead to significant improvements in the effectiveness and security of the department's IT environment.

Initially, the DON will focus on areas that have great potential for improvements in how we do business and for achieving significant cost savings. These areas include data center consolidation, enterprise software licensing, application rationalization, an enterprise portal environment, review of IT acquisition programs for enterprise effectiveness, video teleconferencing optimization, and enterprise IT workforce initiatives.

When it comes to data center consolidation, we plan to initially target midsized data centers that provide services to an individual command or function. We will analyze them, from a fiscal, functional and security perspective, to determine which facilities can be migrated to enterprise-level data centers run by the Navy, Marine Corps, Defense Information Systems Agency, or other military departments. The initial consolidation targets will provide true cost savings due to reductions in physical plant, power, and data center management contracts.

There are more than 1,600 applications used in the department, many of which appear to perform overlapping functions. Additionally, many applications were not designed to effectively function in forward operating and low-bandwidth environments and, therefore, do not adequately support Sailors and Marines in theater. The number of application variations, and the lack of planning for effective use of available bandwidth, add complexity to the department's network environment and greatly have an impact on performance and security. The department is developing a robust process for reviewing applications and determining which ones should be optimized for use across the enterprise, which should continue to function as is, and which should be "killed." Implementation of this review process has the potential to significantly improve performance for Sailors, Marines, and the supporting establishment and enable us to better secure our network and IT infrastructure.

To be effective and achieve the efficiency potential of an organization with the scale and scope of the DON, we need to begin to operate as a true enterprise. An important first step toward achieving this goal is to put in place enterprise-wide software licensing agreements. Led by the Marine Corps, the department will establish agreements for key applications used across the DON. The agreements will ensure the department is getting the best price possible for widely used applications, and once the agreements are in place, we plan to mandate their use by all DON, Navy and Marine Corps organizations.

All proposed IT efficiency courses of action will be supported by a robust business case analysis, and will be reviewed and approved by the DON Information Enterprise Governance Board. As necessary, the analysis will be reviewed by the DON Large Group, which includes the Under Secretary of the Navy, the Vice Chief of Naval Operations and the Assistant Commandant of the Marine Corps. In this way, we will ensure that we understand the potential costs and benefits associated with pursuing a particular IT efficiency initiative and ensure the department's leadership is fully supportive of pursuing proposed courses of action.

We have a great opportunity to optimize IT operations across the department, and to reinvest the savings achieved by this effort into the tip of the spear. I look forward to aggressively pursuing this opportunity to better serve our Sailors, Marines and supporting establishment. CHIPS

Terry Halvorsen

DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER
www.doncio.navy.mil

Interview with David W. Weddel
Assistant Deputy Chief of Naval Operations for Information Dominance (OPNAV N2/N6)


David W. Weddel

David W. Weddel is a former naval officer. He served as the commanding officer of USS Gary (FFG 51) and as assistant chief of staff for command, control, communications, computers and intelligence (C4I), the N6, for U.S. 7th Fleet, among other assignments. He left active service in 2000.

In November 2009, the Office of Naval Operations (N6) merged with OPNAV N2 forming N2/N6, the office of the Deputy Chief of Naval Operations (DCNO) for Information Dominance. Mr. Weddel was appointed as the assistant DCNO for Information Dominance. In this role he has been tasked to assist in leading the Navy into the information age. Working with Mr. Weddel are seven flag officers, five Senior Executive Service members and the N2/N6 staff who manage a portfolio of 140 programs of just under $12.4 billion per year.

CHIPS asked Mr. Weddel to discuss N2/N6 initiatives, including deployment of unmanned aerial vehicles; he responded in writing in March.

CHIPS: You discussed unmanned systems and vehicles at the West conference in January, and indicated the Navy is accelerating the development of UAVs, including a carrier-based combat UAV. Is there any specific threat driving this urgency?

Weddel: While there are no specific threats that are driving the acceleration of development, the Navy remains committed to the aggressive development of a carrier-based UAV to enhance the intelligence, surveillance and reconnaissance (ISR) capability and persistence that the Navy can provide around the globe, especially to locations where basing rights are not permitted.

CHIPS: Some have said that experimentation and testing are more important than ever with defense budgets so tight. Is there a firm schedule for testing and deploying UAVs?

Weddel: Yes, experimentation and testing are critical elements in the development of UAV systems, not the least of which are efforts to ensure cost savings and efficiency. A number of UAV systems are being tested, and experiments are ongoing in order to meet the objectives of effectively and efficiently integrating these emerging technologies.

The Navy uses laboratory technical development and integrated phased quantitative risk assessments to ensure timely deployment and operational success. An example of this process is the testing and experimentation that is being conducted for VTUAV (vertical takeoff and landing tactical unmanned aerial vehicle) integration with the Littoral Combat Ship program. Navy also continues to work with the Joint Unmanned Aircraft System Center of Excellence to ensure lessons learned from the joint environment are incorporated into Navy systems development.

Our Scan Eagle Unmanned Aerial System is deployed and currently supports naval forces at sea and ashore. The MQ-8B Fire Scout Vertical Takeoff Unmanned Aerial Vehicle is currently deployed aboard USS Halyburton (FFG 40), and an upcoming land-based Fire Scout deployment will provide testing and additional operational data, which we can use to improve this system.

Our Broad Area Maritime Surveillance-Demonstrator (BAMS-D) is currently deployed to the Central Command area of responsibility. Navy is learning a great deal from these ongoing operational tests which will directly impact our emergent UASs, resulting in improved system capability and development as we evolve to [the] MQ-4C BAMS program of record, which will achieve initial operational capability (IOC) in 2016.

The Unmanned Combat Air System Demonstrator (UCAS-D) just completed the first set of flight tests last week (Feb. 4) at Edwards Air Force Base in California. The lessons learned and technology gained from UCAS-D will be incorporated into the Unmanned Carrier Launched Airborne Surveillance and Strike (UCLASS) program of record.

CHIPS: Traditionally, carrier wings have been skeptical about integrating UAVs into operations. Has the Navy been testing this concept in exercises, experiments or modeling and simulation?

Weddel: In the Navy's ISR 'family of systems' approach to information dominance, the vision is a mix of manned and unmanned platforms to meet the information needs of commanders and leaders. While our first carrier and Unmanned Combat Air System Demonstrator is not yet an operational system, the Navy is postured to use lessons learned from UCAS-D flight testing for the development and integration of future operational unmanned systems aboard aircraft carriers.

Modeling and simulation is being used as part of the UCAS-D engineering development process. The Navy is using King Air and F/A-18D aircraft as surrogates to test many of the UCAS-D guidance and control interfaces. The F/A-18D tests will include closed-loop autopilot software performance that progresses to fully coupled approaches to touchdown. Initial surrogate testing will be aboard USS Eisenhower (CVN 69) and is scheduled to begin this spring.

CHIPS: What stage of development are the UCLASS and BAMS programs in?

Weddel: UCLASS is a pre-Milestone A system, with the initial capability document (ICD) entered into Joint Staffing for validation by the Joint Requirements Over-

sight Council. After validation, the ICD will proceed to a material development decision at the Defense Advisory Board.

The BAMS program is in engineering and manufacturing development (post Milestone B), and successfully completed critical design review (CDR) this past February. Component testing is underway and initial developmental aircraft are in production. The next major program milestone is Milestone C, scheduled for mid-2013.

CHIPS: Is the Navy working on how it will analyze and distribute the sensor data from unmanned systems in tandem with the development of UAVs?

Weddel: The Navy recognizes the inherent requirement to enhance legacy processes, procedures and capabilities within the tasking, collection, processing, exploitation and dissemination (TCPED) continuum. As such, we have begun a concerted effort to review how each Navy ISR sensor-platform combination currently conducts, or plans to conduct, TCPED operations. This study will highlight how material and nonmaterial improvements can be combined with a Navywide TCPED end-to-end enterprise designed and constructed to optimally support U.S. and coalition operations with specific focus on the maritime domain.

Notably, the continual improvement in information technology has created significant opportunities to innovate all aspects of the TCPED cycle — from the collection and indexing of individual data points — to the final delivery of comprehensive knowledge to commanders, within the necessary timeline to achieve desired effects.

As an example, cloud computing technologies are one key area under consideration to enable the Navy to recognize and react to current and emerging threats swiftly and decisively. Cloud computing capabilities can be employed by operators and analysts to more effectively perform TCPED operations in direct support of the tactical edge, while simultaneously delivering Navywide efficiencies.

We recognize the importance of approaching this issue from a holistic perspective that employs realistic systems engineering concepts to produce an end-to-end solution that accounts for the 'wholeness' of ISR operations. This analysis will include the need to deliver information across security and classification boundaries to individual personnel, as well as more traditional operational watch centers.

CHIPS: In January, Vice Adm. Dorsett said that the Navy has been "out of balance" and needs to concentrate more effort on the "non-kinetic, information side of the house." Can you discuss what the admiral means by this?

Weddel: We are in a new era where globalization and the convergence of computer and telecommunication networks have transformed the information environment from an enabling capability to a core warfighting capability.

As Admiral Dorsett described recently when speaking of the shift from an industrial age military force to an information age force, 'It's now time for the Navy and, frankly, the U.S. joint forces to step up and start dealing with information in a much more sophisticated manner than they have in the past.'

These new concepts in warfighting are creating opportunities to enhance Navy's contribution to national security, but we must fully integrate information, intelligence, command and control, and cyber capability, and wield it as a 'main battery,' transitioning to an information-centric force. This concept and its instantiation is the non-kinetic warfighting domain.

In the past, the Navy has invested in sensors, weapons and control systems, but suboptimized their overall effectiveness through an architecture that welded them to a single platform. This legacy platform-centric approach unacceptably increases our operational risk as we continue to evolve in the information age. We are addressing these gaps by decoupling, both programmatically and functionally, platform-sensor weapon artifacts and reconfiguring them as distributed, adaptively networked enterprise capabilities.

One of the returns on the investment to reorganize as an information dominance directorate has been the increased opportunity to explore and support non-kinetic operations. Our (N2/N6) Cyber, Sensors and Electronic Warfare Division is doing just that as we mature our thinking and developmental efforts with stakeholders across the Navy and throughout DoD.

CHIPS: The stand up of N2/N6 and the reorganization of cyber within the Navy demanded a cultural shift in how the Navy views information. How would you assess progress thus far?

Weddel: Over the last year we made significant progress in revolutionizing cyber warfare and changing how the Navy views information.

The reorganization is largely complete, and I am pleased with the cultural shift that is well underway. We are changing the culture within our own ranks with the implementation of the Information Dominance Corps.

"While there are no specific threats that are driving the acceleration of development, the Navy remains committed to the aggressive development of a carrier-based UAV to enhance the intelligence, surveillance and reconnaissance (ISR) capability and persistence that the Navy can provide around the globe, especially to locations where basing rights are not permitted."

This professional community of over 44,000 personnel has just completed its first year of standup and, with great support of Navy senior leadership, is developing and maturing the personnel side of information dominance. We have also made cyber a priority in our budgeting process where it is a recognized element in achieving superiority across the full spectrum of naval operations.

The establishment of Fleet Cyber Command/10th Fleet was one of the first steps in changing Navy's understanding of cyber operations. Tenth Fleet's relationships continue to mature with U.S. Strategic Command and the operational management of Navy cyber operations.

Cyber defense is critically important

and certainly is part of the Navy culture. It is an all-hands effort. We are elevating the magnitude of cyber security through the development of a robust network inspection and certification process. The formal network inspections will be conducted across the Navy to enforce accountability and shift fundamental behaviors of how our forces operate, maintain and interact with our networks.

Global standardization of network assets is critical to assuring command and control of forces and warfighting systems. We continue to evolve from static, reactive network operations, to a capability that provides proactive, predictive and dynamic operations.

While we have made tremendous strides over the past year, our work is far from over. The pace at which we are advancing is and will remain demanding. We are a global maritime force, and we recognize that we as a service must advance our capability to plan and execute in cyberspace.

PENSACOLA, Fla. (Feb. 3, 2011) The Center for Information Dominance (CID) has become the first nonoperational shore command approved for the newly created Enlisted Information Dominance Warfare Specialty pin. U.S. Navy photo by Gary Nichols.

"We are changing the culture within our own ranks with the implementation of the Information Dominance Corps. This professional community of over 44,000 personnel has just completed its first year of standup, and with great support of Navy senior leadership, is developing and maturing the personnel side of information dominance."

CHIPS: Vice Adm. Dorsett has set targets for information technology streamlining initiatives in regard to enterprise licensing, virtualization and reduction in data centers. Does the Navy have a data consolidation strategy and a plan for reducing servers and data centers?

Weddel: Vice Adm. Dorsett, in his role as the Deputy Chief Information Officer (Navy), has tasked the Navy to develop its data center consolidation and enterprise licensing strategies. This strategy will detail consolidation plans to ensure that the Navy is gaining efficiencies relative to enterprise licensing, virtualization and data center consolidation.

We are utilizing the Federal Data Center Consolidation Initiative, combined with the direction and guidance within NAVADMIN 008/11 (Navy Information Management Information Technology Efficiencies), to guide and develop that strategy.

We are teaming with the Department of [the] Navy Chief Information Officer to address individual focus areas in the department's 'DON IT/Cyberspace Efficiency Initiatives and Realignment Tasking' effort. Members of our staff are actively involved and are serving as the Navy leads for several of these initiatives. We also remain engaged with OMB (Office of Management and Budget) and the DoD Federal Data Center Consolidation Initiative, which intends to reduce the number of data centers across the federal government.

CHIPS: Reaping the benefits of enterprise licensing is ripe for cost savings, but there is a lot of confusion in the Navy about the differences in licensing models, and many commands purchased licenses for applications that are already available on the Navy Marine Corps Intranet. How can the Navy reduce the confusion and help commands meet the Navy's IT cost-saving goals?

Weddel: A centralized solution to enterprise software licensing (ESL) will reduce the confusion and help commands meet the Navy's IT cost-saving goals. DON CIO, the Program Executive Office [for] Enterprise Information Systems (PEO EIS), U.S. Marine Corps, and OPNAV N2/N6 are all working together to establish more rigorous and streamlined ESL policies and procedures.

The 20 December DON CIO memo, DON IT/Cyberspace Efficiency Initiatives and Realignment Tasking, designated the Marine Corps as the DON enterprise software licensing lead. We are actively participating in the DON ESL working group that will address plans to centralize the procurement and management of DON software licenses, support license allocation and tracking, and enable cost recovery for the enterprise.

CHIPS: Anything else you would like to add?

Weddel: With the vision and active support of the Chief of Naval Operations, Adm. Gary Roughead, and the leadership of Vice Adm. Dorsett, we have made great strides in elevating information as a warfare area within the Navy. But there are great challenges ahead.

All our systems and programs are geared toward one goal — providing our Navy and joint warfighters the information they need, at the time they need it, to make the critical decisions they have to make in support of our forces and our nation. With the standup of the Information Dominance Corps, we are bringing our greatest resource, our people, to bear on the challenges we face. I'm confident we will be up to the task. CHIPS

For more Navy news, go to www.navy.mil.

Q&A with Rear Adm. Michael W. Broadway
Deputy Director, Concepts and Strategies for Information Dominance (N2/N6F)

Since the stand up of the Deputy Chief of Naval Operations for Information Dominance (N2/N6) and Director of Naval Intelligence (DNI) organization in November 2009, with Vice Adm. Jack Dorsett at the helm, Dorsett and his directorate have dramatically changed the face of information dominance and how cyber is viewed in the Navy. Some have compared Dorsett to Adm. Hyman Rickover, known as the "Father of the Nuclear Navy," for his transformational vision of how the Navy now treats information as a critical warfighting domain.

N2/N6 is creating a series of roadmaps for the key components of information dominance to provide a framework for delivering on the Chief of Naval Operations' vision to create a fully integrated information, intelligence, command and control, cyber and networked capability to be used as a naval weapon. So far Dorsett has approved seven of 10 Information Dominance Roadmaps. Rear Adm. Broadway has been leading the effort to create the roadmaps in his role as deputy director for concepts and strategies.

Rear Adm. Michael W. Broadway

Rear Adm. Broadway was commissioned through the NROTC program at Auburn University in December 1974. He was designated a naval flight officer in January 1976, flying the S-3A aircraft. Since affiliating with the Naval Reserve Intelligence Program in 1981, Broadway has served in various naval intelligence leadership positions. As a flag officer, Broadway commanded the Navy Intelligence Reserve Command from February 2007 to November 2009.

Rear Adm. Broadway provided a written response to questions about the Information Dominance Roadmaps in February.

CHIPS: How were the categories of roadmaps selected and prioritized?

Broadway: The Information Dominance Roadmap categories were identified in early 2010 to address some of the highest interest issues facing the Navy. Each roadmap was purposely designed to cover a broad warfare area or warfighting domain that we believed could benefit by adopting the concepts, principles and guidelines outlined in the Navy Information Dominance vision.

Our top priority was the Maritime Ballistic Missile Defense Roadmap, due to the national level attention that followed the president's announcement in late 2009 of the European Phased Adaptive Approach (PAA) initiative, which involves putting a Navy Aegis capability ashore in Eastern Europe.

We also pushed for an early release of the Undersea Dominance Roadmap to coincide with the CNO's approval in 2010 of the high-level document, 'Leveraging the Undersea Environment,' which we believed could also directly benefit from the information dominance vision.

The remaining roadmaps were deliberately kicked off in a phased approach over the first half of 2010 to enable N2/N6 and OPNAV leadership, as well as other Navy stakeholders, to dedicate sufficient time and resources to focus on developing and publishing each individual roadmap.

The original 14 identified roadmaps were reduced to 10. To date, seven have been published and printed with the remaining three undergoing pre-publication review. All 10 will be published along with a capstone document by 31 March 2011. Our plan is to iterate and update the roadmaps, but as we progressed in the development of the original roadmaps, a large number of overlapping capabilities and interdependencies became evident. Our plan as we move forward is to collapse the number of roadmaps into some number that will focus on the information backbone, battlespace awareness, information as warfare, and information in warfare.

CHIPS: What do the roadmaps encompass and who is the target audience?

Broadway: Each roadmap contains a concept white paper that briefly highlights the military problems associated with the subject area; outlines how the information dominance vision could be leveraged to enhance, improve or change the current 'as is' state of affairs; identifies key focus areas where specific improvements in current capabilities could be made, or where the development of new capabilities is warranted. In some cases, we have identified game-changing capabilities. The majority of each roadmap is comprised of a detailed action plan that expands on the key focus areas and outlines specific actions, offices of responsibility and due dates.

The target audience is the Navy as a whole, with an initial focus of articulating how information can be used to enable kinetic or non-kinetic effects, or expand a commander's decision space for exploring tactical, operational or strategic options. They also assist those Navy planners looking to impact information-related programs and capabilities within the current and future POM (Program Objective Memorandum) cycle. They have been useful in dialogues with SYSCOM PEOs (systems command program executive offices) and program managers in discussing how and when capabilities could be introduced into existing platforms, as well as informing the R&D (research and development) community on areas of interest for future naval capabilities.

Information Dominance Roadmap Categories:

- Undersea Dominance
- Maritime Ballistic Missile Defense (BMD) command and control (C2)
- Maritime Domain Awareness (MDA)
- Intelligence, Surveillance and Reconnaissance (ISR)
- Unmanned Vehicles (UxS)
- Cyberspace Operations
- Convergence to Single Network
- Integrated Targeting and Fire Control
- Electromagnetic Warfare
- Spectrum Usage

CHIPS: Do the roadmaps include direction for programs of record?

Broadway: Roadmaps are not spend

plans. Think of them as vectors for their respective areas that move toward increased capability. The initial release of [the] Information Dominance Roadmaps is intended to influence, inform and guide program decisions — but not to direct specific program actions for an individual POR. The roadmaps are intended to assist Navy planners and program managers by highlighting high-payoff areas involving Navy information-related activities where specific changes could and should be made to improve Navy's overall warfighting capability.

CHIPS: Can you talk about the roadmap for BMD? An early vision document stated that the roadmap would address "a concept for the nexus between theater ballistic missile defense, space operations, cyberspace operations, and forward cyber security as a core Navy operating niche." Will the roadmap affect shipbuilding plans or platforms on existing ships?

Broadway: What you are referring to is the concept of the Navy maneuvering at the nexus of the space commons, information commons (to include cyber) and the maritime commons to achieve information dominance.

In the case of BMD, we have developed our roadmap around a series of objective areas that are building to all the issues you mention, as well as to C3I (command, control, communications and intelligence), networking, battlespace management, and the manning and training needed to pull it all together on a daily basis and make it work both afloat and ashore.

This roadmap is a perfect example of the interdependencies among roadmaps that I mentioned earlier. It is a combination of those things I just mentioned, plus important aspects of the single network, spectrum usage, EW (electronic warfare) and cyber operations roadmaps. As we move forward, we will be looking to leverage cyber and EW for both kinetic and non-kinetic effects, not only in BMD, but a number of mission areas.

As to shipbuilding, or affecting platforms on existing ships, remember, we are moving from a platform-centric to information-centric approach to warfare. We are not targeting Aegis-equipped cruisers and DDGs (destroyers), for example, in terms of weapon system and hull design. But hopefully we can affect their employment in the BMD mission. The BMD Roadmap is focused more heavily on the *information* part of the mission. But that does not mean we are on the sidelines by any means. The roadmap's stakeholder group includes key BMD personnel from OPNAV N3/N5 (Information, Plans and Strategy) and N86 (Surface Warfare Division) from U.S. Fleet Forces Command (USFF), COMPACFLT (Commander, Pacific Fleet), the numbered fleets, and especially from Navy Air and Missile Defense Command (NAMDC).

"Roadmaps are not spend plans. Think of them as vectors for their respective areas that move toward increased capability. The initial release of [the] Information Dominance Roadmaps is intended to influence, inform and guide program decisions — but not to direct specific program actions for an individual POR."

So the information dominance issues we are developing in the roadmap align directly with important fleet needs. Working through the stakeholder group, as well as through the Navy Ballistic Missile Defense Enterprise (NBMDE), cochaired by NAMDC and N86, the roadmap has direct influence in many areas. Among them are efforts to improve BMD manning and technical training, and in identifying the Navy C3I supporting the presidentially-directed European Phased Adaptive Approach, which will put Aegis missile systems ashore in Europe, as a land-based adjunct to the Navy's forward-deployed Aegis cruisers and destroyers.

CHIPS: Are any other organizations, in addition to N2/N6, working on the roadmaps?

Broadway: The Information Dominance Roadmap process has been a Navywide undertaking led by the N2/N6 staff. Each roadmap has a N2/N6 'owner' responsible for writing, publishing and executing the roadmap, but the roadmap generation process itself was a wide-open process that invited and involved Navy stakeholders in a number of commands. SPAWAR (Space and Naval Warfare Systems Command), for example, participated in the generation of all the roadmaps, NAVAIR (Naval Air Systems Command), AIRLANT (Naval Air Forces Atlantic), and NSAWC Fallon (Naval Strike and Air Warfare Center aboard Naval Air Station Fallon) participated in a number of air-related ones. NAMDC assisted with the BMD Roadmap, and other OPNAV codes, USFF 'reps' and fleet staffs also contributed in several different areas. Prior to the release of each roadmap, a videoconference was also held with appropriate flag-level stakeholders to review and approve the document.

CHIPS: Do combatant commanders or joint commanders have a voice in the process?

Broadway: We did not directly engage the COCOMs, but did interact with fleet commanders where the subject matter was appropriate. In identifying gaps for each roadmap we also examined and reviewed both Navy and COCOM identified gaps and requirements in each roadmap area to determine high-interest issues where we thought we could leverage and exploit the information dominance vision to benefit the Navy and, by extension, the COCOMs.

CHIPS: Vice Adm. Dorsett said that N2/N6 is going to focus on processing, exploitation and dissemination of intelligence data this year. How will this be accomplished?

Broadway: In building the individual Information Dominance Roadmaps, common issues and themes involving tasking, collection, processing, exploitation and dissemination (TCPED) were identified in virtually every roadmap, indicating the need for special emphasis in this area. We, therefore, launched another major effort geared towards specifically addressing the multitude of TCPED issues identified in the roadmaps.

We are actively developing courses of action to determine the best way for Navy to optimally organize and employ its existing resources to handle the large amounts of sensor data we see coming in the next few years from the many new unmanned systems the Navy is acquiring. We will be addressing, not only the platforms and their sensors, and their associated command and control, but

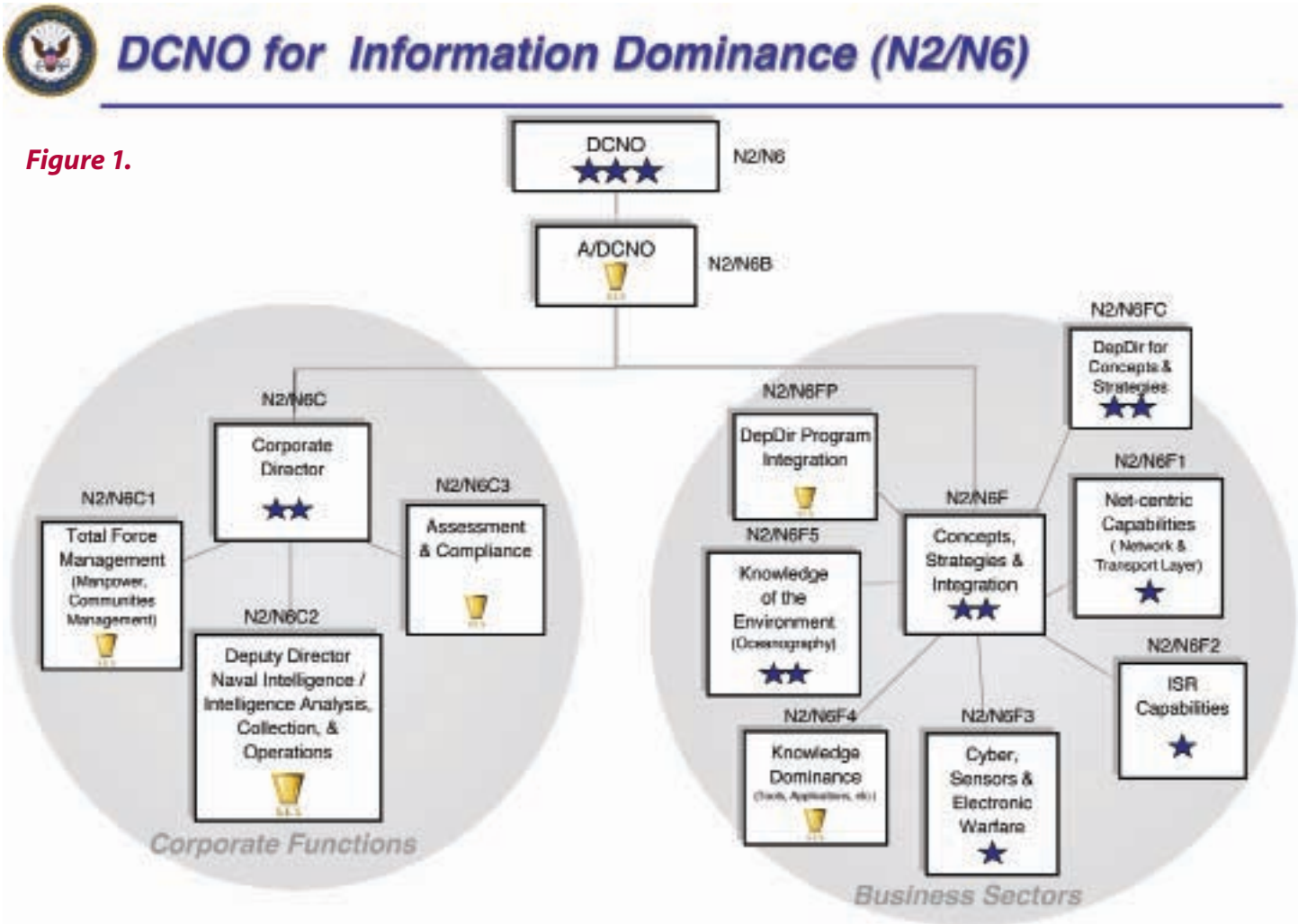


Figure 1.

command and control of the tasking and collection process (TC) and the processing, exploitation and dissemination (PED) process.

We will also be addressing the required transport to move the vast amounts of data, associated data strategies and cloud computing. We will leverage the experience and capabilities of the Army and Air Force where applicable, as well as the capabilities and tools of the combat support agencies, and the intelligence community.

CHIPS: Have budgetary concerns affected the timing for release or scope of the roadmaps?

Broadway: As I mentioned before, if you consider the roadmaps as vectors then you can consider the funding as the velocity component of that vector. We kicked off these roadmaps knowing that the nation's budget issues would impact DoD and Navy budgets in future years. So we did not have to adjust the timing or scope of these roadmaps due to budgetary issues. We did, however, focus on identifying low-hanging fruit and potential quick-wins for the POM 12 and 13 cycles, and we were successful in addressing a number of our information dominance focus areas and priorities in the latest budget.

These completed roadmaps now comprise an integrated and comprehensive plan that identifies workable information-related solutions for future POM cycles, and we intend to update these roadmaps in the years ahead. Our intent is to maintain the direction of those vectors, knowing full-well the velocity, or funding, will depend on priorities within the entire Navy portfolio. Ultimately, these roadmaps will help guide the way the Navy employs its vast information-related resources, [and] collects and processes data into information and intelligence to fully enable 'Decision Superiority in the 21st Century.'

CHIPS: Can you discuss the area of responsibility for the concepts, strategies and integration directorate?

Broadway: The concept, strategies and integration directorate (N2/N6F) leads the integration of concepts, strategies, capabilities, networks, programs and initiatives to elevate information to the envisioned core Navy warfighting capability.

The directorate plans, executes and facilitates strategic decision support for the CNO and Navy leadership regarding information dominance, integrating strategies, concepts, and current and future operational environments with investment plans. (See Figure 1.)

N2/N6F is the resource sponsor for Navy C4ISR (command, control, communications, computers, intelligence, surveillance and reconnaissance), cyberspace operations, EW, MDA (maritime domain awareness), space and naval oceanography programs.

The alignment and synchronization of programs and policies, not only across Navy in these areas, but across the services, joint, national and civil sectors, is also a major part of the mission. CHIPS

Go to www.navy.mil for more Navy news.

Interview with Rear Adm. Wendi B. Carpenter Commander, Navy Warfare Development Command


Rear Adm. Wendi B. Carpenter

Rear Adm. Carpenter received her commission through Aviation Officer Candidate School, Naval Air Station Pensacola, Fla., in 1977 and was designated a naval aviator in July 1979. When the admiral went into the woman's pilot program, it was only a few years old; she was the 31st woman designated. Graduating at the top of her class, she was assigned as the Navy's first Selectively Retained Graduate Instructor Pilot (SERGRAD) in the T-44 aircraft at VT-31, Naval Air Station Corpus Christi, Texas.

Carpenter left active duty and accepted a Reserve commission in February 1985. Remaining highly active in the operational Reserve force, she has accepted numerous recalls to active duty. Carpenter has held a total of five commands at the rank of commander, captain and flag, in the areas of logistics, training and aviation in fleet, joint and coalition operations, giving her a unique warfighting perspective. She has also completed numerous fleet and shore staff assignments.

Carpenter's most recent recall to active duty is her current assignment. In June 2008, she assumed command of Navy Warfare Development Command where she and her team work to deliver capability for Navy, joint and coalition forces through concept generation and development, doctrine, modeling and simulation, and experimentation.

Throughout her career, Carpenter accumulated 3,500 military flight hours. She holds a Bachelor of Science degree in psychology and a master's degree in international relations.

CHIPS: The last time we talked was in August 2008, the day after your promotion and in the middle of the NWDC's move to Norfolk from Newport, R.I. Your lab, the Navy Center for Advanced Modeling and Simulation, is amazing. What makes NCAMS unique?

Carpenter: Virtually everything. Have you ever seen anything like it? The network architecture, technology and distributed nature of what we can do, as well as the incredible team, give us the ability to do Fleet Synthetic Training (FST), wargaming simulation and exercise support on behalf of our fleets. It is a unique capability resident only at NWDC. The technical ability of the engineers and the innovative team we have here is something truly special.

CHIPS: With the closure of Joint Forces Command, will NWDC take on the experimentation and modeling and simulation that Joint Forces Command performs? Will your mission expand?

Carpenter: It would be premature to talk about that as plans are just now being openly discussed and finalized, and we do not know what if anything may directly affect our NWDC team. But irrespective of JFCOM, NWDC's role continues to expand because of our ability in many areas, like doctrinal analysis for fleet and coalition operations, the NCAMS' tactical/operational ability, its command and control linkages, and our value for recommending options across the span of operations. Use of NCTE (Navy Continuous Training Environment) has increased by 75 percent in the last five years. The original intent and vision for NCTE has been long since eclipsed. There remains amazing potential.

CHIPS: I read about your participation in a panel discussion at Notre Dame in February on SouthBendTribune.com where women in combat were discussed. One of the panel members said that technology has leveled the playing field for women where physical strength might have once been a determining factor in what women could do. Now technology can compensate for any physical limitations.

Carpenter: Well, yes it has helped in many ways, but I think it is not the only reason. For example, I was recommended (by the operations officer and others in key roles in the squadron) to be a flight instructor, but I was told that I was too small. That was merely an excuse used by the commander because he was reluctant to break the paradigm. I was only the second women in that squadron, and I flew EC-130s.

When I pointed out that research and tests had shown there were 250-pound former college linebackers who couldn't fly the airplane if the hydraulics failed (called 'boost out') — he really could not object anymore. That fact won the day, and I was allowed to be an instructor. I tell people: size doesn't matter except in a very few specific instances; you have to fly with finesse and also use your head. Any mastery of tactical application can be achieved by anyone with the basic intelligence and drive.

When you think about diversity, recruiting women is a smart way to do business. The diminishing pool of eligible recruits for military service, due to education, fitness and other factors, makes bringing in and retaining more women a strategic business imperative. By excluding women you would eliminate 50 percent of the potential pool. We can excel in the area of the tactical applications of our profession — gender does not matter in that area; nor does it matter at the operational or strategic level. And women should be included broadly across the different communities, not just for numbers, but for the difference in thought and the way we approach decisions. You generally get a better decision by including a more diverse team.

CHIPS: Have you met Capt. Sara Joyner, the first woman carrier air wing commander, who will go to CAG-3 as the deputy CAG starting this summer?

Carpenter: Yes, she is a strong leader with a great reputation. Another tremendous leader is Rear Adm. Nora Tyson, currently in command of Carrier Strike Group Two, and the first female commander of a U.S. Navy carrier strike group.

[Military] women have made a tremendous difference in Afghanistan and understanding cultural differences. Gender simulation training is being developed for many institutions to have a better understanding of culture and gender issues.

I think, very often women have a much better sense of gender and cultural differences. There is evidence to support the idea that a big part of enhancing regional security is through empowering women through education and other opportunities, such as business ownership.

"[Military] women have made a tremendous difference in Afghanistan and understanding cultural differences. Gender simulation training is being developed for many institutions to have a better understanding of culture and gender issues."

CHIPS: When you visit developing countries where women don't have the same opportunities as women in the United States, what are their reactions? Are they intimidated or impressed?

Carpenter: I wouldn't say they are intimidated. I think they are very interested in how things are in this country, and the opportunities that we have. They are happy for us, but desire the same sort of freedoms. Sometimes, I don't think we fully appreciate women's roles in these countries. We have often been naïve to the roles women play in their society and their perspective.

[For example] because of the civil wars in a number of the countries on the African continent, women stepped up to the leadership role in the home and also in areas outside the home. They have held the fabric of their societies together. Yet, they are also often the targets of warfare and terror. But they do not want to be seen as victims. They want to be helped and supported in their efforts to have a better life.

I belong to a group, Women in Aviation, International (www.wai.org/), which was established to encourage women in aviation career fields. I have belonged for about five years; probably more than 75 percent of the members are civilian.

Many of the members are men because they work to open doors for women. There are chapters in other countries as well. I was invited to speak at the opening of a chapter in South Africa by a former Navy associate and longtime friend, Trish Beckman. The CNO was very supportive of my visit there and encouraged me to take a mix of folks with me to make the visit as supportive, and the engagement as rich as possible.

We went to a number of sites to share with high-schoolers and other groups. I am in close and continued contact with many of the women I met at the conference. We have become good friends. Facebook is our method of choice. They ask for advice and support, and they give it back. They appreciate our support, a helping hand, but not taking over. We are sisters in aviation.

The exciting thing is how these engagements and relationships spread through networking to bring other positive influence and effect. From the Facebook postings and interactions with the Southern African WAI Chapter, emerged a challenge from me to one of the folks I mentor — 1st Lt. [Chrystina] Short, United States Air Force. While deployed to Iraq over the past seven months she laid the foundation for and achieved the mile-

U.S. Air Force 1st Lt. Chrystina Short of 777th Expeditionary Aircraft Squadron, C-130 pilot and Horizon East president, poses in front of a C-130 at Joint Base Balad, Iraq, Jan. 8, 2011. Horizon East, the Iraq chapter of the nonprofit organization Women in Aviation, International, was started by women pilots deployed here. It works to inspire and educate Iraqi women for success in aviation careers. USAF photo.

Horizon East has worked with the U.S. State Department, Department of Transportation, Iraqi Ministry of Transportation, Iraqi and U.S. military, aviation corporations and the Iraqi Civil Aviation Authority, as well as the general public, to promote aviation opportunities for Iraqi women.

Kathryn Vernon, Department of Transportation, and U.S. Ambassador to Burkina Faso Jeanine Jackson were tremendously encouraging in the launch of Horizon East, Short said. "Rear Adm. [Wendi B.] Carpenter was instrumental in the effort with her inspiration, mentorship and constant support. She deserves a lot of the credit for making it possible," Short said in an e-mail to CHIPS Feb. 7, 2011.

It is a fitting tribute to the Centennial of Naval Aviation (CoNA), which honors the 100th anniversary of Naval Aviation, to recognize the men and women who pioneered diversity opportunities in aviation and furthered the field of aviation, as well as to recognize new frontiers and trailblazers.

CoNA underscores the commitment to sustaining a Navy, Marine Corps and Coast Guard that wins wars, protects the home front and enables peace. Naval Air Forces are strong because of the support of its service members, their families and the American public. The celebration of Naval Aviation honors America and assures America and its allies that their security is guaranteed by a strong Navy, Marine Corps and Coast Guard team.

For more information about the Centennial of Naval Aviation and events in celebration of CoNA, go to www.public.navy.mil/airfor/centennial/.

stone founding a WAI Iraqi chapter, Horizon East, which opened in January 2011.

These events are a springboard for mentoring and more things that the CNO believes are important outreaches for the U.S. Navy. These organizations, like the U.S. Institute of Peace and Women in Aviation, can be powerful forces for good. CNO is scheduled to speak as the keynote at this year's WAI conference [Feb. 24-26, 2011 in Reno, Nev.]. [Joint Chief] Adm. Mike Mullen has made visits too. He understands their importance and encourages them.

CHIPS: Do you want to share anything else about NCAMS?

Carpenter: This is an incredible facility. I kid around and say I want to move my office into the main area here because I love technology and the *Star Wars* sort of feel. My daughter, Rachel, who knows her mom is a 'geek wanna-be,' calls it the 'central command room.' It does look like something out of *Star Wars* or *Battlestar Galactica*, doesn't it? We have an incredible team with technical know-how and vision; everyone was so diligent to make it right. It represents amazing capabilities for the Navy — a capability that exists because of the brainpower, hard work, devotion and loyalty of the team.

I really admire the technical ability of the engineers here. The director Todd Morgan and deputy director Darrel Morben have immense technical ability, but are outstanding leaders and visionaries, and know how to capture the strengths of the team. I am awed by this incredible and phenomenal facility and the team's ability. I am just privileged they let me hang out with them. I did make a few changes to the facility (it is the interior designer in me). NCAMS is among the finest weapons systems available to the Navy – truly a 'system of systems' with its full potential yet to be realized. The brainpower and energy demonstrated here every day are a marvel to me.

We held an Innovation Summit a few weeks ago with 160 people in attendance. [These events] will do much across the Navy to increase the ability to innovate even further. And this is the place (NWDC) where I think there is the real nexus for this work to be integrated and fully developed on behalf of the Navy and the nation. CHIPS

"NCAMS is among the finest weapons systems available to the Navy – truly a 'system of systems' with its full potential yet to be realized. The brainpower and energy demonstrated here every day are a marvel to me."

Above: (Feb. 4, 2011) NORFOLK, Va. Navy Warfare Development Command's Navy Center for Advanced Modeling and Simulation. NCAMS is a 10,000 square-foot, state-of-the-art modeling and simulation facility completed in June 2010. It supports fleet training, readiness, exercise support and wargaming, as well as Navy concept generation and experimentation, with high-fidelity simulation. The NCAMS synthetic battlespace is a behaviorally accurate, dynamic environmental model used by the Navy, joint forces and coalition partners. Photos by Holly Quick/ SPAWARSYSCEN Atlantic.

For more information about Navy Warfare Development Command, go to http://www.navy.mil/local/nwdc/ or contact the public affairs office at (757) 341-4258.

Implementing DON IT/Cyberspace Efficiency Initiatives & Realignment

By Lynda Pierce

In the January-March 2011 issue of CHIPS, the Department of the Navy Chief Information Officer announced the DON CIO's role in addressing information technology/cyberspace efficiency initiatives and realignment in the Department of the Navy, in response to a memo released by the Under Secretary of the Navy Dec. 3, 2010. The Under Secretary directed the DON CIO to take the lead for this endeavor.

The DON CIO immediately took action, and in a memo issued Dec. 20, 2010, directed three specific DON IT/cyberspace efficiency initiatives: (1) charter and chair a DON IT policy and governance oversight board; (2) establish integrated product teams (IPTs) to tackle individual efficiency focus areas; and (3) publish a new Secretary of the Navy instruction that clearly articulates the roles, responsibilities and relationships of key stakeholder organizations within the information management/IT/cyberspace and information resources management (IRM) framework for the department.

To coordinate efforts, the DON CIO, in partnership with the DON Deputy CIOs (Navy and Marine Corps), chartered the DON Information Enterprise Governance Board (IGB) March 1, 2011, as the department's single, senior IM/IT/cyberspace and IRM policy and governance forum. This executive board is chaired by the DON CIO and comprised of senior Navy, Marine Corps and Secretariat stakeholders. The IGB will review, direct modification, approve, or disapprove DON IM/IT/cyberspace and IRM enterprise initiatives.

The IGB established IT/cyberspace efficiency IPTs structured to enable department-wide solutions that leverage resources and best practices. The IPTs will identify processes and procedures to ensure alignment across the department consistent with Department of Defense practices. The IPTs will work collaboratively and enable participation from across the enterprise to develop effective DON IT/cyberspace efficiency recommendations. They will also conduct rigorous business case analyses as required. If needed, the IPTs will charter working groups and tiger teams to accomplish objectives. The IPTs will report the status of deliverables to the IGB. Focus areas and lead integrators for the IPTs are:

- **Data Center Consolidation:** Identify opportunities for DON data center consolidation and centralization. *Lead integrator: DON CIO.*
- **Application Rationalization:** Identify common applications and tools needed to successfully enable business processes and improve the DON's warfighting capabilities. *Lead Integrator: Assistant Deputy Chief of Naval Operations for Information Dominance (OPNAV N2/N6).*
- **Enterprise Software/Hardware and Software Commodity Purchases/IT Services:** Assess and buy enterprise solutions for achieving the right investment decision for the DON. *Lead Integrator: Marine Corps Systems Command.*
- **Navy and Marine Corps Portal Environment:** Develop a strategy and aggressive plan of action and milestones to implement an integrated Navy and Marine Corps portal environment. *Lead Integrator: DON CIO.*
- **Near-, Mid- and Long-Term Initiatives:** Identify, define and recommend opportunities for IM/IT/cyberspace and IRM efficiency, effectiveness, consolidation, and/or centralization within the DON. *Lead Integrator: DON CIO.*
- **Current and Planned IT Acquisition Programs:** Review existing and planned acquisition programs to ensure alignment and enable the Naval Networking Environment (NNE). Make recommendations to the IGB for changes to programs or requirements, which may be required to achieve the NNE. Stand up for this IPT is on hold. *Lead Integrator: Deputy Assistant Secretary of the Navy C4I and Space.*
- **DON Telecommunications Environment:** Develop a strategic approach and provide recommendations to achieve significant telecommunications cost savings and operational efficiencies across the DON. *Lead Integrator: DON CIO.*
- **IT/Cyberspace Workforce and Training:** Identify, define and recommend opportunities for increasing alignment and possible consolidation or centralization of current and planned DON IT/cyberspace workforce training. *Lead Integrator: DON CIO.*

Scrutinizing the DON's IM/IT/cyberspace and IRM portfolio is ongoing and iterative, aiming for sustainable operations in the most effective and cost-efficient way possible. The DON CIO invites participation and solicits any ideas naval commands may have to achieve a common, enterprise approach to meet the department's operational responsibilities and provide the best equipment and systems to Sailors and Marines.

For the full text of the DON CIO's memo, "Department of the Navy (DON) Information Technology (IT)/Cyberspace Efficiency Initiatives and Realignment Tasking," go to www.doncio.navy.mil/PolicyView.aspx?ID=2073. To see the IGB Charter, go to www.doncio.navy.mil/PolicyView.aspx?ID=2137. CHIPS

Lynda Pierce is the DON CIO chief of staff and DON enterprise IT communications team leader.

Naval Enterprise Networks: The Future of Naval IT

NMCI and NGEN program offices merge

By Michelle Ku

The future of the largest enterprise network in the Department of Defense (DoD) lies in the hands of Capt. Shawn Hendricks, program manager for the Naval Enterprise Networks (NEN) Program Management Office.

On Feb. 24, 2011, the Department of the Navy officially established NEN, which is also known as PMW 205, as the curtain came down on the Navy Marine Corps Intranet (NMCI) and the Next Generation Enterprise Network (NGEN) program offices.

NEN will manage the acquisition life cycle of the DON's enterprise-wide information technology networks. NEN's portfolio of networks includes NMCI, NGEN and the OCONUS Navy Enterprise Network (ONE-Net). NEN provides program management of the NMCI Continuity of Services Contract (CoSC) with Hewlett-Packard (HP), the NMCI and ONE-Net service provider. In the meantime, the NEN program office will continue to develop the acquisition approach and transition strategy roadmap for NGEN's successful implementation. Eventually, the NEN program office will merge with NMCI and ONE-Net into a single enterprise network using the NGEN acquisition approach.

NEN is a strategic and natural evolutionary step in the acquisition of IT networks for the DON, said Rear Adm. Charles "Grunt" Smith, program executive officer for Enterprise Information Systems (PEO EIS). "This is an opportunity to unify the department's terrestrial networks and data management to improve capability and service while saving significant dollars by focusing our efforts under one program office and one enterprise network construct."

NEN program manager Capt. Shawn Hendricks came to the program from the National Reconnaissance Office, where he served as the reconnaissance systems office's principal deputy director. In that post, he led a team of more than 200 military and civilian personnel in the acquisition of a classified spacecraft.

"My vision for the program office is to be the leader in large scale IT procurement, not just in the DoD, but in the federal government," Hendricks said. "When somebody wants to do something of scale in IT, I want them to look to our model and say it is scaled, it is versatile, it is agile, it is efficient, it is effective, it is cost wise, and it serves the people at the level they need to be served.

It is very humbling to be selected as the leader of NEN with its vitally important mission in building the DON's future enterprise network on the foundation of NMCI, ONE-Net and NGEN, Hendricks said. "PMW 205 is about the future. It is a future that provides virtualization, agility, flexibility, mobility and security, all delivered at a better price than they are today. There are no secrets — it is clear what we must do."

"People talk about NMCI seats, a term used to describe an end user's hardware, but it's much more than that," Hendricks said. "The Navy Marine Corps Intranet is the largest weapons system in the world. It touches more Marines, Sailors and civilians each day than any other system in our arsenal. It accomplishes tasks as mundane as entering maintenance data following an engine change or building a PowerPoint presentation, to tasks as life changing as the issuance of orders into battle and, probably more importantly to many, the delivery of a picture of a newborn to a father many miles from home, or the news to a wife or father that their husband or daughter was safe following an aircraft mishap."

Hendricks has a formidable task ahead of him as he takes on a job that has taken two men to accomplish, said James E. Thomsen, principal civilian deputy for Assistant Secretary of the Navy for Research, Development and Acquisition, guest speaker at the establishment ceremony.

It is Hendricks' challenge to "take the network we have today, that we are so dependent on, and with the help of our industry partners, not miss a step and not lose any ground in reliability, supportability and performance," Thomsen said.

Capt. Shawn Hendricks
program manager for the new Naval Enterprise Networks Program Management Office

Merging NMCI and NGEN

Combining the NMCI and NGEN program offices at this time makes sense, Hendricks said. "We have a network that's in operation that will evolve over the next 38 months, and we have a network that will follow it. The same people who are in charge of the operation and maintenance are in charge of planning for the future so that we don't do anything today that hamstrings us for tomorrow. Over time, I believe we will get some efficiency out of it."

The two primary goals of NEN are to ensure that the NMCI network the Navy has today meets the requirements of the fleet and to execute the NGEN acquisition plan to seamlessly transition to a fully government-owned, operated and controlled network by the end of the NMCI CoSC — if not sooner.

The biggest challenges in meeting the goals are time and money, Hendricks said. "NGEN is a very complex acquisition program that must move forward on an exceedingly tight timeline to meet the NMCI CoSC deadline. While the timelines of other programs may slip for one reason or another, the network must be delivered on time," he said.

While the days are already slipping away, budget will be a major overriding factor because the government is operating in an austere environment, Hendricks said. "We have to figure out how to do more, or at least the same, with less. It is a large network, and it comes with an appropriately large bill, but to the extent that we can, we have to try to consume

less and try to deliver the same or better service."

The easiest way for the DON to save money would be to place all 400,000 workstations in the Washington, D.C. metropolitan area with a server farm and help desk nearby, Hendricks said. "But the Navy will not be very well served. So one of the challenges that we have is how do we serve 700,000 users that are spread across the country in remote places, such as a strip mall in Opelika, Alabama, where the recruiting depot is because they have as much right to the network that we provide as I do in my office at the Washington Navy Yard. It is a challenge."

It is a challenge that Hendricks took on because of the importance of IT to the Navy.

"There isn't a broader, more important program in the Navy," he said. "Try to go a day without dealing with one of your IT devices. I challenge anyone to do that, and I certainly know that when the IT devices that our program office provides [to] the senior members of our Navy and Marine Corps don't work, they call really fast because they rely on them."

WASHINGTON, D.C. (Feb. 24, 2011) From left, Rear Adm. Charles "Grunt" Smith, program executive officer for Enterprise Information Systems; Capt. Timothy Holland, the outgoing program manager for the NGEN program office; Capt. Scott Weller, outgoing program manager for the NMCI program office; and Capt. Shawn Hendricks, program manager for the newly established Naval Enterprise Networks (NEN) Program Management Office, or PMW 205, at the ceremony to establish the NEN office. The NMCI and NGEN program management offices were merged at the same time.

Disestablishing two program offices

In addition to establishing NEN Feb. 24, the ceremony was also a celebration of the accomplishments of Capt. Scott Weller, the outgoing program manager of the NMCI program office, and Capt. Tim Holland, the outgoing program manager of the NGEN program office. The two captains were each awarded a Legion of Merit medal for exceptional meritorious leadership and management of their programs.

Weller oversaw the NMCI CoSC negotiations that ensured network services would continue Oct. 1, 2010, at the expiration of the original NMCI contract. The program office continued to advance technical capabilities, such as the hybrid maritime operations centers, with greater command and control capabilities and the synchronized enterprise global address list (GAL) connecting NMCI's directory with e-mail addresses and contact information for personnel from every branch and agency of the DoD.

Due to the hard work of the men and women of PMW 200, the image of NMCI has changed dramatically during his three years as program manager, Capt. Weller said. "Every NMCI office and cubicle in Crystal City and beyond has played an important role in PMW 200's battle plan to win over customers and improve the network these last three years. Not only is the program office set apart by having an incredible collection of government leaders with years of expertise and unstoppable energy to dig in and do what's right, it is supported by the genuine and dedicated efforts of many contractors."

NGEN has had a number of remarkable achievements, Capt. Holland said. The requirements, system design specifications and acquisition strategy have been approved. The integrated master schedule is complete, and every detail of the plan is being worked. The early transition activities have commenced and some have delivered. The intellectual property rights for NMCI have been purchased and infrastructure acquisition has begun.

Holland has been program manager for NGEN since June 2007 and has mixed feelings about leaving the program, he said. "No one can be a part of something as important to our nation and the naval service without taking on a feeling of ownership. I am ready to hand over the helm to Shawn. NGEN deserves a new captain with fresh energy, drive and ideas to take her into the future of naval IT."

The new consolidated program office, PMW 205, has an amazing challenge ahead in continuing to provide the men and women using NMCI and ONE-Net — which represents nearly a quarter of all DoD users — with a high-quality network while moving toward NGEN which is the largest procurement action in the DoD, Hendricks said.

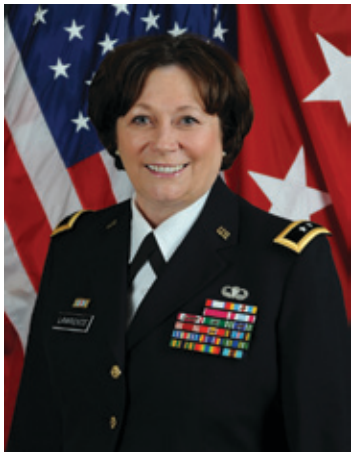
"Ladies and gentlemen of PMW 205, this is your captain speaking — please unfasten your seatbelts, remove the overwing exits and lead us calmly, effectively and efficiently to the network of the future," Hendricks said at the ceremony. "I am honored to join you on this noble journey." CHIPS

Follow PEO EIS on Twitter.com/PEOEIS

Visit the PEO EIS website: www.public.navy.mil/spawar/peoeis/pages/default.aspx.

Michelle Ku is a contractor who supports the public affairs office for the NMCI program.

Interview with Lt. Gen. Susan S. Lawrence U.S. Army Chief Information Officer/G-6



Lt. Gen. Susan S. Lawrence

Lt. Gen. Susan S. Lawrence was assigned as Chief Information Officer/G-6, for the Office of the Secretary of the Army and the Chief of Staff of the Army, Washington, D.C., March 3, 2011. Lawrence most recently served as Commanding General, U.S. Army Network Enterprise Technology Command /9th Signal Command (Army), Fort Huachuca, Ariz.

Lawrence has served as the Commanding General, 5th Signal Command and the United States Army Europe and Seventh Army (USAREUR) Chief Information Officer/Assistant Chief of Staff, G-6 (CIO/G-6). Lawrence's distinguished Army career spans 38 years. She commanded the 7th Signal Brigade, 5th Signal Command, prior to serving as Chief of Staff and Vice Director, J-6, Joint Chiefs of Staff at the Pentagon. She also served as the Director, Command and Control, Communications and Computer Systems, J-6, United States Central Command.

CHIPS spoke with Lt. Gen. Lawrence Feb. 17, 2011, after she delivered remarks to a Women in Defense group in Virginia Beach, Va.

CHIPS: As the commander of the Network Enterprise Technology Command/9th Signal Command (Army) you had the enormous responsibility for operating and defending the Army's information network. The last time you talked with CHIPS in 2009, we talked about the Global Network Enterprise Construct strategy to organize network assets. Can you provide an update?

Lawrence: We are starting to move the football down the field, and we are getting ready to score. If you remember when we talked about the Global Network Enterprise Construct (GNEC), we talked about its three legs. The first leg is the transport, and we are getting ready to put in our fifth regional hub node at the end of this year. Then, any task force will be able to connect globally by reaching any two of our regional hub nodes.

The second leg includes the data and the data strategy. This is part of the Department of Defense's efficiencies — to look at how many data centers we have and consolidate. We are not just doing this in the Army; we are doing it across the entire Department of Defense. The Army is partnering with DISA (Defense Information Systems Agency), the other services, and with industry in some cases, on where to put our data, whether it is in a data center or a 'cloud' virtually, and how to make the data available through the global enterprise network.

The last leg is how we command and control the network, and that is the NETOPS or network operations. We are starting our first big step: single identity and enterprise e-mail. It is a Department of Defense solution, and we are partnering with the other services. We are starting by migrating the Army to an enterprise e-mail. Then very quickly, we will bring in TRANSCOM (U.S. Transportation Command), EUCOM (U.S. European Command) and AFRICOM (U.S. Africa Command), three of our combatant commands.

We are well on our way to delivering the network enterprise.

CHIPS: There has been discussion that already the cyber realm is beginning to be bogged down by layers of bureaucracy and complexity and needs to be incorporated into kinetic warfare. Has the Army realigned cyber as a key warfighting domain as the Air Force, Navy and Marine Corps have done?

Lawrence: There was speculation out there about what's the Army going to do as far as aligning its cyber assets. All along we have been committed to the cyber mission and recognized cyber is a new warfighting domain. We believed that cyber should not be assigned to a current command but a separate command that we stood up in 2010. Our cyber forces are now under that single command, U.S. Army Cyber Command, which is an Army service component command. The commander is Lt. Gen. Rhett A. Hernandez.

Army Cyber Command includes forces from my previous command, NETCOM, and intelligence assets from INSCOM (U.S. Army Intelligence and Security Command) and the Information Operations Command. Army cyber operations now have synergy; we can build, operate, maintain, defend, attack and exploit from a single command.

CHIPS: What is the significance of the Brigade Modernization Command?

Lawrence: We are really excited about the Brigade Modernization Command at Fort Bliss, Texas, which serves as the Army center for network integration. Here, an operational Brigade Combat Team tests and certifies new network technologies and capabilities prior to fielding to operational units. This eliminates the integration burden on deployed units, and provides the most current technology by leveraging commercial industry's developments.

There we are testing anything that can impact the network, whether it is electronic warfare or spectrum. The goal is putting capability in the Soldier's hands as quickly as we can.

CHIPS: The Navy froze its purchase of servers, and halted the creation of new data centers as a step toward reducing its IT infrastructure to save energy, real estate and manpower. The move to reduce data centers is also part of the Federal CIO's push for wider adoption of cloud computing to gain efficiencies and save money. Is the Army moving in this direction?

Lawrence: Before he retired, Army CIO/G-6 Lt. Gen. Jeffrey A. Sorenson signed a moratorium that the Army could no longer procure data center-type equipment until we decided where our final data center sites will be and how we will start moving them. The Base Realignment and Closure activity, or BRAC, has helped serve as a forcing function. Seventeen of our data centers will be closed just from

the BRAC movement, and then we are working another 11 outside of the BRAC as well. Under BRAC, the Army is moving all four-star commands and eight smaller commands.

This year we are going to be executing many other efficiencies. For the most part, they are budgeted in the Program Objective Memorandum for fiscal years 12 to 15.

CHIPS: The Army is expected to cut 27,000 Soldiers, but there is still a need to sustain forces in the field, and also a competing requirement to acquire new equipment and replace worn out and damaged hardware. How do these challenges affect IT planning?

Lawrence: We are going to draw down our forces, and we are going to draw down our budget, as we go through this. The Chief of Staff of the Army is asking his leaders to do a cost-based analysis so we get the most bang for our buck. As we invest the IT dollar, we have to make sure we are investing in the right priorities.

The Network Enterprise Transformation will stay aligned with the operational cadence of our Army and where we need to be at any given time. We will stay focused on that.

We are going to make sure that the network can support all four phases of ARFORGEN (Army Force Generation) — reset, train, available, deploy — as warfighters transition through them. Every Soldier is in one of these phases: (1) reset because they just came back from Iraq or Afghanistan or Bosnia, or anywhere else we have asked them to serve; (2) full training; [and] (3) availability to deploy for any one of the Army's missions.

CHIPS: What has been the most rewarding experience in your Army career?

Lawrence: I am extremely blessed to have had such a wonderful career. I have to say that my best assignments are when I had the opportunity to command our Soldiers and our civilians, the great men and women who serve in our armed forces. That's the most rewarding because you're part of a family, and you're watching these young men and women grow, and they just do so much for our nation. That's where I am closest to them. So whenever I am in command is the most rewarding for me. CHIPS

Above: Maj. Gen. Susan S. Lawrence, outgoing commander, receives the Distinguished Service Medal from Lt. Gen. Jeffrey A. Sorenson, Army Chief Information Officer/G-6. Lawrence received the award during the Network Enterprise Technology Command/9th Signal Command (Army) change of command ceremony Sept. 22, 2010. Photo by Eric Hortin (NETCOM/9th SC (A)).

(Feb. 17, 2011) VIRGINIA BEACH, Va. U.S. Army Maj. Gen. Susan Lawrence speaking at a Women in Defense luncheon. Lawrence was assigned as Chief Information Officer/G-6, for the Office of the Secretary of the Army and the Chief of Staff of the Army, Washington, D.C., March 3, 2011. Lawrence was promoted to lieutenant general March 25. Photo by Holly Quick/SPAWARSYSCEN Atlantic.

"In my career there has never been an environment where Army leaders so clearly understand the need for the network like they do now."

– U.S. Army Chief Information Officer/G-6 Lt. Gen. Susan Lawrence
Feb. 17, 2011

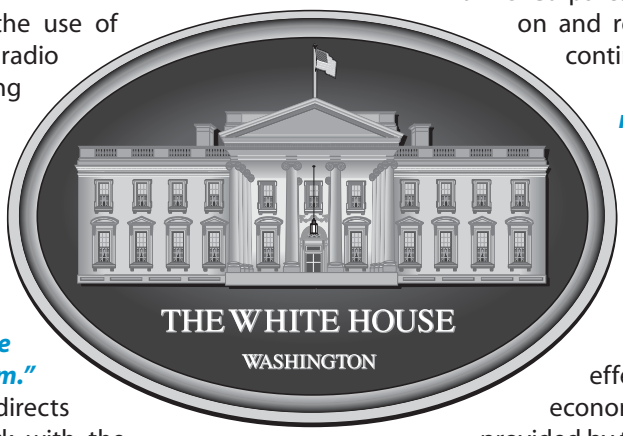
For more information go to the Army CIO's website at http://ciog6.army.mil. The Army CIO strategic communications office can be reached at CIOG6StratComm@conus.mil.

Spectrum Reallocation: Challenges and Opportunities

By Tom Kidd and Mark Rossow

"Few technological developments hold as much potential to enhance America's economic competitiveness, create jobs, and improve the quality of our lives as wireless high-speed access to the Internet," wrote President Obama in a memorandum issued June 28, 2010, titled "Unleashing the Wireless Broadband Revolution."

Now, more than ever before, the use of electromagnetic spectrum, aka radio frequencies, is recognized as having significant contributions to the nation's economy. We need only look around at the myriad wireless devices emerging into the market every day. The President wrote: ***"America's future competitiveness and global technology leadership depend, in part, upon the availability of additional spectrum."*** The presidential memorandum directs the Secretary of Commerce to work with the Federal Communications Commission (FCC) to make 500 megahertz (MHz) of federal and nonfederal spectrum available for wireless broadband use within the next 10 years. The president's directed efforts are intended to make available additional radio frequencies to support and enhance mobile broadband capabilities throughout the United States to spur the economic capabilities of the country.



The memo states: ***"This new era in global technology leadership will only happen if there is adequate spectrum available to support the forthcoming myriad of wireless devices, networks, and applications that can drive the new economy."***

E-commerce, distance learning, and a plethora of other wireless capabilities, not to mention cellular telephones, have dramatically modified private, public, and commercial interests and abilities in the United States. Wireless access is critical to commerce, education and security, and other vital capabilities in the United States, which are now affected significantly by spectrum use. The two naval services within the Department of the Navy (DON) are also experiencing a dramatic increase in spectrum use. Spectrum enables a long list of Navy and Marine Corps capabilities, and their naval reliance on and requirements for spectrum increase continually.

The memo states: ***"The spectrum must be available to be licensed by the FCC for exclusive use or made available for shared access by commercial and Government users in order to enable licensed or unlicensed wireless broadband technologies to be deployed."***

Recognizing the beneficial effects that spectrum has on the nation's economy, as well as the nation's security, as provided by the Navy and Marine Corps, the DON is supporting the Secretary of Commerce, through ongoing Department of Defense (DoD) efforts, to identify spectrum that may be made available to support the president's direction. The DON Chief Information Officer's efforts in this regard are substantial.

The DON is one of the largest users of radio frequencies within the federal government, and its use of spectrum is extremely diverse. As a result of the DON's robust and various uses for spectrum, the DON CIO's spectrum team will conduct intensive analyses on a number of frequency bands to ensure the DON's existing capabilities are not degraded or eliminated when they are relocated to another frequency band, or when they share the use of a frequency band with nonfederal users.

"Spectrum and the new technologies it enables also are essential to the Federal Government, which relies on spectrum for important activities, such as emergency communications,

national security, law enforcement, aviation, maritime, space communications, and numerous other Federal functions," the memo states.

The analyses consider and address complex governance, technical and operational issues, and the results are aggregated to provide decision recommendations to the Secretary of Commerce. However, a decision to reallocate federal spectrum used by the DoD, to nonfederal uses does not solely reside with the Secretary of Commerce.

The National Defense Authorization Act for Fiscal Year 2000 (Title X, Subpart G, Section 1062) requires that the Secretary of Commerce, the Secretary of Defense and the Chairman of the Joint Chiefs of Staff jointly certify that the replacement spectrum band provides comparable technical characteristics to restore essential military capabilities that will be lost when a federal frequency band is reallocated for nonfederal use.

"The Secretaries of Defense, the Treasury, Transportation, State, the Interior, Agriculture, Energy, and Homeland Security, the Attorney General, the Administrators of the National Aeronautics and Space Administration (NASA) and the Federal Aviation Administration, the Director of National Intelligence, the Commandant of the United States Coast Guard, and the head of any other executive department or agency that is currently authorized to use spectrum shall participate and cooperate fully," the president wrote.

The requirement, to jointly certify that federal spectrum reallocations will not result in lost or degraded military capabilities, underscores the fact that the nation's security is comprised of its economic and defense postures and capabilities. This is not a surprise within the DON. Throughout the DON's history, the naval services have capitalized on and employed technology advances that were created, whether in part or in whole, by commercial entities for economic purposes. With this in mind, the risk of losing spectrum within the United States, which is intended to energize wireless broadband use, must be viewed as a potential opportunity for yet another introduction of new and enhanced naval spectrum capabilities.

"As the wireless broadband revolution unfolds, innovation can enable efficient and imaginative uses of spectrum to maintain and enhance the Government's capabilities," the president wrote.

The presidential memorandum, Unleashing the Wireless Broadband Revolution, is available at www.whitehouse.gov/the-press-office/presidential-memorandum-unleashing-wireless-broadband-revolution. CHIPS

Mr. Kidd is the director for strategic spectrum policy for the Department of the Navy. Mr. Rossow is a senior spectrum analyst supporting the DON spectrum team. For more information, contact the DONSpectrumTeam@navy.mil.

GOING MOBILE

Controlling Rising DoD Cellular Service Costs

By John Gibson, Tracy Allison, R. Ramnarayan, Norman Jones and Marine Corps Capt. Josh Dixon

The Department of Defense, through its various commands and programs, contracts a significant number of cellular communications annually. The advent of digital, packet-switched cellular communications, in conjunction with the use of IEEE 802.11n (wireless networking standard), may provide a means of reducing reliance on wired infrastructure for much of in garrison and deployed communications. Smart phones provide a highly flexible platform for mission enhancing tools and critical computational capabilities to fielded troops. The growth of smart phone usage postures wireless technology to become the preferred means of administrative and operational communications for emergency personnel contact, recall and other uses. However, wireless usage assumes a ubiquitous, ever-present infrastructure that is not always accessible within structures or in remote operating locations. Options exist to resolve such issues; however, care must be taken to constrain the cost of acquiring and operating wireless technologies.

This article describes a path to exploring the utility of establishing select in-house services normally associated with mobile virtual network operators as a means of controlling costs. MVNOs provide tailored cellular services as an intermediary between consumers and mobile network operators (MNOs) or commercial wireless providers.

There are two domains in which one might propose the use of cellular technologies; each has a significantly different goal yet the potential for cost savings crosses both. For in garrison use, the potential exists to extend the normal workspace beyond the walls of a cubicle or an office so that the office is wherever the user happens to be. For deployment support, tactical military systems are increasingly overshadowed and outperformed by the capabilities emerging within the commercial sector. Further, commercial off-the-shelf smart phones provide capabilities that support applications that are relevant to the military, such as position/location determination and reporting, movement tracking, orientation, texting and streaming video. Many of these commercial applications are already in use by military members as part of their daily off-duty activity. With the evolution of Web-based information sharing and data rendering standards, such as XML and HTML, the smart phone is also posed as a cost-effective interoperability enabler.

One need not look far to see how cellular technologies are shaping the future of government and business communications, nor to project how they may affect command and control. While the use of cellular technologies has yet to saturate the DoD (i.e., hundreds of thousands of subscribers compared to more than 3 million employees), the number of individual commercial subscriptions for cellular technologies and services issued by DoD is significant. While specific quantities are difficult to enumerate, more than 250,000 cellular service accounts are active within the DoD, not including special programs that have purchased services in bulk to satisfy mission requirements. When emerging initiatives are considered, this number could easily grow to more than 2 million subscribers, many with more than one device. The devices often house more than a single radio transceiver. Miniaturization of smart phone technologies continues, and remote access capabilities are becoming sufficiently secure to meet DoD requirements. Smart phones are more than just personal communications devices; they have become asset tracking and command and control components.

The potential for savings or unnecessary expense is staggering; a situation exacerbated by fragmented technology adoption by DoD organizations. A niche industry, the mobile virtual network operator, has grown within the commercial sector to control cellular service costs within the private and business sectors. MVNOs have made prepaid cellular service and flat-rate subscription service possible.

The DoD has long relied on a mix of contracted and in-house communications services to meet mission requirements. In the 1980s, the emergence of office automation systems changed how documents are generated, reducing the need for clerical support. The emergence of packet-switched networks changed how text and data are delivered. Now cellular technology may represent a revolutionary change in how DoD provides voice services, in and out of the office. When coupled with wireless access to Internet Protocol networks, there is great potential for cost savings. The question then arises: "What is the most appropriate way for DoD to acquire or provide cellular services to personnel?" Perhaps the wireless industry has an answer.

There are options for cellular service that can significantly alter the decision process. Central to this issue are the concepts of the mobile virtual network enabler (MVNE) and the mobile virtual network aggregator (MVNA). A MVNO provides communication services based on the needs and interests of its customer base. A MVNE provides services, such as administration and billing, infrastructure management, technical support, and logistics to the mobile virtual network operator, freeing a MVNO from many operational burdens. A MVNA provides aggregated access to multiple carriers without individual agreements between a MVNO and MNOs. The crux of a MVNO is that its focus is on its customers and how it can tailor applications or services for its customers.

Additionally, a MVNO may opt to employ a limited amount of infrastructure to mitigate coverage issues specific to certain localities or to extend coverage to areas outside that of its supporting MNO/MVNE arrangement. Such might be the case for the DoD, where a limited employment of cellular

infrastructures, for remote locations or within the confines of military facilities, may be used to extend access to areas underserviced by commercial carriers or to provide specialized location-based capabilities.

Several obstacles must be overcome for the DoD to maximize its use of commercial cellular technologies. These include security considerations, acquisition regulations and policy constraints, which may pose a barrier to rapid integration of emerging cellular technologies. Security concerns are being addressed by the commercial sector in response to business considerations as well as privacy issues. Industry may provide paths to resolve similar concerns within military or crisis response operations. However, the accreditation path by which technologies are certified for operational use must support the pace at which technologies are emerging, a daunting task at best. Further, policy directives must allow commanders the necessary leeway to use wireless technologies with careful consideration to the risks associated with them.

Emerging cellular technologies play an increasing role in the day-to-day activities of an ever-increasing number of users. Cellular technologies offer significant opportunities for DoD to leverage. However, without careful consideration, the costs of wireless services may become prohibitive. Careful consideration of the alternatives for acquiring and managing wireless technologies may mitigate the growth of costs. A carefully crafted solution may provide long-term savings, while increasing the communications and computational capability of DoD users and reducing interoperability disparities between data acquisition and delivery systems. CHIPS

Additional information:

- "Mobile Virtual Network Enabler" – www.scribd.com/doc/17688599/Mobile-Virtual-Network-Enabler.
- "What is a MVNE?" and "What is a MVNO?" – www.mobilein.com/what_is_a_mvne.htm and www.mobilein.com/what_is_a_mvno.htm.
- "What does it take to launch a successful MVNO?" (The Besen Group) – www.mobilein.com/MVNO_White_Paper.pdf.
- "14th Mobile Wireless Competition Report" (FCC 10-81) May 20, 2010 – http:// wireless.fcc.gov/index.htm?job=cmrs_reports.

John Gibson is a retired Air Force lieutenant colonel who serves as a lecturer at the Naval Postgraduate School. Mr. Tracy Allison is with the Defense Information Systems Agency and is the chief of the advanced radio frequency branch. Mr. R. Ramnarayan works in the DISA advanced RF branch. Mr. Norman Jones is a retired DISA employee of 30 years and a consultant for DISA supporting the advanced RF branch. Marine Corps Capt. Josh Dixon, previously a computer science and business school student at NPS, is attached to MAGTF C2, Weapons & Sensors Development & Integration (MC2I PG11).

New DON Enterprise Wireless Contracts Driving Cost Savings

By Tine Thompson

The new Department of the Navy enterprise wireless multiple award contracts, covering commercial cellular providers, managed by Fleet and Industrial Supply Center, San Diego (FISCSD), are now in effect. Commands should be aware of the additional cost-saving opportunities now available that can help drive down monthly spending on both wireless devices and services.

Significant changes include:

More vendor choices: all major continental United States providers — AT&T Wireless, Sprint, T-Mobile and Verizon Wireless — now have contracts with the DON;

Free Devices: each plan features up to three free devices;

Unlimited texting: added in response to DON usage trends; and

Tethering: laptop Internet access via smart phone, a low-cost option to an air card – $10/month versus $40.

The DON is taking a comprehensive approach to ensure maximum cost savings are realized on an ongoing basis. To be successful, commands must proactively manage their wireless program or plan, a task that will now be much easier. For example, the new contracts will provide commands with much greater visibility into wireless spending each month through the use of vendor-hosted portals. This will facilitate identifying areas where costs may be managed through better plan selection or elimination of devices with little or no use. The portals will also function as a 24/7 support center and will include the ability to accept submission of requests for quotes and task orders.

Additional actions to support the Navy and Marine Corps in wireless management are underway including the use of expense management tools, and training by FISCSD for transitioning to the new contracts and using the vendor portals. Lastly, the DON Chief Information Officer will release updated guidance to assist commands in reviewing and reducing their wireless costs without any decrease in service.

The contracts, an ordering guide and template, and all the latest information are available on the Naval Supply Systems Command website at https://www.navsup.navy.mil/navsup/ourteam/comfiscs/prod_serv/contracting/market_mgt. CHIPS

Tine Thompson is a strategic marketplace manager on the FISCSD strategic marketplace management team. For further information the FISCSD wireless team may be reached at cellmac@navy.mil.

SPAWAR Project Lead Receives Joy Bright Hancock Leadership Award

By Elisha Sullivan, Space and Naval Warfare Systems Center Pacific Public Affairs

A Space and Naval Warfare Systems Command service member received a Capt. Joy Bright Hancock Leadership Award from the Sea Service Leadership Association and the Military Officers Association of America March 15, 2011.

The award was presented to Lt. Sarah Rice at the Joint Women's Leadership Symposium luncheon at the Sheraton San Diego Hotel and Marina.

"I am deeply honored and would like to thank SPAWAR and the entire Navy engineering duty officer (EDO) community for all the opportunities they have given me. Without those opportunities I would not be receiving this award," Rice said. "They've allowed me to find and pursue some of my passions. The gateway toward success is finding a place where you fit in that is also supportive of what you would like to do."

Rice, a Navy EDO and former surface warfare officer, is assigned to the Space and Naval Warfare Systems Center (SSC) Pacific where she is the project lead for the cryogenic exploration of radio frequency (CERF) project.

The CERF project is using subzero temperatures to make cryogenically cooled, low-noise amplifiers and tunable filters to enhance radio performance and signal reception.

"Lt. Rice just returned from the first installation of CERF capabilities aboard USS Cape St. George (CG 71) where she was able to work directly with Sailors and document the operational parameters of these newly designed technologies," said Anna Leese de Escobar, principal investigator for the CERF project. "This is just another example of the close working relationship SPAWAR maintains with the fleet and the added benefits of having fleet officers, like Lt. Rice, working alongside civilian engineers at SSC Pacific."

SSC Pacific Commanding Officer Capt. Joseph Beel praised Rice's efforts on the CERF project. "Information is a main battery for the Navy. The CERF project is one of many SPAWAR research and development efforts helping to ensure the fleet's ability to seize and control the information domain 'high ground' whenever, wherever and however required for decisive competitive advantage across the full range of Navy missions," Beel said. "SPAWAR plays a leading role in the Navy's ability to maintain a robust set of information capabilities that result in information dominance — the ability to collect, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."

Rice also serves as a member of the retention pillar team of the EDO community diversity working group (DWG) which is responsible for identifying issues and implementing solutions to encourage female junior EDOs to stay in the Navy.

"Navywide, women make up 14 percent of Sailors. In the EDO community, it's about 7 percent, so we're few and far between," Rice said. "I think it's a fantastic way to connect EDOs who have things in common that may not otherwise interact on a regular basis, and to give and receive mentoring advice."

Along with her fellow DWG members, Rice cofounded the "Network of EDO Women" and is actively involved in conferences on both the East and West Coasts.

"We hope to inspire other diversity groups to get together as we have done. I think that one of the first steps to embracing a culture of diversity is to acknowledge our differences, so that they can be appreciated and used to the best advantage," Rice said.

In addition, Rice serves as SSC Pacific's sexual assault prevention and response (SAPR) representative. Through the coordination of training on sexual assault awareness for victim advocates, command leadership, general military and all incoming Sailors, Rice has turned the SAPR into a successful, active and robust program. Her involvement continues through her support of the Navy Region Southwest victims advocate watchbill, remaining on call around-the-clock to respond to victims calling the response line.

Lt. Sarah Rice received the Junior Officer Capt. Joy Bright Hancock Leadership award presented by (from left) Vice Adm. Carol Pottenger and Lt. Cmdr. Nicole Shue at the Joint Women's Leadership Symposium. The awards are presented annually to recognize inspirational leadership of Navy service members on active or reserved duty. Photo by Chief Petty Officer Lesley Maceyak.

Lt. Sarah Rice

Rice has also volunteered more than 60 hours of her own time in support of SSC Pacific's technical outreach program, targeting middle school young women, to promote science, technology, engineering and mathematics.

"I've been raised with the idea that service to others is important. I've also learned that it's sometimes difficult for people to take a first step to ask for help, guidance or even just companionship," Rice said.

Lt. Rice's extensive community involvement also includes holding a position as marketing chair for the Women in Defense San Diego Chapter, volunteering at Habitat for Humanity's Women Build events and serving as a mentor for a "Girls on the Run" 5-kilometer race. CHIPS

4 From Industry

Industry's Perspective on DON IT Challenges: Insight from Cisco, HP Enterprise Services, Oracle and Microsoft

The Under Secretary of the Navy tasked the department to leverage Defense Department IT consolidation efforts and rethink the way the DON approaches information management/information technology initiatives. As the lead for these efforts, the DON Chief Information Officer is focusing on efficiency in all IT areas, including procurement and business processes, and will define a department strategy to shape the way forward in IM/IT and cyberspace ensuring enterprise solutions are developed.

The DON CIO is aware that commercial IT providers have overcome some of the same challenges that the DON is facing. They can provide lessons learned and best practices for current and emerging technologies and business processes. Four commercial IT providers, which provide hardware and software that are critical to DON desktop computing, were asked to share insight on data center consolidation, IT cost-saving strategies and software licensing. The companies sharing their views in these areas are:

- **Cisco –** the predominant provider of switches, routers and network technologies for the DON IT infrastructure. Cisco technology is used for data, voice, video, mobility and security solutions.
- **HP Enterprise Services –** the services provider for the largest DON network (more than 360,000 seats) through the Navy Marine Corps Intranet Continuity of Services Contract (CoSC). HP Enterprise Services supplies and manages the IT infrastructure for the NMCI CoSC, and is the licensor for TRIM, the primary records management software used in the DON.
- **Microsoft –** the predominant desktop/laptop operating system (Windows) and productivity software (Office) for the DON, installed on more than 500,000 computers (including those managed by HP Enterprise Services under the CoSC).
- **Oracle –** the database that the Navy and Marine Corps is licensed to use for business applications. The agreement includes military and civilian personnel, contractor support, as well as non-human devices such as sensors.

Industry participants were asked the same questions and responded in writing.

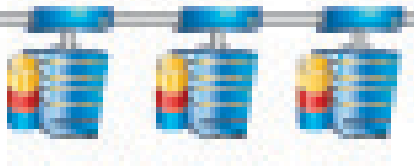
QUESTION 1

The Department of the Navy issued a directive in December 2010 (http://www.public.navy.mil/bupers-npc/reference/messages/Documents/NAVADMINS/NAV2011/NAV11008.txt) that initializes a plan for achieving IM/IT efficiencies through several efforts that will include a reduction in data centers and servers across the department. The DON Chief Information Officer (DON CIO) Terry Halvorsen said the department has to think through a data strategy that meets its business and operational requirements. Mr. Halvorsen said that data must be discoverable, accessible, usable and trusted. There are a lot of opinions on how to structure and consolidate an organization's data. Do you have any recommendations?

CISCO

With shrinking IT budgets and greater demand on computing resources, federal agencies are seeking to consolidate physical infrastructure while at the same time providing agile compute and storage services to their users. Cloud computing is an industry paradigm shift toward the reduction of data center footprints through virtualization (of compute and infrastructure) and segmentation, as well as the decoupling of data from the 'physical' location of the data center. This offers a means for government executives to address issues of budget constraints and agility of service, while safeguarding data and meeting all information assurance (IA)/certification standards.

The previous trend within enterprise organizations was to construct physical 'data centers' in an on-demand fashion as new applications and services were required. This led to the construction of multiple data centers with siloed applications (and infrastructure) that may serve only a single purpose. In some cases a *data center* would be a single server sitting in a wiring closet. Siloed data centers require a tremendous amount of operational overhead and provide very little continuity of operations (COOP) protection. To achieve this goal of COOP, consolidation of infrastructure and agile compute services, federal agencies should begin the migration of services toward a cloud-based architecture that includes compute, network, storage, applications, and management consolidation. The first step in the transition to cloud services is for federal government agencies to define a strategy, architecture, and solutions for cloud computing and data consolidation. Cisco defines cloud computing as a means to deliver IT



resources and services in an abstract fashion from underlying components, with traits of at-scale, on-demand and multi-tenancy. These traits directly contribute to the cost savings (both the operating expenses [OpEx] and the capital expenses [CapEx] sides of the equation) and the flexibility of IT service delivery.

As federal agencies develop a cloud strategy and create their service catalogue, which abstracts the service offering (Software-as-a-Service, Infrastructure-as-a-Service and Platform-as-a-Service) from physical system components, underlying architectural considerations must be investigated. As the application or data is moved into the cloud, the 'data center interconnect' becomes critical. Proper provisioning of bandwidth, quality of service and security must be implemented from the user locations to the data centers, as well as between data centers, providing secure access to applications and data, as well as replication and mobility of the applications and services.

Cisco is using its data center interconnect solutions both internally and to help other IT organizations meet business continuance and corporate compliance objectives, while offering benefits that include:

- Reducing business impact of any disaster events to help ensure business continuance;
- Improving productivity through enhanced application and data availability; and
- Meeting corporate and regulatory compliance needs and improving data security.

These solutions transparently extend local area network (LAN) and storage area network (SAN) connectivity and provide accelerated, highly secure data replication, server clustering, and workload mobility between geographically dispersed data centers. This enhances business resilience and helps enable application and data mobility between data centers, while maintaining operational consistency.

HP ENTERPRISE SERVICES

The Department of the Navy's referenced directive is a positive step to execute a cost-effective strategy that drives a more efficient information technology infrastructure. DON actions to consolidate all of its networks, while ensuring they are interoperable from ship-to-shore globally, is an industry recognized best practice. The DON CIO, Mr. Halvorsen, has acknowledged that to maximize the benefits of a data center consolidation initiative, the DON must also tackle the corresponding applications and data in alignment with consolidation efforts. In HP Enterprise Services' experience, this combined approach generates significant mission and total cost of operations (TCO) benefits.

Some recommendations for a successful data center consolidation strategy are:

1. Align data usage with mission needs: To Mr. Halvorsen's point, the DON's data needs to be discoverable, accessible, usable and trusted. Segmentation of the DON's data and applications into major usage groups would ensure the right people have access to the right data. A one-size-fits-all approach can be limiting for certain mission needs. Examples of usage groups may include: enterprise-wide, mission or command specific, non-specific, individual/collaboration and external usage.
2. Limit and maximize applications: For enterprise and mission data and applications, the Navy should consider rationalizing the applications it's using on the network to limit duplication in functionality and feature. This would enable the DON to reduce cost and to reduce the complexities encountered during the data center consolidation process. In our experience, alignment of action and governance oversight for this effort with the functional area owners yields benefits in time and cost of application migration.
3. Adopt a mission-driven storage platform: For broad-based individual and collaboration data and applications, the DON should consider adopting an enterprise-wide collaboration/storage platform with logical segmentation for community of interest information. Such an enterprise collaboration capability would generate significant warfighter productivity through speed and access. This approach can also lower TCO by limiting data duplication and reducing the number of diverse applications and infrastructure required to access, store and secure the information globally.
4. Link-up the funding authority and governance process. The entity charged with overall execution of large scale data center consolidation benefits from continuous, visible accountability to those responsible for overall mission outcomes and funding responsibility. For mission-driven organizations, such as the DON, such alignment ensures the proper balance of effectiveness with efficiency.

MICROSOFT

The age-old challenge has been and continues to be, how to deliver the right content to the right person at the right time in order to make a decision. Our warfighters deal with this on a daily basis and even have knowledge management cells stood up to address these issues. Organizations need to enable users with desktop and enterprise search capabilities to seamlessly allow discovery across myriad data stores provided by different manufacturers that comply with industry standards of interoperability. As the product lines evolve, the ability to make data more discoverable and accessible is built from the beginning into many products with

the end result a consolidated dashboard, report, or portal experience based on the user's needs.

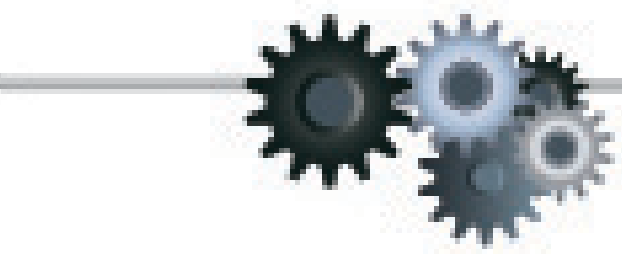
The ability to make data available to the end user at any time, and readable on any device is Microsoft's vision for the future. The Navy's move to consolidate data centers and manage the infrastructure in a more tightly controlled environment is similar to the approach taken at Microsoft to support one of the world's largest networks. In order to run our own networks, we have developed tools that support IT operations, virtualization, data center management, identity and security for our online services. These online services, which have gained an industry term of the 'cloud,' bring capabilities to the user which until recently needed to be hosted by individual commands or companies. Through our partnership with the Navy, many of these capabilities are available today. As the Navy moves forward with data center consolidation, management and virtualization capabilities will be a real key to success.

End-to-end capabilities from data storage and protection to display in a commander's dashboard; these capabilities are available from Microsoft today to assist the warfighter in making the right decision at the right time.

ORACLE

Adoption of a private cloud Software-as-a-Service (SaaS) model and continued focus on service oriented design and governance are key to accomplishing data center consolidation, service discovery, and providing for a secure operational environment. Four fundamental approaches address these requirements:

1. Continue to focus on designing for service orientation. Leverage service oriented architecture governance tools for documentation of SOA assets (services and metadata), service dependencies, and asset discoverability. Focus on reuse of services as enterprise assets. Ensure that requirements for service orientation are part of the acquisition process.
2. Leverage industry standards for service interoperability and Web service security. Use tools for monitoring and auditing service interactions.
3. Leverage the cloud computing SaaS model to provide a secure foundation for deployment of discrete services, service orchestrations and business processes.
4. Use SaaS to provide complete database and shared database services in a Navy private cloud. Reduce number of database versions. Standardize database provisioning, monitoring, audit analysis and security updates. A common infrastructure capable of supporting the demands of online transaction processing, decision support applications and mixed workloads delivers efficiencies for cloud computing.



QUESTION 2

The former deputy DoD CIO Dave Wennergren (now the DoD assistant deputy Chief Management Officer) said the DoD has to stop building a new IT system every time it wants to solve a problem — systems cost too much to deliver and sustain — and they take too long to build. He recommends system reuse and Web services, among other methods. What are some of the considerations or methods to consider in delivering an enterprise IT service across the DoD or DON? Given the unique national security requirements of the DoD, do any of these IT cost-saving strategies make sense: cloud computing, Software-as-a-Service, Infrastructure-as-a-Service or Platform-as-a-Service? Are there any new strategies for savings on enterprise e-mail services?

CISCO

DoD agencies need to balance key mission area requirements when they are looking at technology insertion: warfighting, business, intelligence and the enterprise information environment. There are four major areas where an enterprise organization needs to focus when it is considering technology insertion — governance, compliance, business, and finally, underlying technology requirements. All four of these areas are intertwined and need to be considered when we look at implementing new IT strategies, such as moving applications to the cloud (Software-as-a-Service) or consolidation of IT infrastructure (Infrastructure-as-a-Service or Platform-as-a-Service).

Governance and compliance are two of the most complex tasks to take on when talking about implementation or consolidation of any type of enterprise service. The governance model sets the direction for the life cycle implementation process for that IT service, while the requirements for compliance (certifications and other federal-specific requirements) set the acquisition policy. A balance must be reached between governance and compliance to procure/implement a solution that meets the specific needs of government agencies. As new requirements and services are developed, the governance model must evolve and adapt to the changing technological and business needs.

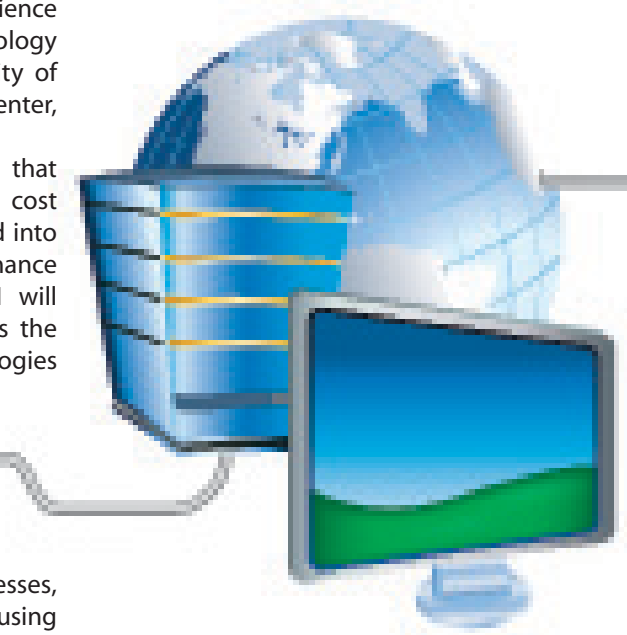
When services are moved to the cloud, whether a private cloud within the Navy or distributed in a community cloud (inter-DoD agency), governance plays a major role. Critical questions that need to be asked when you begin this process are:

- Directing: Who will establish the key IT investments and rules for such investments in each agency?
- Controlling: Who controls processes and services critical to mission and strategies within the agency?

- Executing: Who participates in the execution of processes for services delivery within the agency?
- Communicating: What horizontal and vertical communications are required, and who is responsible for delivering them within the agency?
- Approving and Establishing Principles: Who will approve and guide the establishment of policies related to decision making?

Once the governance questions are answered, the business and technical requirements need to be examined to ensure that the end-user experience is going to provide similar performance and functionality to that of a locally hosted service. A balance must be struck between these two functional areas as well. From a business perspective, it may appear that the best value would be to maximize consolidation efforts, such as SaaS, IaaS and PaaS; however, the end-user experience could be adversely affected due to technology requirements/constraints (bandwidth, quality of service, security, distance of user to data center, etc.).

In summary, Cisco strongly believes that governance policies are key to enabling cost savings for IT infrastructures to be deployed into the DoD and DON enterprises. Once governance policies are evolved, the DoD and DON will then be able to realize cost savings across the enterprise with currently available technologies such as cloud and IT consolidation.



HP ENTERPRISE SERVICES

A. While there are a lot of different processes, HP Enterprise Services recommends using IT Service Management as a guidebook and a method to manage IT services. A one-size-fits-all approach doesn't work, but designing the infrastructure once, keeping in mind that the design should be modular so multiple components fit specific requirements, and building in standardization will lower cost and minimize security risk. With multiple DON entities and industry suppliers interacting to produce IT services, IT Infrastructure Library process implementation broadly is required. These methods and approaches drive reuse and consistency in infrastructure, application, data and Web services across an enterprise like the DON.

B. Given the unique national security requirements associated with DoD IT networks, defense users may wish to consider the adoption of a private or dedicated version — or a hybrid model such as HP Enterprise Services offers of these evolving IT business models.

These emerging business models are pay-for-utilization, pay-as-you-go, and limited upfront investment based models. Providers in these capabilities leverage scale, component uniformity, service consistency and pool excess capacity to make the average costs attractive to their clients. While the DoD as a whole, and most likely, individual services have IT scale at sufficient volume to execute a private version of these models, if commanders share infrastructure control and ownership across organizational boundaries they will achieve reduced TCO. The DoD is large enough in terms of the operations and scale for these models to execute successfully as they have across private industry, but the DoD should consider leveraging and utilizing them as a whole, not four separate clouds or models for each service.

C. Just as with enterprise services, a one-size-fits-all approach doesn't fit all user needs. One strategy for cost savings on enterprise e-mail services that industry is using, is a Web-based system that allows functions, such as [the] calendar [function], to interoperate with other applications. However, the security and resiliency of these approaches may not always be sufficient to adapt to all classifications of data and mission requirements.

MICROSOFT

The Navy has been a leader for years in looking for the right mixture of IT innovation to support the myriad of needs from afloat to ashore. From early efforts to Web-enable the Navy to the largest IT service contract in history, the Navy has been a leader. As the Navy moves towards the Next Generation [Enterprise] Network, it is prudent to consider the options that industry provides today and consider the right mixture of services. There are many options available, such as hosted unclassified e-mail, Software-as-a-Service, Infrastructure-as-a-Service and Platform-as-a-Service. These choices are not all or nothing but can provide the right balance of on-premise and off-premise hosting. At Microsoft, we believe organizations need and want the flexibility and control to consume cloud services in the ways that best meet their unique needs. This is whether in Navy data centers, with a partner-hosted data center or from a Microsoft data center — and whether in a private cloud, public cloud, community cloud or a hybrid cloud. Large, complex organizations, like the U.S. Navy, need to take a holistic approach to get to the desired IT and mission benefits from cloud computing across a matrix of these deployment and service models.

None of these models are all-encompassing. Part of the cloud's unique power is its flexibility. Cloud models are designed to work together, so you can use the right models across an organization, as well as for individual workloads. Microsoft is delivering on that vision today by providing organizations a set of identity, security, management, development and end-user

IT services that are common to, and integrated across, the cloud deployment and service models.

Many federal government organizations are looking to the public cloud to deliver 'utility' workloads, like messaging and collaboration. However for the Navy, the security and other mission requirements needed to support afloat and forward deployed units require on-premise private cloud solutions.

Moving to a private cloud infrastructure can also decrease server and network sprawl and costs by large margins. Properly implementing a private cloud is a complex task that will require significant planning and cooperation among central IT staff and business/program IT consumers. On-premise private cloud computing is about more than leveraging virtualization technologies. While virtualization has resulted in significant benefits in hardware and data center consolidation, creating a private cloud also requires:

- Centralized monitoring across the entire data center from:
  - o server, network and storage hardware;
  - o virtualization and operating system layers; and
  - o health of the application workloads and the end-user experience in consuming them.
- Automation of both the human and IT system processes.
- Management of these resources as a single, expandable fabric.
- Applications and development tools that truly scale up and down.
- IT service management that [is] measurable for business stakeholders.

At Microsoft, we have deployed these solutions to support our own environment and have deployed them to support the military and other federal agencies by defining and delivering the optimal solution needed to bring maximum efficiencies to each organization.

ORACLE

Cloud computing is a significant advancement in the delivery of information technology and services. By providing on demand access to a shared pool of computing resources in a self-service, dynamically scaled and metered manner, cloud computing offers compelling advantages in speed, agility and efficiency. Today, cloud computing is at an early stage in its life cycle, but it is also the evolution and convergence of several trends that have been driving enterprise data centers and service providers over the last several years.

Cloud computing builds off a foundation of technologies, such as grid computing, which includes clustering, server virtualization and dynamic provisioning, as well as service oriented architecture shared services and large scale management automation.

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud service models include:

- Software-as-a-Service (SaaS). Applications delivered as a service to end users over the Internet.
- Platform-as-a-Service (PaaS). Application development and deployment platform delivered as a service in the cloud.
- Infrastructure-as-a-Service (IaaS). Server, storage and network hardware and associated software delivered as a service in the cloud.

Deployment models include:

- Public cloud. Available via the Internet for the general public to use.
- Private cloud. A dedicated cloud for exclusive use by a specific organization or enterprise. Sometimes called an enterprise cloud; can be on-premise or off-premise hosted by a third-party provider.
- Community cloud. Shared by various organizations in support of a specific community; can be either off-premise or on-premise.
- Hybrid cloud. A mix of the specified cloud models cited above, or the use of technologies selected for their cloud capabilities integrated into traditional data centers.

Public sector organizations are increasingly being driven to improve operational efficiency, share information and integrate processes across operational boundaries while maintaining control over costs. Recently, cloud computing has captured significant attention as both a business model and a computing infrastructure model that enables public sector organizations to achieve these objectives.

Several key factors are driving cloud computing in the public sector including centralized IT management and procurement leadership and initiatives, including shrinking agency budgets through the consolidation of data centers and telecom networks owned and operated by government organizations. Here are some of the key points we have seen in the public sector:

- Cloud computing builds on well-established distributed computing and shared services concepts.
- Data center consolidation is a logical step in the evolution of an organization toward a cloud computing model.
- For public sector, the U.S. federal government's National Institute of Standards and Technology provided a comprehensive framework to describe cloud computing, including service and deployment models and a framework for the development of cloud computing interoperability and security standards.

- There are important differences between the public and private cloud deployment models.
- Operating system (OS) virtualization is not equivalent to cloud computing; it is only one of many enabling technologies.
- Virtualization can be delivered at different levels; service-driven virtualization, rather than infrastructure-driven virtualization, is the most beneficial form of virtualization.

- OS virtualization (hypervisor-based) is limited and deficient because it essentially promotes creating 'virtual silos' instead of physical silos; it therefore does not necessarily deliver the benefits of a true cloud model.

Due to security, integration and cost considerations, customers may be looking at private clouds hosted in DoD data centers or third-party service providers that meet DoD requirements.

- Private clouds offer greater control of security, compliance and quality of service. Private clouds enable IT to maintain control of security, including: data loss and privacy, compliance (data handling policies, data retention, audit), and regulations governing data location, and quality of service since private clouds can optimize networks in ways that public clouds do not allow.
- Easier integration. Applications running in private clouds are easier to integrate with other in-house applications such as identity management systems.
- Lower total costs. Private clouds may be cheaper over the long-term compared to public clouds, since it is essentially owning versus renting. According to several analyses, the break-even period is between two and three years.

QUESTION 3

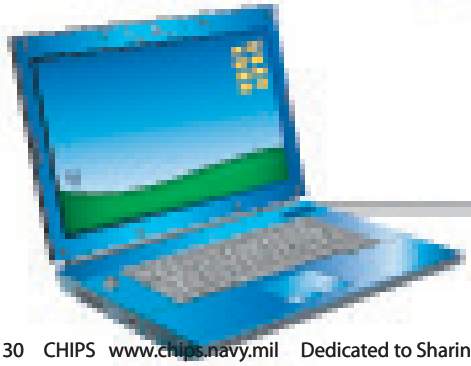
The Defense Department's Enterprise Software Initiative (ESI) (http://www.esi.mil) has negotiated licenses for commercial software applications for the DoD with enhanced terms and conditions that support the department's IT objectives and industry best practices for software management since 1998 achieving more than $3 billion in cost avoidance. How is software licensing in your company managed, and do you have any recommendations for reducing software licensing costs?

CISCO

Federal organizations have made sizable investments in Cisco technology to enable their networks to function as the platform for delivering the full spectrum of data, voice, video, collaboration and mobility services. A key and necessary component in delivering these services is the maintenance of application software, as well as maintenance of the operating system software for the routing and switching infrastructure.

Contract management across a government enterprise can prove to be a difficult and time-consuming task. Across an enterprise, many Cisco hardware procurements are awarded each year on various programs and initiatives with associated services contract numbers generated in relation to those product orders. Maintaining records of all these contract numbers and keeping track of their various expiration dates can cause frustration and lapses in coverage, putting the maintenance of the network at risk. Furthermore, the government is forced to deal with multiple points of contact for their maintenance needs, and contracting officers are forced to handle multiple procurements each year to renew the contracts — as opposed to handling one large, consolidated contract.

Cisco has developed an Enterprise Services Agreement (ESA) concept that is Federal Acquisition Regulations (FAR)-compliant and uses a services contract multi-year consolidation strategy specifically designed for federal end-users to help them alleviate the above described burdens. The multi-year consolidation strategy includes a very simple process of consolidating an



end user's existing services contracts into one list with one coterminous contract end date. Pricing is prorated based on the period of performance required to successfully consolidate and coterminate the contracts. After the base year contract value is established, Cisco also provides up to four additional option year renewal prices to keep the contracts organized in this manner for future out-years.

The Cisco ESA strategy provides the following benefits to our federal end-users:

- Cost control with fixed pricing over the term of the contract.
- Avoidance of Cisco annual service contract price increases.
- Ability to consolidate service contract procurements, reducing government contracting costs.
- Easier to budget with predictable cost year after year.
- One vendor controls the contract throughout the option years, providing one single point of contact.
- Ability to 'true-up' on an annual, semiannual or quarterly basis.
- Comprehensive coverage of network software and assets to improve overall network support.

Cisco has implemented numerous ESAs within the Department of Defense and other civilian federal agencies. These agreements have resulted in tremendous cost savings in actual dollars spent, as well as cost reduction gained through process efficiencies. Having an ESA has also enabled federal agencies to accurately plan for budget expenditures and allowed them to leverage the network as a platform to deliver IT services to improve the end-user experience.

HP ENTERPRISE SERVICES

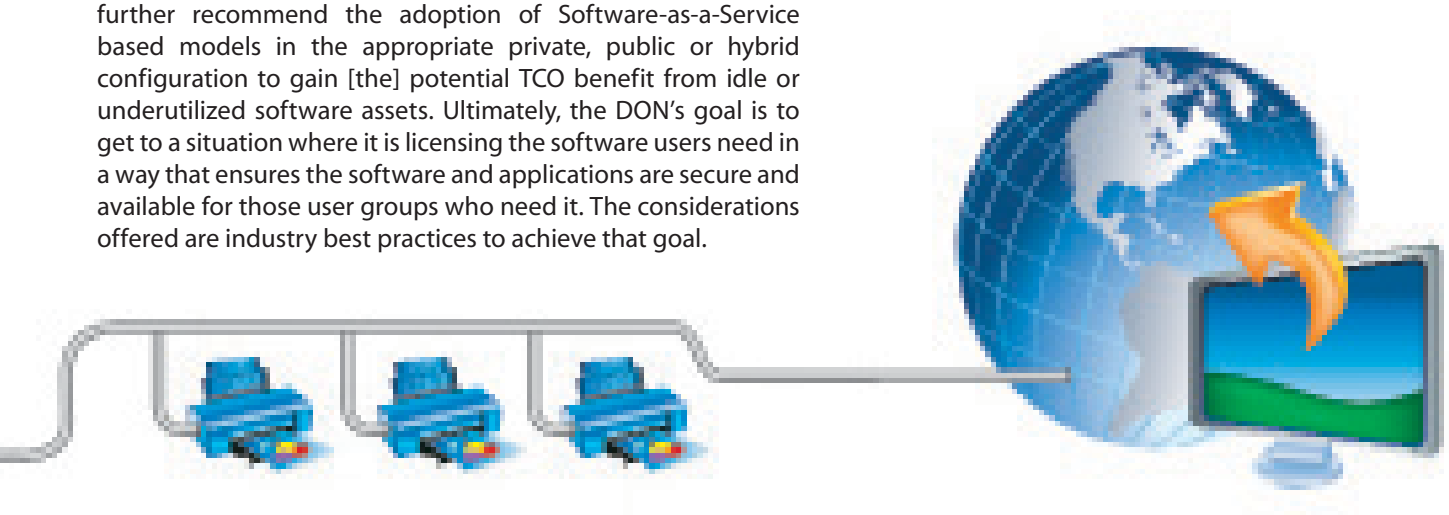
Similar to ESI, HP Enterprise Services manages the licensing and procurement of commercial software at an enterprise level and recognizes the benefits associated with this approach. Additionally, HP Enterprise Services manages its own intellectual property (i.e., software) and offers these types of agreements to its clients globally. HP Enterprise Services recommends the DoD undertake the rationalization of its ESI licenses biased toward eliminating duplicate or underutilized commercial software applications. In alignment with Mr. Halvorsen's stated viewpoint, the adoption of a data and application strategy across the Navy will enable a reduction in the number of licenses it currently has and [can] determine which ESI license is needed and who (what user group) needs it. As discussed, HP Enterprise Services would further recommend the adoption of Software-as-a-Service based models in the appropriate private, public or hybrid configuration to gain [the] potential TCO benefit from idle or underutilized software assets. Ultimately, the DON's goal is to get to a situation where it is licensing the software users need in a way that ensures the software and applications are secure and available for those user groups who need it. The considerations offered are industry best practices to achieve that goal.

MICROSOFT

The optimum way for organizations to own and manage software licenses is with consolidated enterprise agreements acquired and managed at the enterprise level, in this case the Department of the Navy, and used throughout the Navy and Marine Corps by users, commands and program managers. This differs from many of today's practices where license ownership resides within programs, a model that tends to obscure the cost of licenses and creates many divisions of management, which themselves obscure the total picture of license ownership from the organization. This new model of 'enterprise ownership program use' allows government agencies to acquire licenses at the lowest cost by leveraging economies of scale purchasing and receive the most advantage from benefits associated with those licenses. Government agencies then provide licenses to programs as government furnished equipment. This lowers the cost of both license ownership and programs thus creating an asymmetric degree of savings. The benefits are not limited to license cost. With fewer transacting entities, workforce costs are also lowered. And finally, enterprise-wide license agreements allow government agencies to project costs and growth over the FYDP (Future Years Defense Program) and POM (Program Objective Memorandum) cycle to ensure the resources are in place to meet requirements and programs solutions.

ORACLE

Oracle's approach to our customers is similar to how we manage internally. We have the ability to engineer a solution that will complement the requirements of most organizations. There are a number of licensing options that can be considered to reduce software costs while maintaining the technology integrity required by the environment. The structure of a solution can be based on total population, infrastructure components, application segmentation and consolidation. The primary success factor to achieving the cost reductions required is to establish policy and governance on 'what, who, when and where' software will be used. To the extent that can be achieved, a license agreement can be structured to drive cost avoidance, eliminate unauthorized procurements and decrease maintenance costs. As important however, is the ability to enable the enterprise with technology that is current, reliable and agile. CHIPS



Interview with J. Terry Simpson
PEO C4I Principal Deputy for Intelligence

J. Terry Simpson

In his role as the principal deputy for intelligence, Mr. Simpson drives alignment and innovation across the Program Executive Office for Command, Control, Communications, Computers and Intelligence (C4I) portfolio of transformational intelligence, surveillance and reconnaissance (ISR), information operations (IO) and METOC (meteorology and oceanography) capabilities to meet fleet requirements. He partners with the greater Defense Department intelligence community to develop the intelligence workforce and leverages best practices and technology opportunities in support of naval intelligence needs.

Mr. Simpson spoke on the topic of "Cross-Navy Initiatives in Unmanned Systems" with a distinguished panel of experts at the West 2011 conference in San Diego, Calif., Jan. 26. Later that day he spoke at a media roundtable. CHIPS asked Mr. Simpson to follow-up on his responses to reporters in February. He began the discussion with opening remarks.

Simpson: The Chief of Naval Operations has established a vision for the Navy to be prominent and dominant in unmanned systems operating from the sea. This vision encompasses a number of implicit and explicit operational aspects and challenges; it is more than just a vision about new platforms … it represents a good rallying vision for the Navy/Marine Corps team. As we consider this in terms of the Commandant of the Marine Corps, CNO and DoD expectations for the Navy/Marine Corps team to be our nation's force from the sea, bringing our own basing, bringing our own capabilities forward to a conflict, I think it is imperative that we pursue a collaborative, coordinated strategy between the Navy and Marine Corps in the area of unmanned systems.

We have also heard an emphasis from CNO and from Vice Adm. Jack Dorsett (Deputy Chief of Naval Operations for Information Dominance (N2/N6) and Director of Naval Intelligence (DNI)) about a strong partnership with the Air Force in unmanned systems, focused on the Global Hawk and BAMS-D (Broad Area Maritime Surveillance–Demonstrator) platforms, and related joint basing and operational capabilities.

I think there are a number of different areas in which we can smartly collaborate across [the] services as we increase operational deployment of unmanned systems. It is a great thing that DoD leadership [and] our naval military leadership are openly seeking out those opportunities.

Unmanned systems are bringing a shift in capabilities and operational cultures to all the services, and we are discovering that we can collaborate and all benefit in new ways.

In terms of SPAWAR (Space and Naval Warfare Systems Command) and our involvement in unmanned systems, we have engagements both from an engineering standpoint and acquisition standpoint. SPAWAR, and our Systems Centers Pacific and Atlantic organizations, are working a lot of the hard engineering problems for the Navy, the Marine Corps and [the] joint services that relate to integrating unmanned systems capabilities from a C4I standpoint and ISR standpoint.

It is unique among the services that the Navy has such a capable organic engineering capability to solve some of these problems working across program offices and PEOs. That is a big benefit of SPAWAR that we bring to this warfare area [engineering for unmanned systems].

Another is clearly evidenced through the fact that we acquire and provide the infrastructure in terms of communications and networks, plus the processing, exploitation and dissemination (PED) capabilities for the Navy. It is incumbent upon us to ensure that those solutions are scalable and flexible to be able to effectively integrate unmanned systems operations, as well as other platforms. Our infrastructure and PED capabilities should appropriately scale across platforms, and they need to address manned and unmanned systems in the undersea, surface, aviation and space domains.

At PEO C4I, our unmanned systems efforts are predominantly led by PMW 750, our Carrier and Air Integration Program Office. PMW 750 is focused on scaling C4ISR programmatic solutions to address the needs of the air platforms, and on integrating those platforms from a C4ISR standpoint. PMW 750 has been very proactive in working with NAVAIR (Naval Air Systems Command), and in working with the other systems commands, and with the PEOs and program offices at NAVAIR, to address C4I needs, such as communications links, data dissemination and networking requirements, from those platforms.

We have a PMW 750 liaison permanently assigned at NAS Pax (Naval Air Station Patuxent River) to actively work these types of cross-program integration opportunities with NAVAIR. PEO C4I has made it a significant organizational priority to lead these types of partnerships across the Navy/Marine Corps team, and we are very pleased with the real progress made as a result.

Q: What are the top issues with unmanned systems?

A: Taking an information-centric view, the top issue that we see is the need for an adequate network and communications infrastructure, in both the afloat and the ashore environments, to be able to handle the large and dynamic data volume that the proliferation of sensors and platforms are producing. A robust infrastructure is the No. 1 challenge.

Number two is fleshing out the CONOPS (concept of operations) and the tactics,

techniques and procedures of how we want to do business with all these new platforms. In the Navy we have some obvious operational culture shifts to overcome, for example, involving all the equities of traditionally-piloted versus remotely-piloted aircraft. But we also have a very real workforce capacity challenge. We will need to exploit and process huge volumes of data in very short timeframes and with highly focused regional geographic considerations across the globe. How do we man, train and equip a force to handle that … or perhaps we focus on greater automation of processing and exploitation capabilities to alleviate a degree of manpower requirements?

What could/should the role of 10th Fleet be in terms of functional commander responsibilities, working with geographic commanders, and in managing a workforce that is more agile and distributed to tackle dynamic new mission sets driven by new sensor platforms?

In considering the tasking, collection, processing, exploitation and dissemination (TCPED) functions, it is anticipated that we will have a shortfall in the number of skilled analysts to perform these tasks in traditional ways. Notably, one recent TCPED study estimated a future need for over 300 additional intelligence analysts to execute these increased mission functions.

J. Terry Simpson, PEO C4I principal deputy for intelligence, in his office Feb. 28, 2011. Headquartered on the Old Town Campus of the Space and Naval Warfare Systems Command in San Diego, Calif., the mission of the Navy's Program Executive Office for C4I is to provide integrated communication and information technology systems that enable information dominance and the command and control of maritime forces. Photos by Rick Naystatt/SPAWAR A/V specialist.

The technology is one aspect, but we have to be very smart about how we invest in technology capabilities and how we man, train and equip to ensure that we are taking a balanced approach. We cannot continue to invest in sensor platforms without a full plan on how we will exploit and operationalize the data that is produced. Where do we get the manpower for the human piece of the intelligence analysis and exploitation that will be needed?

There is also a technology side of that question: how much can we do through automated processing? We need to push the automation and the information analytics as far out to the tactical edge as possible to reduce the volumes of data that must be moved around.

Q: Have you done analysis between investing more money on the technology side versus the manpower side?

A: There have been some initial analysis efforts to drive a more balanced investment strategy. You can point to the Navy's creation of the Information Dominance Corps, with all of the careful planning behind it, as a manifestation of the fact that we are evolving our workforce strategy to address these types of new mission demands.

"Taking an information-centric view, the top issue that we see is the need for an adequate network and communications infrastructure, in both the afloat and the ashore environments, to be able to handle the large and dynamic data volume that the proliferation of sensors and platforms are producing. A robust infrastructure is the No. 1 challenge."

It's important to note that this is not exclusively an unmanned systems issue; we have to consider all kinds of platforms that carry sensors. If you consider the Navy's ISR Roadmap, we plan to field an array of manned platforms, such as [the] Joint Strike Fighter, P-8s (Poseidons, formerly the Multimission Maritime Aircraft), and others with various sensors, in addition to unmanned systems.

We could envision multiple types of sensors and multiple sensors on each platform whether manned or unmanned.

There are real opportunities for greater levels of integration with the other services and the intelligence community in some of these areas. If we take a strategic approach, perhaps we can find opportunities to leverage, not only infrastructure and systems capabilities, but also analytical capabilities provided by a distributed multi-organizational workforce to support the growing mission demands. We have to think innovatively about a total mission capability spanning the workforce and the systems.

Q: Can you talk about the intelligence products that PEO C4I delivers?

A: PEO C4I's products support the TCPED functions and beyond for the Navy. Intelligence capabilities represent more than just the 'I' in C4I, without the communications, networks, command and control applications, and integrated capability packages that we deliver, the intelligence mission could not be adequately supported.

We deliver critical SATCOM (satellite communications) systems, tactical networks, programs like the Distributed Common Ground System–Navy, and other exploitation and processing systems. Additionally, we deliver capabilities to support multiple types of intelligence areas, such as SIGINT (signals intelligence), IMINT (imagery intelligence) and ACINT (acoustic intelligence).

We absolutely have an end-to-end capability focus, but we often don't have direct responsibility for some of the key

pieces that may comprise an end-to-end capability. For example, other PEOs and systems commands are responsible for particular payloads that might go on an aircraft, or particular sensor systems or flight control stations.

One area in which we do have responsibility for providing sensors and processing capabilities is in the meteorological area. We build sensors and capabilities for METOC requirements, and have responsibility for delivering the systems to collect the data, exploit it, store it and disseminate it via a network infrastructure. Additionally, we deliver the command and control capabilities to make decisions, develop operational and tactical plans, and create situational awareness pictures, including the environmental aspects of the battlespace.

Q: One of your priorities is to improve the networking and communications infrastructure both ashore and afloat. Can you give us some perspective on what needs to be done to avoid the data tipping point?

A: It is not a massive overhaul. We have excellent opportunities to leverage and capitalize on infrastructure investments that are being made within the intel community (IC) and within the DoD via the DISN (Defense Information Systems Network), the GIG (Global Information Grid).

For example, DISA (Defense Information Systems Agency) is pursuing a high capacity 100-gigabit-type network backbone, a cipher text core backbone that could significantly increase our naval C4ISR mission bandwidth capabilities ashore. From a warfighting standpoint, I think we need to look at all options like these to capitalize on other partners' investments. Leadership should continually reassess and adjust where we are going to make sure that we're making the wisest investment decisions all along the way.

The context of my answer was taken from the earlier question on the biggest challenge areas… I point out the critical role of network/communications infrastructure because we are going to see an avalanche of data unlike anything that our current systems were designed to handle.

You have probably heard about the move to data center consolidation within DoD and within [federal] government. The Federal CIO Vivek Kundra and Navy CIOs are pursuing data center consolidation efforts in order to concentrate more capabilities within existing footprints without proliferating brick-and-mortar solutions. It is about how we can integrate and use our global infrastructure more smartly.

However, if we address data center consolidation in such a way that we don't take into account the full warfighting mission requirements of DoD, we are probably still not capitalizing on all the opportunities that may exist. For example, most enterprise data center consolidation efforts are focused on business systems data, personnel data and e-mail systems. These types of data are fairly static in terms of growth and in terms of rate of change or refresh. It is also typically well-structured data.

"If we address data center consolidation in such a way that we don't take into account the full warfighting mission requirements of DoD, we are probably still not capitalizing on all the opportunities that may exist."

Contrastingly, volumes of C4ISR warfighting mission data are exponentially increasing, some structured and some unstructured, typically coming from environments where we don't have a robust network/communications backbone. I believe that we need to take a wider look at our data strategies to ensure we have a full game plan for data management that addresses the DoD's mission data, as well as some of the more traditional structured data that runs the business side of DoD.

The key is realizing that there is no single silver bullet — this will require a multi-pronged approach. We have to do some data reduction and automated processing as far out on the edge as possible. We need smart and adaptive methodologies to manage mission data so we are not shipping the same product back five different ways and storing it 12 different times. It is a complex problem but an exciting one to tackle.

Q: In acquisition terms, I've heard experts say that the longer it takes to field a capability, the less relevant it is to the warfighter. What is the timeline for fielding the capabilities you talked about?

A: It would be ideal to operate within an 18-month cycle, with the capability to accelerate faster. This would pace Moore's Law and provide a hope of pacing the dynamic nature of requirements in this area. In other words, if it takes us longer than 18 months to field the latest and greatest IT capabilities to support fleet requirements, then it begins to become irrelevant.

Within the military, we're still budgeting, acquiring [and] fielding capabilities using industrial age processes that take us anywhere from six to eight years to field IT hardware and software.

"We need smart and adaptive methodologies to manage mission data so we are not shipping the same product back five different ways and storing it 12 different times. It is a complex problem but an exciting one to tackle."

Processes, such as (Navy Modernization Process) NMP/SHIPMAIN, for the Navy make no sense for information-centric cyber capability requirements. The days of huge, generations-long programs are over for the acquisition community and industry in the cyber domain.

We must be able to support the employment of dynamic cyberspace operations, which take us to a predictive, rather than reactive posture, in how we operate and defend our networks, and also to deliver effects-based offensive cyber capabilities that are aligned with our traditional warfighting systems. The pace of cyber warfare threats and rapid advancements in information technology magnify this challenge. CHIPS

Follow SPAWAR on Twitter: http://twitter.com/SPAWARHQ or Facebook: www.facebook.com/spaceandnavalwarfaresystemscommand.

DON Enterprise Architecture: Supporting Effectiveness and Efficiencies

By Victor Ecarma

The Department of the Navy (DON) Enterprise Architecture (EA), with its initial release in July 2009 and version 2.0.000 release in July 2010, continues to support departmental efforts toward effectiveness and efficiency by providing standardized processes, detailed guidance, and a central location for DON EA information. By using the DON EA, program managers can avoid duplication of effort and more quickly produce enterprise architecture solutions for their program.

The DON EA authoritative process will support the initial DON IT/cyberspace efficiency focus areas, cited in the DON CIO memo, "Department of the Navy Information Technology (IT)/ Cyberspace Efficiency Initiatives and Realignment Tasking," of Dec. 20, 2010. These efficiency focus areas support the DoD IT consolidation efforts for IM/IT/cyberspace and Information Resources Management. Future DON EA releases will incorporate key attributes of the efficiency focus areas (e.g., standardized processes and requirements) to support the DON's effectiveness and efficiency implementation efforts.

The DON EA provides an authoritative process for decision makers to assess all Information Technology/National Security Systems (IT/NSS) investments for Global Information Grid mission areas against DON strategic goals and objectives. (The GIG mission areas consist of the Business Mission Area, Enterprise Information Environment Mission Area, Warfighting Mission Area and Defense Intelligence Mission Area.) DON EA links compliance assessments to key DON IT/NSS investment management and review processes, including the DON IM/IT Investment and Annual Review and Title 40/Clinger-Cohen Act (Title 40/CCA) confirmation. As future releases occur, the DON EA will support the system engineering technical review and FORCEnet consolidated compliance checklist processes.

The DON EA contains artifacts ranging from traditional Department of Defense Architecture Framework (DoDAF) viewpoints, such as the Integrated Dictionary, to nontraditional or "fit-for-purpose" artifacts, such as commercial off-the-shelf fielding (COTSF), within the DON artifacts. Traditional DoDAF products and architecture common element lists in the DON EA assist department program managers in the development of solution architectures mandated by the Joint Capabilities Integration and Development System and Defense Acquisition System processes.

These traditional artifacts help minimize the need for solution architects to recreate portions of the enterprise architecture that are not specific to individual programs. Existing laws, regulations, policies and guidance form the basis of other nontraditional DON artifacts, such as the COTSF artifact described above. These "actionable" artifacts, extracted from existing DON policies or strategy, guide the department's IT/ NSS investment toward achieving departmental goals and objectives.

The DON EA compliance and waiver processes provide a transparent mechanism for DON programs to ensure the execution and implementation of existing DON EA policy and strategic goals. In addition, the metrics produced, resulting from the DON EA compliance and waiver process, provide the DON with new insights into the quality, practicality, and successful implementation of existing policy and guidance.

The next scheduled DON EA release is planned for July 2011. Official DON EA releases and updates will be disseminated via Navy messages. DON CIO will make informal announcements about DON EA updates and changes via the Intelink eChirp microblogging tool. DON EA users may subscribe to this tool at https://www.intelink.gov/chirp/group/donea. Authoritative and current information about DON EA policy, procedures, and content is accessible from https://www.intelink.gov/wiki/DONEA. CHIPS

Victor Ecarma supports the DON CIO enterprise architecture and emerging technologies team..

Talking with Capt. Sara A. "Clutch" Joyner

First woman carrier air wing commander

This year the Navy, Marine Corps and Coast Guard celebrate 100 years of naval aviation with a series of events across the country. One hundred years ago carrier flight operations were unimaginable — except to a few visionaries. Today, America's seapower would not be possible without them. From medical evacuations, to search and rescue, to combat, naval pilots have stood tall among America's heroes, including Capt. Sara A. Joyner.

Joyner had just detached from the Office of the Chief of Naval Operations for Warfare Integration (OPNAV N88) as the Joint Strike Fighter requirements officer when she spoke to a Women in Defense group in Norfolk, Va., in January.

As the JSF requirements officer, Joyner was responsible for bringing the next generation of carrier strike aircraft to the fleet. She has been selected as the first woman carrier air wing (CVW) commander "CAG" and will go to CAG-3 as the deputy CAG starting this summer. She reported for duty at the end of January for refresher training.

Joyner doesn't like to emphasize the "firsts" she has achieved as a woman aviator, rather she refers to them as the "fantastic opportunities" that the Navy has provided; opportunities that are available to all who are willing to give their best.

Joyner said she was 11 years old when the U.S. Naval Academy announced that it would be accepting women, and she knew that she wanted to be among the first to graduate. At first, she did not get a lot of encouragement from her father, who was a Naval Academy graduate. "My dad actually said, 'Over my dead body.'" But he was quickly won over when he realized how hard Joyner was willing to work to achieve her dream.

Indeed, Joyner said she didn't want the Navy to reduce its requirements for women to succeed, rather she, and pioneers like her, wanted to exceed the Navy's expectations. She received her commission in 1989 graduating with merit from the Naval Academy with a Bachelor of Science degree in oceanography.

After graduation, Joyner attended flight school and earned her naval aviator wings in July 1991 from VT-24 in Beeville, Texas. In 1994 Joyner reported to Commander Strike Fighter Wing, Pacific in Lemoore, Calif., as assistant operations officer. Joyner has flown the FA/-18 Hornet and Super Hornet; she has served in many capacities, including department head for maintenance, operations and safety.

In January 2002, she reported to U.S. Joint Forces Command in Norfolk, Va., where she served in the current operations branch as force deployment officer for U.S. Northern Command, U.S. European Command and the U.S. Central Command areas of responsibility in support of Operations Enduring and Iraqi Freedom. In March 2007, Joyner assumed command of VFA-105, the "Gunslingers," a Super Hornet Strike Fighter Squadron. On Nov. 2, 2007, she led the Gunslingers on a combat cruise to the Persian Gulf in support of Operation Iraqi Freedom. Under her leadership, the squadron performed more than 1,880 combat missions totaling more than 4,950 flight hours delivering 35,000 pounds of ordnance in support of coalition ground forces in Iraq. Carrier aircraft have provided the majority of close air support in Afghanistan. Super Hornets have sensors that can locate improvised explosive devices or roadside bomb positions.

Joyner calls carrier operations the best example of men and women coming together on equal terms to do a job. "When I was dropping ordnance to defeat IEDs, those on the ground didn't care who was in the plane. They were just glad you were there."

When asked about the Navy's efforts for recruiting a diverse force, Joyner said the Navy has led the other services in offering opportunities, and she looks forward to the day when there are no more "firsts." "I think of what the Navy offers as an equality of opportunities."

Capt. Sara A. Joyner

CHIPS: How important is information technology to the aviation community?

Joyner: It is incredibly important. Every aspect of the Joint Strike Fighter is IT-related; the JSF is a flying sensor. There are antennas and sensors all over the aircraft, all of which have to be integrated, all of which have to process and fuse [data], and that information then needs to be put into the right places so that it is interpreted and put together into a coherent picture for the pilot but also for off-board [processing] as well.

Every aspect of what we are doing in aviation now is IT-related, especially with the newer aircraft. Each generation that we bring in, the demands become higher and higher for your IT capacity, your expertise and your ability to process and work with the information and how you use it. All of those systems have to integrate into our existing equipment that we have onboard so interoperability is huge.

The communications and the ability to integrate with legacy systems are so important for information exchange, and new systems must be integrated with legacy systems.

CHIPS: It is a complex process.

Joyner: One of the systems that we work with in the Hornet is JMPS, which is the Joint Mission Planning System. It is an IT process where we load up a 'memory brick' (we call it a memory card); we take it out to the plane and then we plug it in.

When we get it wrong, the plane does

The Joint Mission Planning System provides an integrated planning capability for aircraft, weapon and sensor missions for both fixed- and rotary-wing aircraft and unmanned aerial vehicles. JMPS is a Windows XP, PC-based solution using COTS and host platform unique mission planning applications.

not do what it is supposed to do, and there are a lot of problems. Any fighter pilot today recognizes that we are in a high technology world where information systems are so important. When JMPS malfunctions we are banging our head against the computer screens trying to fix the problem and bringing in the right people to assist us to make sure that we can handle what is going wrong, and so we can program and have the planes do what they are supposed to do because they are technological machines.

Aircraft are no longer legacy analog systems; computers are part of the plane. Systems that are on the ground are as important as what is in the plane, and they have to work well with each other, and they all have to function coherently.

CHIPS: Can you talk about your role as the Joint Strike Fighter requirements officer?

Joyner: As the requirements officer I represented the CV variant, the carrier variant, which is the F-35C. Part of our requirements is for information exchange and to be able to 'talk' with legacy shipboard systems, and to be interoperable with the rest of the fleet systems, including the other aircraft.

Overall warfighting requirements also include IT and that is part of what I was working with to make sure we get the right capabilities so that when the new plane comes out, the interoperability requirements are met and we don't have a standalone system that is isolated from the other shipboard systems.

CHIPS: Did you bring lessons learned from performing close air support to the job?

Joyner: All of the requirements officers are warfighters from their various platforms. When you are bringing in a new platform you try to get somebody from the most equivalent platform, and I was a Super Hornet pilot flying Lot 28s. Production lots reflect increasing capability so a Lot 28 was a pre-AESA (Active Electronically Scanned Array) radar Super Hornet, but still had a lot of high-tech toys, and it was very technologically advanced.

Super Hornets and JSF will be the two complementary platforms on the 2020 aircraft carrier. My background in Super Hornets gave me a firm foundation for JSF requirements and an understanding of the required missions to include: close air support, air-to-air, suppression of enemy air defenses — all of the missions including those that require working with the troops on the ground.

The need to be able to go in different warfare environments against different types of threats — and the threat awareness — all of that comes from the job that you do. That was my qualification coming through the door. Most recently, air-to-ground is mainly what we have been doing in theater, but there is always a requirement to maintain air-to-air skills as well.

CHIPS: What other qualifications do you need?

Joyner: It is an essential balance. We require an understanding of the budget process combined with warfighting experience. We learn the budget aspect of the requirements billet, but we come through the door with operational experience. Within the naval service we combine budget with requirements so we know when we say this platform has to do a specific mission or have a specific capability that we have to make it fit in a budget 'box' which I think is service unique to the Navy.

I don't think the other services do that. I think that is very powerful because it makes us question whether we are getting every requirement correct. It is a Navy-unique approach to requirements planning. None of us are budget experts, but we have a good understanding of what we are given and how well we need to optimize within our budgetary limits. It puts constraints on us.

It's the difference between going to the store with an open credit card that is not yours vice walking in with a debit card that has a specific balance that you cannot exceed. You have a better understanding

ATLANTIC OCEAN (March 24, 2007) – Commanding Officer Cmdr. Sara Joyner of Strike Fighter Squadron (VFA-105), puts on her gloves while dressing out in full flight gear before flight operations aboard Nimitz-class aircraft carrier USS Harry S. Truman (CVN 75). Joyner is the first female commanding officer of a fighter squadron. Truman is underway conducting Tailored Ship's Training Availability (TSTA), a standard used to evaluate a ship's readiness for deployment. U.S. Navy photo by Seaman Kevin T. Murray Jr.

[of the] limitations placed on your wish list so that you can appropriately prioritize your warfighting requirements.

CHIPS: Will you have to qualify when you go back to the carrier?

Joyner: I will, and I will be training for the next six months in order to refresh my flying skills. I am trying to get tactical again. I am looking forward to the first day I take off, and I look out of the side of the windscreen and I see that LAU. The LAU is located on the tip of [the] Hornet wings out of the canopy and carries [the] AIM-9 (Sidewinder). It is very visible from the cockpit, and I am lucky enough to fly more than one TMS (type/model/series). I am going to fly legacy Hornet, the Super Hornet, and I hope the Growler a little bit as well.

Then I get to be 'guest pilot' with the E2 (Hawkeye) and the helos. It is really a great job. It is a fantastic opportunity.

F-35C Lightning II Joint Strike Fighter

The Joint Strike Fighter program is building a tri-service family of next-generation strike fighter aircraft that is flexible and survivable. With its all-aspect stealth strike design, internal weapon carriage, fully fused mission systems, and unrefueled combat radius of approximately 650 nautical miles, the Navy's F-35C Lightning II will complement the capabilities of the F/A-18E/F Super Hornet now serving as the Navy's premier strike fighter. The F-35C will enhance the flexibility, power projection and strike capabilities of carrier air wings and joint task forces. Initial operational capability for the F-35C Lightning II is late fiscal year 2014. The F-35 Lightning II Program is in the test phase.

NAVAL AIR STATION PATUXENT RIVER, Md. (Feb. 11, 2011) The U.S. Navy variant of the F-35 Joint Strike Fighter, the F-35C, conducts a test flight over the Chesapeake Bay. Lt. Cmdr. Eric "Magic" Buus flew the F-35C for two hours, checking instruments that will measure structural loads on the airframe during flight maneuvers. The F-35C is distinct from the F-35A and F-35B variants with larger wing surfaces and reinforced landing gear for greater control when operating in the demanding carrier take-off and landing environment. U.S. Navy photo courtesy of Lockheed Martin.

My job as CAG is to direct all aviation from the carrier, but also to lead from the front and be involved with what the squadrons are doing and to understand what the squadrons need. I will have great skippers, COs of the squadrons, working for me, the best staff ever, all hand-picked professionals.

CHIPS: What did your dad say after you graduated from the Naval Academy?

Joyner: I did him a disservice by only mentioning his initial reaction to my wanting to attend the Naval Academy. He is deceased now, but he was my No.1 fan. He thought it was going to be too rough of an environment for his daughter, and he did not want me to have a rough time because he knew it was not going to be easy. My dad wanted me to join the Coast Guard. He said you can be in command of a ship as a young person. But he was very proud of me and got to see me go out on my first deployment.

CHIPS: Do you consider mentoring junior officers part of your job?

Joyner: Yes, absolutely. I am on a mentorship website for the Navy. It is very difficult to find mentors of the same gender, so a lot of us turn to men that are willing to step in, and there is a lot of value in that as well. I am involved in women mentorship groups because we have unique needs that come up in childcare, marriage and pregnancy. There are a lot of issues that men don't have to deal with, and you need advocates that understand.

I will be honest, a lot of the women quit because they just don't see a way ahead, and they don't know how to get where they want to go. They look at it and say, 'This is insurmountable, and I just can't get there.' Some of what the mentorship program does is we take away those barriers by saying, 'Here's a way you could and here's another way, and if this doesn't work…'

There are plenty of great moms out there, who were fighter pilots, who couldn't see a way to get around that or just thought that their families were so important that they did not want to give up on that and that's OK too. Being a mom is a hard job too, and being a parent is the most important job in the world since you are basically safeguarding our country's future. Doing it all doesn't always work out for men or women, and sometimes we are forced to prioritize.

CHIPS: What made you persevere against the odds?

Joyner: Family support. My husband [Cmdr. James Joyner] is fantastic. Because we are both fighter pilots, we have an understanding of what the other is doing. Without him I wouldn't be here; there is no doubt. There is not a single decision we made that wasn't done as a family where we discuss it and figure out 'OK, how do we do this to make this work?'

What I tell women that I mentor is don't look too far ahead; don't plan how you are going to be the CO when you are a lieutenant. Instead, plan how you are going to get to the next step because if you look too far ahead, it looks too hard. Don't listen to bad advice.

CHIPS: What kind of bad advice?

Joyner: There are plenty of people who will say don't have a family; you won't be able to do it. Don't listen to the don'ts and the can'ts. Just do the best you can, and if it is not working, or if it is so painful that it's not worth it, then give up. But if you never try, you will never succeed. Don't give up in advance; get to the point where you know you have tried your best.

CHIPS: What have been your most satisfying accomplishments?

Joyner: Overall, the most satisfying event has to have been the opportunity to take a finely honed Hornet squadron to sea on a combat cruise and then bringing them all safely home again. I can't think of a greater opportunity.

All of my career milestones required doors to be opened just in the nick of time and individuals having faith in my ability to succeed.

My initial warfare transition and people believing that I could be a Hornet driver required a leap of faith by leadership in Lemoore back in 1995 when things weren't going all that well for women training in combat aircraft. The support of my peers and leaders has allowed me to be where I am today. CHIPS

Editor's Note: Cmdr. Scott "Intake" Kartvedt is now the requirements officer (OPNAV N88) for the Navy's F-35C. CVW-3 consists of Strike Fighter Squadrons VFA-32, VFA-37, VFA-105 and VMFA-312; Tactical Electronics Warfare Squadron VAQ-130; Carrier Airborne Early Warning Squadron VAW-126; and Helicopter Anti-Submarine Squadron HS-7. For information about the Centennial of Naval Aviation go to www.public.navy.mil/airfor/centennial.

Section 508 of the Rehabilitation Act: *What You Need to Know*

By Sherrian Finneran

Section 508: Why Comply?

It's the law! Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998, requires federal departments and agencies to ensure that electronic and information technology (E&IT) ***developed, procured, maintained, or used*** provides: (1) individuals with disabilities, who are federal employees, comparable access to and use of information and data that is available to federal employees who are not individuals with disabilities; and (2) individuals with disabilities, who are members of the public seeking information or services, to have comparable access to and use of information and data by such members of the public who are not individuals with disabilities. Comparable access is not required if it would impose an undue burden on the department or agency. National Security Systems that comply with the definition in section 5142 of the Clinger-Cohen Act of 1996 are exempt from Section 508 requirements.

It's the Right Thing to Do

Consider these statistics from the U.S. Census Bureau regarding people with disabilities:

- 29 million (10 percent of the population) are deaf or hearing impaired.
- 11.4 million people have visual conditions not correctable by eyeglasses.
- 6.4 million new cases of eye disease occur each year.
- 2.8 million people are visually handicapped from color blindness.
- 1.1 million people are legally blind.

Website Accessibility

Section 508 requires that all website content be equally accessible to people with disabilities. This applies to Web applications and Web pages and all attached files. It applies to intranet, as well as public-facing Web pages. Websites must comply with U.S. Access Board Standard 1194.22 for Web-based intranet and Internet information and applications. In an effort to ensure that Department of Defense websites meet minimum requirements, the office of the DoD Deputy CIO conducts quarterly reviews of DoD component websites. Results are shared with component Section 508 coordinators and website administrators.

Procurement Oversight

The General Services Administration (GSA) is randomly sampling E&IT solicitations posted on FedBizOpps.gov to assess the extent to which solicitations properly consider Section 508 standards. After the assessment, GSA will send an e-mail to the originating agency explaining how the selected solicitation was assessed. Quarterly summaries of the findings are sent to the Office of Management and Budget. Federal Acquisition Regulation (FAR) Part 39, Acquisition of Information Technology, subpart 39.201, states that Section 508 must be addressed in all solicitations to purchase E&IT. The FAR requires agencies to acquire accessible E&IT unless an exception applies, in which case the requiring official must provide documentation to the contracting officer for inclusion in the contract file.

Buy Accessible Wizard

The Buy Accessible Wizard is a tool developed by the GSA to help construct Section 508 standard-compliant requirements and solicitations for E&IT products and services. Additionally, the tool can help you determine whether Section 508 applies to your purchase, and it can even write the solicitation language for you. The Buy Accessible Wizard leads you through a step-by-step process to document compliance with Section 508 standards effectively, consistently and efficiently. The data summary report produced using the wizard serves as a compliance audit trail documenting decisions made concerning relevance, applicability, market research and exceptions as a demonstration of due diligence for compliance. Additional information on the Buy Accessible Wizard is available at www.buyaccessible.gov.

Computer/Electronic Accommodations Program

The Computer/Electronic Accommodations Program (CAP) (www.tricare.osd.mil/cap/), in the office of the Assistant Secretary of Defense for Health Affairs, was established to eliminate employment barriers for people with disabilities. CAP helps by providing assistive technology and services at no cost to the agency. To assist with Section 508 compliance, CAP provides:

- Technical assistance to all DoD and partner organizations;
- Demonstrations of assistive technology and accessible environments at the CAP Technology Evaluation Center (CAPTEC); and
- Assistance to office automation organizations to ensure help desk personnel understand accessibility requirements and compatibility issues.

Section 508 is not only the law; it is the right thing to do. Taking care of our people is a Department of the Navy priority. Compliance with Section 508 also ensures equal access for the DON's workforce, whose needs may change over time, and new hires, including those who may come from the Wounded Warrior Program. It is important that all DON personnel do their part in keeping the department's electronic information equally accessible to all. CHIPS

Sherrian Finneran is the DON Section 508 coordinator.

References

In 1986, Congress added Section 508 to the Rehabilitation Act of 1973. Section 508 established non-binding guidelines for information technology accessibility. On Aug. 7, 1998, the president signed into law the Workforce Investment Act of 1998 (P.L. 105-220) that included the Rehabilitation Act Amendments of 1998. These amendments significantly expanded and strengthened the IT accessibility requirements in Section 508, and made them binding for federal agencies.

In the Federal Register of Dec. 21, 2000, the Architectural and Transportation Barriers Compliance Board (Access Board) published the Electronic and Information Technology (E&IT) Accessibility Standards; final rule (36 CFR Part 1194). These standards became effective June 21, 2001.

In the Federal Register of April 25, 2001, the Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council published a final rule amending the Federal Acquisition Regulation (FAR), Electronic and Information Technology Accessibility (48 CFR, Chapter 1, Parts 2, 7, 10, 11, 12 and 39). These regulations became effective June 25, 2001.

Finding Cyber/IT Workforce Management & Training Efficiencies: The Fundamentals of Workforce Planning

By Mary Purdy

On a daily basis, Mr. Chris Kelsall, director of the Department of the Navy Chief Information Officer (DON CIO) Cyber/IT workforce management team, collaborates with federal and Department of Defense organizations to develop policies and initiatives to ensure the DON Cyber/IT workforce is supported and provided resources to enhance professional development. However, when the situation requires strategic review to effect change, the DON CIO has traditionally brought together subject matter experts to define and shape the enterprise transition.

In 1998, the DON CIO brought together Echelon I and II organizations to determine the totality of the IM/IT workforce and develop the first IM/IT Workforce Strategic Plan. In 2001, a DON CIO-sponsored workforce integrated process team (IPT) defined the process for civilians to transition to the Navy Marine Corps Intranet contractor workforce. In 2005, the DON CIO stood up the information assurance (IA) workforce working group to develop new processes and procedures for the implementation of the IA Workforce Improvement Program (WIP).

Now in response to tasking by the Under Secretary of the Navy and the subsequent DON CIO memo "DON IT/Cyberspace Efficiency Initiatives and Realignment Tasking" of Dec. 20, 2010, the DON IT/Cyberspace workforce and training integrated product team was established. This IPT will streamline current and planned Cyber/IT workforce management and training initiatives.

Mapping to the Strategic Plan: The DON CIO released the "DON Cyber/IT Workforce Strategic Plan FY 2010-FY 2013" in July 2010. (Visit: www.doncio.navy.mil/Products.aspx?ID=1839.) The strategic plan establishes the DON's priorities for workforce excellence by identifying the goals and objectives that will allow the department to recruit, manage, develop, sustain and retain a talented workforce. Looking to the future to determine how the department needs to adapt, improve and find efficiencies, the recently established IPT will use the strategic plan as a cornerstone of its consolidation endeavors.

Cyber/IT Workforce Scope: The key areas of the cyberspace workforce are: offensive operations, defensive operations, information assurance, and operations and maintenance. This also includes the cyber law enforcement and counterintelligence community.

For the purposes of this IPT, the DON Cyber/IT workforce is defined as the military (active and Reserve components) and government civilians who:

- Are engaged in provisioning, operating, maintaining and defending classified, unclassified and proprietary systems and networks owned/operated by the Department of the Navy;
- Provide the workforce capabilities required to plan, budget, manipulate, control and archive information throughout its life cycle;
- Develop, acquire, implement, evaluate, maintain and retire information, information systems and IT, and the technology required to transmit friendly and influence adversary information and information systems; and
- Develop the policies and procedures required to manage and apply warfighting measures, policies and procedures to effectively optimize information, information systems and networks.

Enterprise Collaboration: It is envisioned that the IT/Cyberspace workforce and training IPT will facilitate department-wide collaboration to improve enterprise policy, processes and tools that shape the DON's future Cyber/IT workforce. As the IPT endeavors to provide options for improving workforce and training effectiveness and efficiency, it will also strive to bring discipline to workforce management, providing resource funding justification through a valid "as is" and "to be" manpower foundation. Three critical elements are:

1. Cyber/IT Workforce and Training Management: This includes those activities necessary to develop and maintain the Cyber/IT workforce baseline (work, roles, structure and manpower) to support workforce management, planning and programming. It also includes activities supporting training implementation.

Areas the IPT will review:

- DON Cyber/IT Learning Management Solution; and
- DON Cyber/IT Workforce Chief Learning Officer (CLO) Organization.

2. Information Assurance Workforce: This includes those actions necessary to improve IA workforce training, certification and qualification, with specific emphasis on IA and operating system certification percentages, sustainment of current certifications, continuing education, and IA WIP oversight.

Areas the IPT will review:

- DON Cyber Range ; and
- DON Cybersecurity/IA Workforce Efficiencies.

3. IT/Cyberspace Community Management: This includes actions taken to develop and maintain a closer relationship between DON, Navy and Marine Corps leadership and community managers (military and civilian) to provide an enterprise view of the total force to enhance leadership decisions regarding makeup, staffing and risk management.

Area the IPT will review:

- DON Cyber/IT Community Manager Community of Practice (COP).

Strategic and Tactical Wins: The IPT will address key aspects of workforce management business processes in an enterprise manner. IPT subgroups have been established and have looked at both short- and long-term goals. Initial strategic topic areas for consideration are initiatives that will require additional research or collaboration to conduct a valid business case analysis.

Strategic Areas include:

- DON Cyber/IT Learning Management Solution;
- DON Cyber/IT Workforce CLO Organization; and
- DON Cyber/IT Civilian Community Manager COP.

The IPT is prepared to address key areas and identify near-term "tactical wins" that support the improvement of the effectiveness and efficiency of the DON Cyber/IT workforce and training efforts. Tactical wins include initiatives that were addressed previously or need to be addressed out of fiscal necessity that have sufficient background information and maturity such that if the actions recommended are undertaken a tangible result can be achieved in the near term. As an example, the IA Workforce Improvement Program exists with known challenges and possible efficiencies.

Tactical wins include:

- DON Cyber Range;
- DON Cybersecurity/IA Workforce Efficiencies;
- Training Support Agent (Navy); and
- DON Librarian.

The Cyber/IT workforce faces the challenge of expanding its cyber capabilities. Operating in and defending cyberspace affects both the department's inherent cyber warfare mission, as well as the other warfare domains. It is critical to define clear consistent workforce management, education and training objectives that will enhance the Cyber/IT professionals' ability to carry out their multitude of responsibilities. The IPT will find effective and efficient best practices so that every member of the Cyber/IT workforce engages in continuing professional education to stay ahead of and adapt to the flurry of technical advances. CHIPS

Mary Purdy provides support to the DON CIO Cyber/IT workforce team.

Ballistic Missile Tracking Exercise Using ARAV-B

By Naval Surface Warfare Center, Port Hueneme Division Public Affairs

Naval Surface Warfare Center, Port Hueneme Division (NSWC PHD) White Sands Detachment supported a successful tracking exercise at the NASA Wallops Flight Facility in Virginia, Jan. 22, 2011. The test was part of exercise Atlantic Trident 2011.

The Aegis Readiness Assessment Vehicle (ARAV), a short-range ballistic missile target, was used in the exercise. All three Navy ships involved in the test event, USS Monterey (CG 61), USS Ramage (DDG 61) and USS Gonzalez (DDG 66), successfully tracked the ARAV-B, also known as Terrier-Oriole. The three ships were able to provide simulated target solutions that would have resulted in a successful intercept.

The ARAV, a product of the NSWC PHD White Sands Detachment, is a solid-fuel rocket-based target vehicle that emulates ballistic missile threats. It is a target system that saves money — approximately 85 percent in cost savings compared to other ballistic missile targets. NSWC PHD's efforts, as well as the efforts of the entire Aegis BMD team, were recognized by Rear Adm. Joseph A. Horn, Jr., program executive for Aegis Ballistic Missile Defense, and Rear Adm. John Clark Orzalli, vice commander of Naval Sea Systems Command.

Monterey, an Aegis cruiser, and Ramage, an Aegis destroyer, took turns tracking and simulating engagement of the target while Gonzalez, a guided-missile destroyer, tracked the target. No live missiles were fired from the ships, and the target ARAV fell harmlessly into the Atlantic Ocean.

Ballistic missile defense is a Navy core mission. The Missile Defense Agency and the Navy modified 21 Aegis BMD combatants (five cruisers and 16 destroyers). Of the 21 ships, 16 are assigned to the Pacific Fleet and five to the Atlantic Fleet. The Secretary of Defense announced in 2010 that six more destroyers would be upgraded to the Aegis BMD capability. Atlantic Trident 2011 is the first live fleet BMD exercise to take place in the Atlantic. CHIPS

Above: The ARAV-B (Terrier-Oriole) ballistic missile target is launched from NASA Goddard Space Flight Center's Wallops Flight Facility Jan. 22, 2011, as part of a tracking exercise.

The Diffusion of Innovation

By Lt. Daniel W. Berger

Most individuals evaluate an innovation, not on the basis of scientific research by experts, but through the subjective evaluations of near peers who have adopted the innovation.

Have you ever wondered why some inventions take the world by storm, such as the iPhone and smart phone technology, while others seem to fail, lie dormant for decades, but when their time has come, their use grows quickly, even explosively, like the fax machine did.

Most inventions achieve slow infiltration at first, and then their adoption grows more quickly, but later slows down again. This process of adoption is called the "Diffusion of Innovation." It is a broad social theory that assesses the psychological and sociological patterns of adoption, explains the mechanism of adoption, and assists in predicting whether and how a new invention will be successful within a population.

The first diffusion theory was developed in the early 1950s, and the theory continues to be widely used. In 1962 Everett M. Rogers proposed four main elements that influence the spread of a new idea: the innovation, communication channels, time and a social system. This article summarizes Rogers' Diffusion of Innovations theory. My purpose is to help us improve how we design, implement, operate and maintain future technology.

Diffusion Theory

Diffusion is the process by which an innovation is communicated through channels over time among the members of a social system. Diffusion is a special type of communication concerned with the spread of messages that are perceived as new ideas. An innovation is an idea, practice or object that is perceived as new by an individual or other unit of adoption. The characteristics of an innovation, as perceived by the members of a social system, determine its rate of adoption. The four main elements in the diffusion of new ideas are: (1) the innovation; (2) communication channels; (3) time; and (4) the social system or context.

Why do certain innovations spread more quickly than others? For the innovation to spread and be adopted it should contain the following five perceived attributes. These attributes play key roles in determining the rate of adoption: (1) relative advantage; (2) compatibility; (3) complexity; (4) trialability; and (5) the ability of people within the social system to observe the innovation.

Communication is the process by which participants create and share information with one another to reach a mutual understanding. A communication channel is the means by which messages pass from one individual to another. Mass media channels are more effective in creating knowledge about innovations, whereas interpersonal channels are more effective in forming and changing attitudes toward a new idea, and thus in influencing the decision to adopt or reject a new idea. Most individuals evaluate an innovation, not on the basis of scientific research by experts, but through the subjective evaluations of near peers who have adopted the innovation.

The time dimension is involved in diffusion in three ways. First, time is involved in the innovation decision process. The innovation decision process is the mental process through which an individual (or other decision making unit) passes from initial knowledge of an innovation to forming an opinion about the innovation, to a decision to adopt or reject, to implementation of the new idea, and then to confirmation of the decision.

An individual seeks information at various stages in the innovation decision process to decrease uncertainty about an innovation's expected consequences. The five-step process includes:

- Knowledge – person becomes aware of an innovation and has some idea of how it functions;
- Persuasion – person forms a favorable or unfavorable attitude toward the innovation;
- Decision – person engages in activities that lead to a choice to adopt or reject the innovation;
- Implementation – person puts an innovation into use; and
- Confirmation – person evaluates the results of an innovation decision already made.

The second way in which time is involved in diffusion is in the innovativeness of an individual or other unit of adoption. Innovativeness is the degree to which an individual or other unit of adoption is relatively earlier in adopting new ideas than other members of a social system. There are five adopter categories or classifications of the members of a social system based on their rate of innovativeness.

The third way in which time is involved in diffusion is in rate of adoption. The rate of adoption is the relative speed with which an innovation is adopted by members of a social system. The rate of adoption is usually measured as the number of members of the system that adopt the innovation in a given time period. (See Figure 1.) Members and their composition in the social system consist of:

- Innovators – 2.5 percent;
- Early adopters – 13.5 percent;
- Early majority – 34 percent;
- Late majority – 34 percent; and
- Laggards – 16 percent.

The fourth main element in the diffusion of new ideas is the social system. A social system is defined as a set of interrelated units that are engaged in joint problem solving to accomplish a common goal. The members or units of a social system may be individuals, informal groups, organizations, and/or subsystems. The social system constitutes a boundary within which an innovation diffuses.

A second area of research involves how norms affect diffusion. Norms are the established behavior patterns for the members of a social system. A third area of research has to do with opinion leadership, the degree to which an individual is able to informally influence other individuals' attitudes or overt behavior in a desired way with relative frequency.

Another component of the social system is the change agent who attempts to influence the other members' innovation

Successful innovation is a key contributor to organizational success. Understanding how new ideas are adopted in an organization can help leaders implement change. However, what it means to innovate successfully and how to build organizational processes that facilitate more effective innovation are complex issues. An organization can adopt too few innovations — fewer than its needs and capabilities would suggest — or adopt too many at one time.

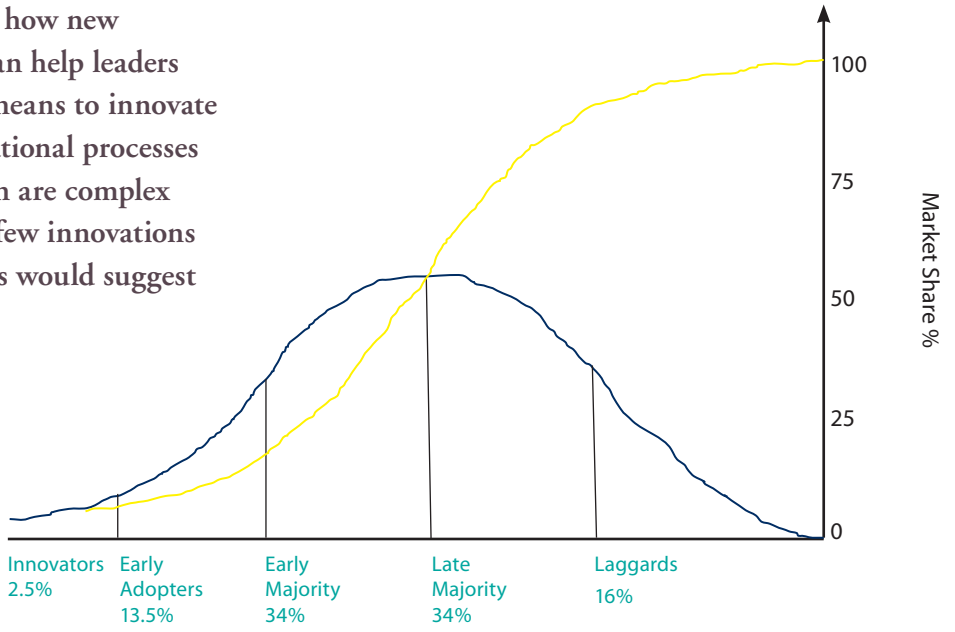


Figure 1. The diffusion of innovations according to Rogers (1962). With successive groups of consumers adopting new technology, or other innovative changes (shown in blue), its market share (yellow) will eventually reach the saturation level.

decisions in a direction that is deemed desirable by a change agency.

A final crucial concept in understanding the nature of the diffusion process is the critical mass that occurs at the point at which enough individuals have adopted an innovation so that the innovation's further rate of adoption becomes self-sustaining.

The concept of the critical mass implies that outreach activities should be concentrated on pushing the use of the innovation to the point of critical mass. These efforts should be focused on the early adopters; the 13.5 percent of the individuals in the system to adopt an innovation after the innovators have introduced the new idea into the system. Early adopters are often opinion leaders and serve as role models for many other members of the social system. Early adopters are also instrumental in getting an innovation to the point of critical mass, and hence, in the successful diffusion of an innovation.

Characteristics of an Innovation

Relative advantage describes the degree to which an innovation is perceived as better than the idea it supersedes. The degree of relative advantage may be measured in economic terms, but social prestige, convenience and satisfaction are also important factors.

It does not matter so much if an innovation has a great deal of objective advantage. What does matter is whether an individual perceives the innovation as advantageous. The greater the perceived relative advantage of an innovation, the more rapid its rate of adoption will be.

Compatibility is the degree to which an innovation is perceived as consistent with the existing values, past experiences and needs of potential adopters. An idea that is incompatible with the values and norms of a social system will not be adopted as rapidly as an innovation that is compatible. The adoption of an incompatible innovation often requires the prior adoption of a new value system, which is a relatively slow process.

Complexity is the degree to which an innovation is perceived as difficult to understand and use. Some innovations are readily understood by most members of a social system; others are more complicated and will be adopted more slowly. New ideas that are simpler to understand are adopted more rapidly than innovations that require the adopter to develop new skills and understanding.

Trialability explains the degree to which an innovation may be experimented with on a limited basis. New ideas that can be tried on the "installment plan" will generally be adopted more quickly than innovations that are not divisible. An innovation that is able to be given a trial period represents less uncertainty to the individual who is considering it for adoption, and who can learn by doing.

Observability represents the degree to which the results of an innovation are visible to others. The easier it is for individuals to see the positive results of an innovation, the more likely they are to adopt it. Such visibility stimulates peer discussion of a new idea because friends, neighbors or coworkers of the adopters often seek information.

The Adoption of an Innovation

Innovators are the first 2.5 percent of the individuals in a system to adopt an innovation. Innovators can be compared to "techies" who must have the latest and greatest IT device — no matter whether they need it or not. Embracing new technology or a new idea is almost an obsession with innovators. This interest in new ideas leads them out of a local circle of peer networks and into more cosmopolite social relationships. Communication patterns and friendships among a clique of innovators are common, even though the geographical distance between the innovators may be considerable.

Being an innovator has several prerequisites. Control of substantial financial resources is helpful to absorb the possible loss from an unprofitable innovation. The ability to understand and apply complex technical knowledge is also needed. The innovator must also be able to cope with a high degree of uncertainty about an innovation at the time of adoption.

While an innovator may not be respected by the other members of a

social system, the innovator plays an important role in the diffusion process by launching the new idea into the system, importing the innovation from outside of the system's boundaries. Thus, the innovator plays a gatekeeping role in the flow of new ideas into a system.

Early adopters are the next 13.5 percent of individuals in a system to adopt an innovation. Early adopters are a more integrated part of the local system than innovators. Whereas innovators are cosmopolites, early adopters represent localities. This adopter category, more than any other, has the greatest degree of opinion leadership in most systems.

Potential adopters look to early adopters for advice and information about the innovation. This adopter category is generally sought by change agents as local messengers for speeding the diffusion process. Because early adopters are not too far ahead of the average individual in accepting innovativeness, they serve as role models for many other members of the social system.

Early adopters are respected by peers and are the embodiment of successful, discrete use of new ideas. Early adopters know that to continue to earn the esteem of colleagues, and to maintain a central position in the communication networks of the system, they must make judicious innovation decisions. Early adopters decrease uncertainty about a new idea by adopting it, and then conveying a subjective evaluation of the innovation to near peers through interpersonal networks.

The early majority is the next 34 percent of the individuals in a system to adopt an innovation. The early majority adopts new ideas just before the average members of a system. The early majority interacts frequently with peers, but members of the early majority seldom hold positions of opinion leadership in a system.

The early majority's unique position between the very early and the relatively late to adopt makes this category of adopters an important link in the diffusion process. Early majority members provide interconnectedness in the system's interpersonal networks. Early majority members include one of the two most numerous adopter categories, making up one-third of the members of a system. The early majority may deliberate for some time before completely adopting a new idea. "Be not the first by which the new is tried, nor the last to lay the old aside," fits the thinking of the early majority. This group follows with deliberate willingness in adopting innovations, but seldom leads.

The late majority is the next 34 percent of individuals in a system to adopt an innovation. The late majority adopts new ideas just after the average members of a system. Like the early majority, the late majority makes up one-third of the members of a system. Late majority adoption may be the result of increasing network pressure from peers.

It does not matter so much if an innovation has a great deal of objective advantage. What does matter is whether an individual perceives the innovation as advantageous. The greater the perceived relative advantage of an innovation, the more rapid its rate of adoption will be.

For the late majority, innovations are approached with a skeptical and cautious approach. They do not adopt until most others in their system have done so. The weight of system norms must definitely favor an innovation before the late majority is convinced, and the pressure from peers is necessary to motivate adoption. The relatively scarce resources of the late majority mean that most of the uncertainty about a new idea must be removed before the late majority will think that it is safe to adopt.

Laggards are the last 16 percent of the individuals in a system to adopt an innovation. They possess almost no opinion leadership. Laggards are the most localized in their outlook of all adopter categories; many are near isolates in the social networks of their system.

The point of reference for the laggard is the past. Decisions are often made in terms of what has been done previously. Laggards tend to be suspicious of innovations and change agents. Resistance to innovations on the part of laggards may be entirely rational from the laggards' viewpoint because their resources are limited, and they must be certain that a new idea will not fail before they will adopt.

Exploring Organizational Theories

Successful innovation is a key contributor to organizational success. Understanding how new ideas are adopted in an organization can help leaders implement change. However, what it means to innovate successfully, and how to build organizational processes that facilitate more effective innovation, are complex issues.

An organization can adopt too few innovations — fewer than its needs and capabilities would suggest — or adopt too many at one time. Organizations can adopt the wrong innovations, ones that do not provide significant advantages given an organization's particular situation.

An organization can adopt the right innovations but at the wrong time; so soon that the costs and risks of adoption exceed the likely payoff, or so late that the competition has already gained a competitive advantage.

Organizations can adopt the right innovations at the right time but fail to implement them in a way that nets benefits. Fortunately, our understanding of the processes of innovation diffusion has grown considerably since information technology researchers first became interested in this area.

As researchers have considered the many distinctive characteristics of IT innovations and their adoption, there has been a corresponding effort to develop more sophisticated models that go beyond traditional approaches to incorporate the effects of institutions, knowledge barriers, increasing returns, adaptive structuration and social bandwagons. A rich opportunity exists to explore and validate these promising streams and synthesize them into more complex and realistic models of IT innovation diffusion. CHIPS

Lt. Daniel W. Berger is an Information Professional officer and Project Management Professional (PMP) who works in the consolidated maintenance department of Naval Computer and Telecommunications Area Master Station Pacific, Wahiawa, Hawaii. The basis of Berger's article is from the Diffusion of Innovations, 4th edition, Simon & Schuster Inc., 1995.

The Collaborative Community: Improving Marine Corps IT Health

By Pete Gillis

Ever had a problem and thought, "I'm not the first person to have this problem; someone must have the answer?" If you're like me, it happens pretty often, and it got me thinking. It has been written that the average knowledge worker generates 2 to 3 gigabytes of information annually. How much of that information can help in your work? How much of your 2 to 3 GB of data could help others? Collaboration and information sharing are necessary pillars for building a true community of professionals. By communicating through a variety of methods and platforms, we can help one another solve our problems and increase the value we provide to the enterprise.

Since 1990, the ability to collaborate and share information has changed radically. In the 1990s, your ability to collaborate was limited. An organization presented not just an administrative boundary, but also an informational one because you only had a telephone, and basic e-mail in some cases, for communication. You interacted only with people you knew, and that usually meant seniors, peers and subordinates within your organization. You had a computer, and you stored any content you created on your hard drive. Any value you generated (ideas, documents, etc.) was realized at the organizational level. As the Internet increased in popularity and reach, this paradigm started to change.

Information now flows across organizational boundaries. People you don't know are instantly accessible through blogs and discussion boards. Content that you create can be uploaded to SharePoint, posted on YouTube, and shared with others. Most importantly, there is the potential to realize the value you generate across the enterprise. Today's technology enables us to break down the barriers to information sharing and improve our "information health," a term the CIO Executive Board defines as the quality, trustworthiness, timeliness and ease of access to information.

In the Marine Corps information technology community, we want to realize value across the enterprise by improving our information health. How do we get there? I believe there are three environmental factors that influence this process. First, we have an occupationally diverse community. We have the information technology management series (2210), telecommunications personnel (0391), computer engineers (0854) and scientists (1550), computer operators (0332) and technicians (0335), as well as librarians, library technicians and the technical information services series (1412).

The wide array of occupations means a wide array of information and knowledge is generated. Some of this information will be series specific, but what remains to be determined is how much of that knowledge can transcend series boundaries. For example, DON librarians, who are part of the 1412 series, could be breaking new ground in information management. However, because we are not sharing knowledge across series boundaries, their expertise may be benefitting just a small slice of the Marine Corps community. In addition to a wide array of occupations, we have a geographically diverse community. From Okinawa to Europe, civilian IT professionals are individually generating 2 GB of information. This abundance of information was a barrier to improving information health. But today's technology allows a computer operator at Marine Corps Air Station Iwakuni, Japan, to get an answer to a question from an IT specialist in Pensacola, Fla.

The Marine Corps IT community is certainly not the only stakeholder (or potential stakeholder) in our information health or in the methods we will use to improve it. Other stakeholders might include Marine Corps organizations, such as Manpower and Reserve Affairs, Training and Education Command, or other Marine Corps communities of interest. Indeed, the list may include audiences external to the Marine Corps. As we move forward, we will want to carefully consider the effects of these environmental factors and leverage any strengths we identify.

The Marine Corps IT community is targeting a number of platforms to increase information health. First, we are increasing the size of our access list to the community's SharePoint site. By the end of this year, we hope to give virtually all community members access. Further, we need to better leverage the existing capabilities that SharePoint offers. Second, our public-facing website (www.marines.mil/unit/hqmc/c4/itmcoi) will transfer to the Armed Forces Public Information Management System by this summer. The migration will allow us to completely update the format and page structure. Once the migration is complete, we will overhaul the content. Third, we debuted our community Facebook page (search for "Information Technology Management Community of Interest") and our Twitter account (http://twitter.com/USMC_ITMCOI) in January 2011. These platforms give us vehicles to pass information and also to engage in two-way dialogue. Finally, we're going to expand our presence on milSuite, the U.S. Army-sponsored collection of online tools that promotes workforce collaboration and secure information-sharing behind the Department of Defense firewall. MilSuite (https://www.milsuite.mil/) provides an array of tools that can facilitate knowledge sharing.

The Marine Corps IT community will reap tremendous benefits from improving our information health. In a fiscally restrictive environment, we need to be looking for ways to get more value from our resources. If we create an environment of information and knowledge sharing, we can save the time required to solve our problems, and time is money. Leveraging the technology at our disposal, we can break down barriers to information sharing and realize value at the enterprise level. In the future, this will be critical to maintaining a vibrant community and being "information healthy." CHIPS

Pete Gillis is the community manager for the Marine Corps information technology management community of interest. Mr. Gillis works for the command, control, communications and computers department (C4), Headquarters Marine Corps.

Follow the USMC ITM COI on Facebook at "Information Technology Management Community of Interest" (www.facebook.com/usmc.itm.coi).

Navy Center for Advanced Modeling and Simulation

A one-of-a-kind center for the Navy uniquely suited to design the force multipliers of synthetic training and testing in support of fleet readiness, exercises and wargaming, as well as concept generation and experimentation

By Holly Quick

Navy Warfare Development Command (NWDC) is the Navy's champion for the rapid generation and development of game-changing innovations in concepts and doctrine to enhance maritime capability at the operational level enabling seamless integration in the joint and coalition arena.

Among NWDC's many capabilities is the Navy Center for Advanced Modeling and Simulation (NCAMS) operated by NWDC's modeling and simulation (M&S) directorate. The directorate conducts state-of-the-art, high-fidelity modeling and simulation that enables the Navy's end-to-end training continuum, supports concept generation and development, executes key fleet exercises, and provides high-end, analytical wargaming and experimentation.

"NCAMS is the most sophisticated modeling and simulation development lab in the Navy," said M&S deputy director Darrel Morben, and he proved it with a tour of the remarkable 10,000 square-foot facility in February for CHIPS staff. Morben led the CHIPS staff to each component of the lab while explaining how an event unfolds.

NCAMS is not only where the capacity and bandwidth of the network are actively monitored, but also where the "synthetic battlespace" is generated. Behaviorally realistic platforms, such as tanks, ships and aircraft, operate inside real-time integrated environmental effects supported by authoritative Navy databases to model realistic conditions.

NCAMS Components

Exercise control is the operational heart for synthetic events supported by NCAMS. The elevated platform located in the center of the lab is where the control director supervises the simulation as the control group, manning workstations, monitors the event, documenting actions and decisions for later review by the analysis group. The "sim" operators at workstations on the main lab floor control the virtual entities that populate the synthetic battlespace while liaison officers generate the voice communication to stimulate the exercise or experiment sometimes over a 13-hour shift. Events can last several days or even weeks.

In the engineering bay, software engineers create the core simulation, and network engineers develop and test new methods to transport the simulation and command, control, communications, computers, and intelligence (C4I), to dispersed geographic locations. Interface engineers integrate the simulation with each partnering system or unit; weapons and C4I systems engineers connect and stimulate onboard systems; and control engineers reduce the variables and increase the reliability of the simulation.

The concentration of modeling and simulation and engineering innovation is rooted in the realities of warfighter needs, gaps and challenges. Much of the success of NCAMS can be credited to the flexibility of the engineers, according to Morben. "The engineers resolve technical issues or process issues on the fly — that makes the event come together."

NCAMS Infrastructure

NWDC operates a robust high-speed, switched IP network that provides reliable bandwidth 24/7. The network includes NWDC's Navy Continuous Training Environment (NCTE) and Navy's Joint Semi-Automated Forces (JSAF).

Designed and maintained by the NWDC modeling and simulation directorate, NCTE is a global network infrastructure and integrated communications enterprise. NCTE provides a complete simulation environment of the entirety of war, meaning the complete battlespace with all the dynamic systems, physical models and environmental factors, as well as everyone operating inside it.

NWDC is the program manager for JSAF, a simulation system that generates entity-level simulations that interact individually in a synthetic environment. Individual entities include infantrymen, tanks, ships, aircraft, munitions, buildings and sensors that can be controlled separately or organized into appropriate units for a given mission.

Simulated events are sponsored by many organizations, including the Chief of Naval Operations, U.S. Fleet Forces Command, Office of Naval Research, Office of the Secretary of Defense and combatant commanders, as well as from within NWDC for concept experimentation and validation of concepts under development. Many of these events are joint in nature involving the other services. Coalition forces can also participate once they have been integrated into NCTE. The NCTE has the capability to support multiple events simultaneously. For example, Navy vessels at piers around the globe tie into the network that delivers modeling and simulation data to stimulate the combat and C4I systems on board. Sailors get better training because they train at their workstations, and they can respond to more realistic threats, according to Morben.

"Sailors *are* getting better training through the use of distributed M&S. For example, in ballistic missile defense training, we can provide a realistic simulation of the threat, so modeling and simulation is very important to BMD training."

Sometimes in an experiment or exercise, something unexpected can occur, but Morben said that's OK. "It's good because we are using ships' systems during the exercise, and you will have the same kinds of equipment failures in the real world. It could be a maintenance issue or problem with comms gear."

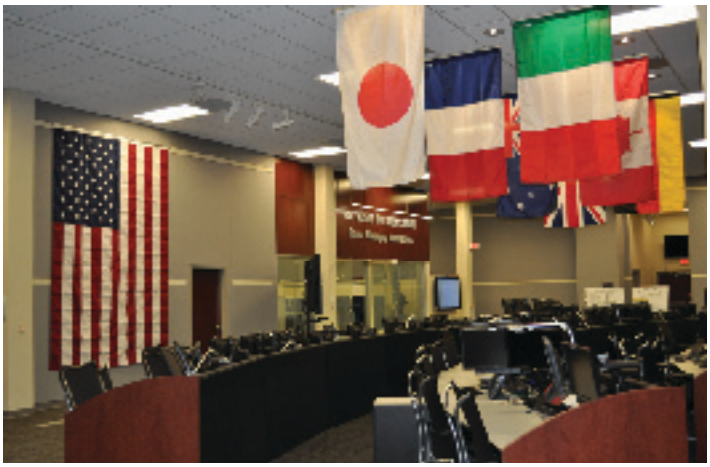
Flight simulators and other federated training devices using the NCTE simulation architecture can also connect into the virtual environment and participate in an event. In addition to providing the network connectivity and integration services, the NCTE also provides the tools that training commands use to generate the synthetic scenario, including the rich

level of environmental detail necessary to properly stimulate all signal gear and monitoring equipment.

The NCTE network delivers real-time voice and command and control among distributed participants even though units may actually be on different sides of the world.

While NCAMS may be hosting one event, other training sites may also be using the NCTE network to distribute synthetic events at the same time. NCTE is not only the largest and most reliable simulation network in the world, but at any given time, it may be supporting multiple training, exercises, experimentation, wargaming or concept development events. The infrastructure extends to all fleet concentration areas on both coasts and the Pacific Rim, all operational naval air stations with air simulators, and connection to an expanding number of coalition forces, represented by the many national flags suspended from the ceiling in the facility. NCTE also partners with the Joint Training and Experimentation Network to distribute simulation to participating locations of the other services and joint forces. "NCTE and JTEN enable real-time battle simulation aboard ships and with joint (Air Force and Army training simulators) and coalition partners," Morben said.

Aboard Norfolk Naval Station, NWDC Commander Rear Adm. Wendi Carpenter poses with NCAMS staff Feb. 4 — just before Super Bowl Sunday. Front row, from left, Doug Sutherland, Capt. Treci Dimas, Todd Morgan, Victoria Arthur, Jack Surroche, Mark Hess. Directly behind Carpenter, Darrel Morben, Tom Reitmeyer and Jay Kocan. Back row, Joel McElhannon, Kelly Leighton and Matt Labarge.



Suspended from the ceiling of the NCAMS lab are the national flags of the expanding number of coalition forces connecting with NCAMS infrastructure. Photos by Holly Quick/ SPAWARSYSCEN Atlantic.

The Simulations

There are many different types of simulation exercises, in addition to strategic engagement scenarios, such as humanitarian relief, search and rescue operations, and resupply. Experimentation and concept generation can include new or hypothetical systems prior to acquisition, as well as examination and analysis of new operational schemes of maneuver.

The NCTE uses combinations of three forms of simulation in the exercises and experiments it distributes: live, virtual and constructive. Live simulations involve real people using real systems, typically on a range, to simulate other real systems. An example of a live simulation is a U.S. Navy submarine playing the role of an enemy submarine.

Virtual simulations involve real people using simulated systems, such as a cockpit simulator, instead of real equipment. Constructive simulations involve simulated ships, aircraft and other units controlled by simulation operators, who act behind the scenes to stimulate the training audience — without controlling the outcome of the event. The combination of the forms of simulation enables the focus to be on "man-in-the-loop" decision making with the NCTE simulating the battlespace and stimulating onboard combat and C4I systems so that console operators can report information to officers making warfighting decisions. These actions are then populated across the NCTE to all other participants, thus expanding the man-in-the-loop involvement beyond the individual unit and across the entire integrated joint warfighting team.

With a diminishing defense budget, synthetic training and experimentation are important, according to Morben. "When we began to do modeling and simulation it was in addition to live training, but because of the quality and confidence that planners and decision makers have in the modeling and simulation, we see an increase. Modeling and simulation can insert a level of complexity and multiple events that cannot be duplicated in live training. Cost avoidance is also important. A 2008 CNA (Center for Naval Analyses) study estimated the annual cost savings of simulation training in hundreds of millions of dollars."

It takes at least six months and often, the directorate has a year, to build a complex event, Morben said. "We need the time to build the concept and architecture which includes the network, simulation and software. We build what we call a MSEL, master scenario event list based on training objectives. For more routine events, the timelines are much shorter."

The value and operational relevance of NCTE is exemplified by the full calendar of events occurring year-round since 1998 in support of fleet readiness and experimentation demands. "The requests for exercises and experiments are increasing with more than 350 synthetic events planned for NCTE next year," Morben said. CHIPS

Holly Quick is a contributor to CHIPS and supports the public affairs office of SPAWARSYSCEN Atlantic. For more information about NWDC, go to http://www.navy.mil/local/nwdc/.

USS Enterprise SHF Cross-Connect Configuration Increases Allocated Bandwidth by 100 Percent

By Cmdr. Eric Johnson

To maximize total allowable bandwidth for deployment, USS Enterprise Strike Group staff, in collaboration with the flagship communications department, conducted the first-ever satellite system cross-connect test with Europe Central Region Network Operations Center (ECRNOC). The proof of concept test was conducted to demonstrate Enterprise's ability to cross-connect Internet Protocol services with another network operations center (NOC) outside the continental United States.

USS Enterprise (CVN 65) had been cross-connecting the Defense Satellite Communications System (DSCS) and Commercial Broadband Satellite Program (CBSP) data paths with the Unified Atlantic Region Network Operations Center (UARNOC) in Norfolk, Va., as standard operating procedure during its workup cycle.

However, this is not standard procedure in 5th or 6th Fleet, and no aircraft carrier using the Automated Digital Network System (ADNS) Increment IIA (also known as ADNS-J) had attempted to cross-connect satellite services in either area of operation. After successfully testing the concept using the NOC in 6th Fleet, Enterprise became the first to cross-connect in 5th Fleet, cross-connecting with the Indian Ocean Region Network Operations Center (IORNOC).

Limitations of ADNS-J

ADNS Inc IIA ships, like the Enterprise and other aircraft carriers and amphibious warfare ships (LHA/LHD), similarly equipped with super high frequency (SHF) satellite communications AN/WSC-6(V)5, or (V)7 terminals capable of supporting dual DSCS data paths, have experienced bandwidth limitations resulting from the inability of the systems to dynamically load balance or dynamically allocate bandwidth.

However, over the last two years, Second Fleet ships have been cross-connecting DSCS and CBSP data paths in an effort to maximize bandwidth running over traditional CBSP paths. Although this doesn't provide load balancing or solve the problem that ADNS Inc IIA ships experience when given two DSCS leases for IP services, it does provide a means to use the two DSCS leases independently in a cross-connection configuration, or use a combined DSCS and CBSP lease to more effectively manage bandwidth.

For argument's sake, let's say an East Coast carrier operating in Second Fleet can get two DSCS leases at 2.048 megabits per second (Mbps) of throughput each and one CBSP lease at 1.024 Mbps of throughput. Once deployed, the same carrier might expect 4.096 Mbps of throughput on each of the three leases. Assuming ADNS-J allowed load balancing across the two DSCS data paths, we would have more than twice the aggregate bandwidth we had in the continental United States: 5.120 Mbps (4.096 Mbps DSCS + 1.024 Mbps CBSP) versus 12.288 Mbps (8.192 Mbps DSCS + 4.096 Mbps CBSP).

Unfortunately for Enterprise and other ADNS Inc IIA ships, dynamic bandwidth allocation across multiple paths (load balancing) is not possible because ADNS-J was not engineered to support load balancing in its current configuration. It wasn't until ADNS Inc III (ADNS-K) was deployed that ships were able to take advantage of aggregating multiple satellite leases into an effective bandwidth management plan based on operational requirements.

Consequently, in 5th Fleet we would not see an aggregate throughput of 8.192 Mbps of bandwidth on DSCS, but instead only 4.096 Mbps because the second DSCS lease is nothing more than a backup. This is where the benefit of cross-connecting DSCS and CBSP pays dividends because the services that traditionally transverse CBSP are overutilized, while services that transverse DSCS are underutilized.

Cross-Connect to Increase Bandwidth

By cross-connecting incoming DSCS and CBSP connections prior to transmission through the ADNS router (see Figure 1) and configuring the router at the servicing NOC, ships can experience upward of 100 percent or more in bandwidth increase or rate of data transfer, especially if they can negotiate a single DSCS lease at a higher bandwidth, instead of two leases at lower data rates. This makes a lot of sense for Enterprise and other ADNS limited Inc IIA ships, considering the second DSCS lease is essentially unused.

It is important to note that ADNS Inc IIA ships are not capable of processing two DSCS leases simultaneously, thereby sharing the aggregate bandwidth. They can, however, use one as a backup or configure them in an upload/download configuration. This configuration describes a lease that sends data while the second lease is used to receive data.

Cross-Connecting Aboard USS Enterprise

Enterprise was fresh out of the shipyard, preparing for its first at-sea period in nearly two years, when the approved (and slightly modified) satellite access request from Second Fleet was received. Second Fleet had provided Enterprise with two DSCS leases (capable of transmitting 2.048 Mbps of data) but no CBSP services. This IP services arrangement was out of the ordinary, considering an aircraft carrier would normally get at least one commercial lease at data transmission rates of 1.024 Mbps. No CBSP? How could the strike group N6 staff and the ship communicators possibly provide quality of life services and other operational products for the ship's crew?

That's when Mike Coleman, from fleet communications at Second Fleet, told the staff about the work Naval Computer and Telecommunications Area Master Station Atlantic (NCTAMS LANT) had been doing with cross-connecting DSCS and CBSP paths to ensure ships received traditional services provided by both satellite systems at the maximum allowable bandwidth.

As it turns out, the first cross-connect proof of concept test was conducted aboard USS Iwo Jima (LHD 7) with the UARNOC in 2007 by Commander, Amphibious Squadron 4's fleet systems engi-

neering team (FSET) support contractors, Allen Knapp and Matthew Klym, who are currently assigned to the Enterprise Strike Group staff. With their initiative, a little shore-side configuration help from NCTAMS LANT, and some creative satellite resourcing from Second Fleet's fleet resources department, the cross-connect concept quickly turned into a standard operating procedure on the East Coast in late 2008 and paved the way for how ADNS Inc IIA ships, like USS Enterprise, can more efficiently manage bandwidth.

As a result, we were able to use both DSCS leases independently to provide IP services and effectively increase traditional CBSP bandwidth throughput by 100 percent to 2.048 Mbps — an increase from the traditional 1.024 Mbps rate.

For Enterprise's second underway period, the ship was given a single 2.048 Mbps data transmission CBSP lease and a single 3.072 Mbps data transmission DSCS lease. Again, we were able to cross-connect DSCS and CBSP to maximize bandwidth that would normally transverse the CBSP path, effectively achieving a 200 percent increase in bandwidth.

Benefits of Cross Connecting

The real advantage of cross-connecting occurs with DSCS leases providing more bandwidth than typical leases for deployed units in 5th and 6th Fleets. In the Second Fleet area of operations, satellite leases provide less bandwidth, and the availability of commercial leases decreases because bandwidth is allocated among the many ships homeported on the East Coast.

Aircraft carriers and L-class ships can usually get a single commercial lease; however, as the Navy moves toward less expensive X-band services, the C-band leases will naturally decrease. As a result, ADNS Inc IIA ships will be forced to meet operational commitments with only a single satellite system, DSCS, to support all shipboard IP services. Consequently, communicators onboard ADNS Inc IIA ships will need to have the knowledge and ability to cross-connect two DSCS data paths to maintain the same aggregate bandwidth.

Enterprise has been cross-connecting DSCS and CBSP services for the past year and has continued the process to maximize bandwidth during deployment. Instead of a single CBSP lease at 4.096 Mbps throughput and dual DSCS leases at 4.096 Mbps, Enterprise was able to leverage a successful test with ECRNOC into a single CBSP lease (4.096 Mbps) and a single DSCS lease (initially 6.144 Mbps and later 8.192 Mbps) depending on our mission set as Commander Task Force 50 or Commander Task Group 50.1.

During dual carrier operations in 5th Fleet, the carrier tasked with duties as CTF 50 is responsible for Operation New Dawn, the follow-on to Operation Iraqi Freedom (OIF) in the Arabian Gulf. Commander Task Group 50.1, consequently reports to CTF 50 and assumes responsibility for Operation Enduring Freedom (OEF), supporting combat operations in Afghanistan.

Both carriers have antipiracy missions supporting 5th Fleet operations in the Gulf of Aden, Arabian Sea and Gulf of Oman. Under this two-carrier construct, CTF 50 is allocated more satellite resources as the "senior" carrier, than CTG 50.1.

The net benefit for Enterprise was a 50 to 100 percent increase in bandwidth rate running over traditional CBSP paths compared to traditional 5th Fleet allocations.

In the end, this was a significant quality of life improvement for Enterprise and its Sailors. Equally significant, was the improvement for the warfighter and operations because we increased and more efficiently used the total aggregate bandwidth available. In the future, cross-connecting DSCS and CBSP will benefit other ADNS Inc IIA ships deploying to 5th and 6th Fleets by providing a means to more efficiently and effectively use allocated bandwidth. CHIPS

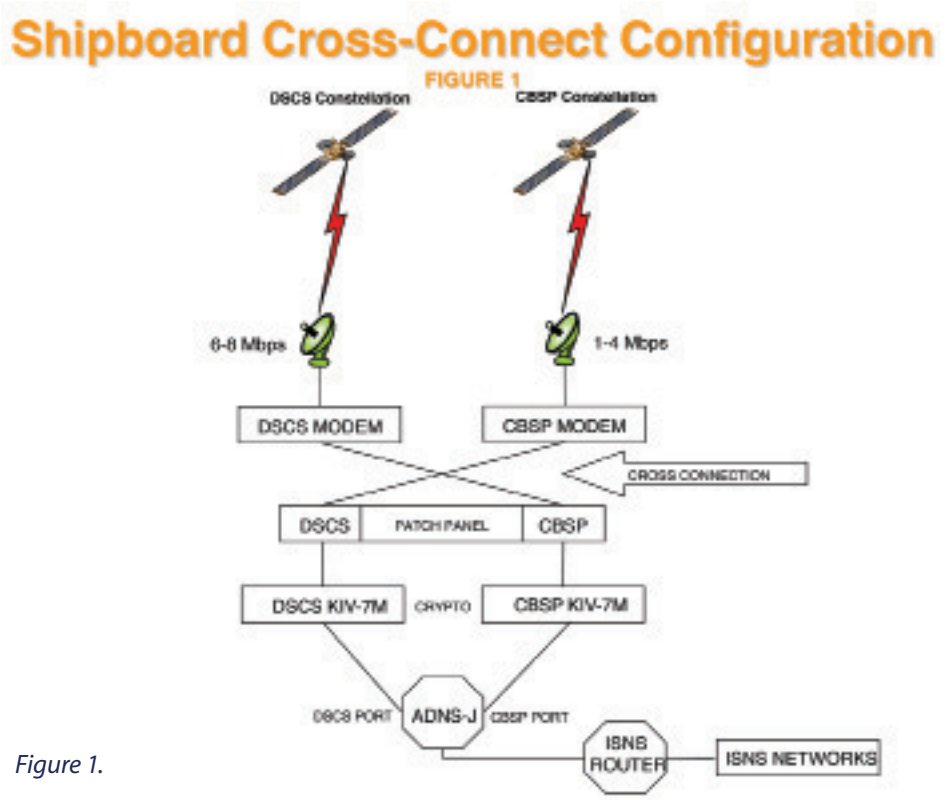


Figure 1.

By cross-connecting incoming Defense Satellite Communications System (DSCS) and Commercial Broadband Satellite Program (CBSP) connections prior to transmission through the Automated Digital Network System (ADNS) router and configuring the router at the servicing network operations center (NOC), ships can experience upward of 100 percent or more in bandwidth increase or rate of data transfer, especially if they can negotiate a single DSCS lease at a higher bandwidth, instead of two leases at lower data rates. The KIV-7 is a National Security Agency Type-1, single-channel encryptor. KIV-7M speeds up to 50 Mbps and supports the High Assurance Internet Protocol Interoperability Specification (HAIPIS).

Cmdr. Eric Johnson is an Information Professional officer currently serving as the deputy N6 assigned to Commander Strike Group Twelve staff aboard USS Enterprise. Johnson will report to NCTAMS PAC as the chief staff officer in June.

Contractor Improperly Handles PII

By Steve Muck

The following is a recently reported personally identifiable information data breach involving a Department of the Navy (DON) support contractor who improperly handled PII. Incidents such as this will be reported in each CHIPS magazine to increase PII awareness. Names have been changed or omitted but details are factual and based on reports sent to the DON Chief Information Officer (CIO) Privacy Office.

The Incident

A contractor working on a contractor-owned and operated information technology (IT) system sent an e-mail to 10 recipients, including four government personnel and six contractors, with an attached list of unique Social Security numbers from the IT system to be used for testing and further processing. The list did not contain data elements that could uniquely link the SSNs to individuals. The recipients did not have a "need to know" and the sender had never completed the annual PII training course. The e-mail was not digitally signed and did not carry the "For Official Use Only (FOUO)" privacy warning.

The IT system was registered in the Department of Defense IT Portfolio Repository-Department of the Navy (DITPR-DON), had an approved privacy impact assessment (PIA), and accurately reflected that it collected PII.

Actions Taken

Approximately two hours after the e-mail was sent, a DON recipient sent an e-mail asking the nine other recipients to delete the e-mail immediately, purge file copies, and reply with an e-mail confirmation. The DON CIO Privacy Office was contacted a short time after the action was taken.

The DON CIO Privacy Office advised that an SSN by itself may or may not constitute a high risk breach when context becomes the determining factor. In this case, the SSNs were contained in a Microsoft Excel file, there was one SSN without the dashes per data cell, and there was no other information contained within the file. Therefore, the SSNs could not be linked to an individual. Accordingly, the DON CIO determined that notifications to the personnel whose SSNs were e-mailed were not required.

While this breach was considered low risk to affected personnel, it could easily have been determined to be high risk if there had been a linkage between the SSN and a person's name. CHIPS

Steve Muck is the DON CIO privacy team lead.

Lessons Learned

- DON support contractors who handle PII must receive annual PII training.
- DON support contractors must comply with all privacy protections under the Privacy Act when handling PII.
- Contractor-owned or maintained IT systems under contract to the DON must be registered in the DITPR-DON.
- There are many IT systems that are contractor owned or operated, and contracts between the commercial vendor and the DON must contain two specific contract clauses from Federal Acquisition Regulation (FAR) 52.224-2 as noted on the next page.

Additional Lessons Learned

- Real/live PII data should never be used to test or evaluate a new or altered IT system.
- PII should only be disclosed to those who have a need to know in the performance of their official duties.
- Managers and supervisors must review PII processes and procedures to ensure they are complying with DON privacy policy. They must ensure that a PII compliance spot check is completed twice yearly as required by DON policy.
- All electronic or paper copy documents and attachments containing PII must be marked with the following: FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE: Any misuse or unauthorized disclosure of this information may result in both criminal and civil penalties. Refer to Secretary of the Navy (SECNAV) Instruction 5211.5E.
- E-mails containing PII must be digitally signed.
- E-mails containing 25 or more PII records must be encrypted using WinZip or another authorized DON enterprise solution. Refer to DON CIO message DTG 171952Z APR 07: "Safeguarding Personally Identifiable Information."
- PII collected and/or disseminated in separate data calls may not be PII, but when combined with other data elements becomes PII, such as using SSNs in one data call and names in a separate data call. Put together, data calls containing privacy data may result in a PII breach.

52.224 - 1 - Privacy Act Notification

The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation may involve the imposition of criminal penalties.

52.224 - 2 - Privacy Act

(a) The Contractor agrees to –

(1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies

(i) The systems of records; and

(ii) The design, development, or operation work that the contractor is to perform;

(2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and

(3) Include this clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.

(b) In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor and any employee of the Contractor is considered to be an employee of the agency.

(c) For Systems of Record

(1) "Operation of a system of records," as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.

(2) "Record," as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.

(3) "System of records on individuals," as used in this clause, means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

DON CIO Discusses Future IT Initiatives

SAN DIEGO, Calif. (Jan. 26, 2011) Terry Halvorsen speaking at the Cyber/IT Workforce Town Hall in a question and answer period with workforce members.

Recordings and transcripts of three sessions hosted by the Department of the Navy Chief Information Officer, Terry Halvorsen, during the West Coast DON Information Technology Conference, are now available. The sessions include: the Cyber/IT Workforce Town Hall, the DON IT Way Ahead Discussion, and the Functional Area Managers/Command Information Officers session. During the town hall and way ahead discussion, Halvorsen and members of the leadership team discussed the role of the DON CIO and what they believe are their key priorities and challenges.

During the FAM/Command CIO session, discussion centered on the functional area managers and the application rationalization process, specifically its challenges and future steps.

The DON CIO has received feedback from department personnel on the value of the information provided. If you couldn't travel to the DON IT Conference, you can still learn about important initiatives and be a participant in the ongoing discussion.

The East Coast DON IT Conference will be at the Virginia Beach Convention Center, Virginia Beach, Va., May 10-12, 2011. You can register for the conference at www.doncio.navy.mil/contentview.aspx?id=2101. CHIPS

Recordings

Cyber/IT Workforce Town Hall: www.doncio.navy.mil/uploads/TownHall.mp3 (Encoding: MP3; size: 35 MB; duration: 1 hour, 27 minutes).

DON IT Way Ahead Discussion: www.doncio.navy.mil/uploads/ITWayAhead.mp3 (Encoding: MP3; size: 27.5 MB; duration: 1 hour, 8 minutes).

Functional Area Managers/Command Information Officers session: www.doncio.navy.mil/uploads/FAM_CIODiscussion.mp3. (Encoding: MP3; size: 19.1 MB; duration: 47 minutes).

Transcripts

Town Hall PDF: www.doncio.navy.mil/Download.aspx?AttachID=1441 (78 KB).

DON IT Way Ahead Discussion PDF: www.doncio.navy.mil/Download.aspx?AttachID=1442 (73 KB).

FAM/CIO Discussion PDF: www.doncio.navy.mil/Download.aspx?AttachID=1443 (61 KB).

SPAWARSYSCEN Atlantic provides capability driven, sustainable voice engineering solutions

By Nick Werner

Mission-essential, real-time secure voice and data communications are a critical element of the Navy's command, control, communications, computers and intelligence (C4I) infrastructure; voice communication is the most fundamental element of tactical and operational communications used by warfighters.

Space and Naval Warfare Systems Center (SPAWARSYSCEN) Atlantic voice systems integrated product team's (IPT) mission is to ensure information superiority through the use of encryption, authentication and access control technologies to protect information traversing Navy voice circuits, whether tactical (radio broadcast) or strategic (telephone).

The IPT is sponsored by the Information Assurance and Cyber Security Program Office (PMW 130), Tactical Networks Program Office (PMW 160) and Shore and Expeditionary Integration Program Office (PMW 790), with its Navy Defense Red Switch Network (DRSN) sub-portfolio sponsored by Navy Cyber Forces and U.S. Air Forces Central Command.

The team's voice engineering laboratory, located in Portsmouth, Va., is the Navy's only dedicated secure voice lab. The state-of-the-art facility is ideally located, only minutes from U.S. Fleet Forces Command, Naval Computer and Telecommunications Area Master Station Atlantic, Norfolk Naval Shipyard, Huntington Ingalls Industries Inc. in Newport News, Va. (formerly Northrop Grumman Shipbuilding), and other fleet assets in Hampton Roads.

The voice systems IPT's efforts span a number of interrelated but distinctly different technologies that together represent the continuum of naval voice communications support, encompassing legacy and modernized secure and non-secure voice, as well as selected secure data services over voice networks.

The team's initiatives are divided into several major efforts and initiatives meant to enable or support similar core capabilities despite the obstacles inherent in the Navy's somewhat ad hoc, but rapidly evolving communications infrastructure.

PORTSMOUTH, Va. (Dec. 16, 2010) During a tour of the voice engineering lab, Kevin Thompson, the unified capabilities sub-IPT lead, explains the functions of the lab to Chris Miller, SPAWARSYSCEN Atlantic technical director. Jim Farley, the voice systems lead looks on. The lab is the Navy's only dedicated secure voice facility. Photo by Joe Bullinger/ SPAWARSYSCEN Atlantic.

Direct Fleet Support

The voice systems IPT leverages its favorable proximity and specialized resources to provide the means to rapidly resolve fleet voice communications issues. As the Navy's secure voice In-Service Engineering Activity (ISEA) and the voice element of the Automated Digital Network System (ADNS), the team responds to a wide variety of trouble calls, ranging from radio voice broadcasting to Internet Protocol (IP)-based network voice shortfalls.

On-site technical assistance can often be provided within an hour for local issues. Distant troubleshooting efforts often start by leveraging the fully operational lab assets, which in many instances enable virtually instant remote troubleshooting for voice applications and their associated networks, worldwide and at a moment's notice.

The secure voice team also maintains a cadre of on call, highly qualified Secure Communications Interoperability Protocol-Interworking Function (SCIP-IWF) experts immediately available for global 24/7 service, 365 days a year. SCIP is a multinational standard for secure voice and data communication.

Verify and Validate

Another vital function of the voice systems IPT is its role as the Navy's lead verification and validation activity for secure voice-related engineering changes. The rapid and often simultaneous introduction of updated computer software, new networking technologies, and changes to operations and policies can affect real-time services, such as voice and video teleconferencing, in unexpected ways.

The fully operational voice engineering lab is used to capture and evaluate these changes prior to fielding. The voice systems IPT conducts formal testing to validate the viability of the proposed changes from a voice perspective, verify expected performance and demonstrate that existing communications interoperability is not unduly affected. The test results often form the core of technical summaries that are used to help build consensus and shape informed discussion across the diverse field of naval voice stakeholders.

Cryptographic Modernization

The voice systems IPT is responsible for ensuring that the Navy's secure voice (current and long-term) interests are protected in the face of rapidly evolving joint technologies. These efforts are especially evident in the Navy's partnership with the U.S. Air Force-led acquisition of modernized radio cryptographic replacement devices necessary to support updated National Security Agency encryption algorithms. VINSON/Advanced Narrowband Digital Voice Terminal (ANDVT) Cryptographic Modernization (VACM) replacement devices are destined to

Space and Naval Warfare Systems Center Atlantic voice systems integrated product team's mission is to ensure information superiority through the use of encryption, authentication and access control technologies to protect information traversing Navy voice circuits, whether tactical (radio broadcast) or strategic (telephone).

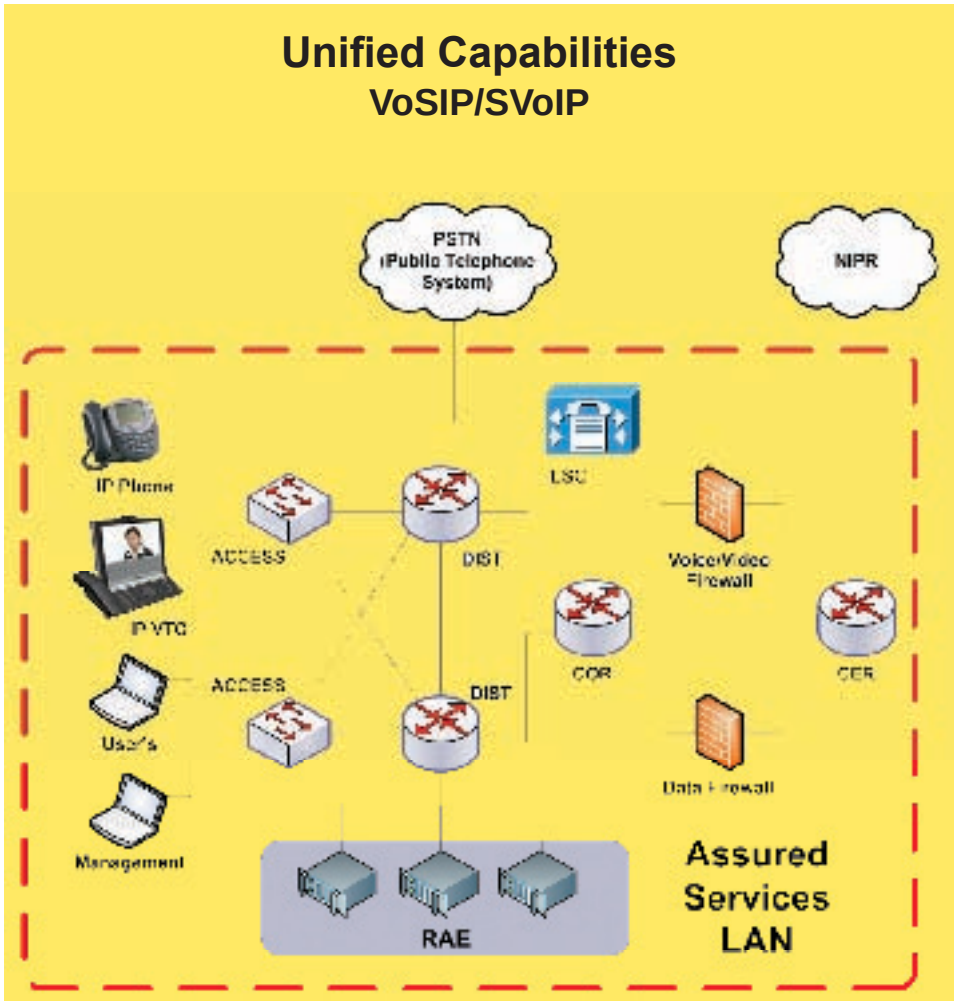


Figure 1. Voice over Secure IP (VoSIP)/Secure Voice over Internet Protocol and other secure real-time services provided by the voice systems integrated product team.

replace aging cryptographic units, including KY-57, KY-58, KY-99A, KY-100 and KYV-5.

As the Navy's VINSON/Advanced Narrowband Digital Voice developmental and engineering agent, the secure voice team is responsible for validation and verification of low rate initial production variant VACM products, including addressing emergent technologies and their viability over various communication transports.

The Navy's secure voice team's active participation puts Navy technical requirements on equal footing with that of the Air Force, and its specialized expertise ensures the appropriate technical validation for Navy-unique requirements, particularly environmental variables, such as salt water, temperature and pressure tolerances, that would otherwise have been overlooked.

The secure voice team continues to be a key member of the multiservice VACM acquisition team, and will be responsible for monitoring vendor technical performance and conducting independent verification and validation testing on preproduction models prior to Navy acceptance.

ADNS Voice

The majority of the voice systems IPT's recent engineering work was dedicated to ensuring voice capability using the Navy's ADNS for transport. Under the direction of Automated Digital Network System engineering, the voice team supports formal test and evaluation of any ADNS voice-related component of SPAWAR's enterprise engineering and certification testing, including voice communications interoperability, circuit emulation over IP, and homeport dial tone.

The naval networking infrastructure is under continuous modernization in response to the Defense Information Systems Agency's (DISA) unified capabilities requirements (UCR 2008). Unified capabilities requirements specify technical standards for telecommunication switching equipment to be connected to the Defense Information Systems Network (DISN); emphasis is on military unique features, e.g., Multilevel Precedence and Preemption (MLPP).

The Automated Digital Network System voice team is meeting DISA's requirements by adapting legacy voice circuits for transport using IP-based technologies to both increase bandwidth efficiency and consolidate naval communication pathways across the ADNS network links.

The ADNS voice team introduced the SCIP-IWF as the technological solution capable of coupling legacy telephony products, such as secure terminal equipment and various shipboard telephone switches, to modernized networks capable of servicing a greater number of concurrent calls with more features and at reduced costs in terms of connectivity overhead requirements. The SCIP-IWF transformed naval operational voice by transparently enabling off-ship secure and nonsecure voice connectivity, supporting global telephony from virtually every vessel in the Navy. The ADNS voice team continues to manage and maintain this critical program and is providing installations and engineering support for the SCIP-IWF's integration into the Naval Undersea Warfare Center's Common Submarine Radio Room.

Evaluate Emerging Technologies

While ADNS transport is a critical element of voice communications modernization, it is complemented by DISA's unified capability requirements, which provide a series of integrated and complementary technical standards and products

necessary to meet future Defense Department communications operational and security requirements. These include a mix of real-time communication services, such as telephony (including IP-based telephony), videoconferencing and real-time chat, which will eventually be integrated with unified messaging, such as integrated voice mail, e-mail, short message service (text communication service component of phone, Web or mobile communication systems), and fax transmission.

The UC requirements also establish communication and resource priorities, provision for access and control, and provide multilevel precedence and preemption capability to assure access for command and control users.

The Joint Interoperability Test Command (JITC) is responsible for UC testing to ensure its proper implementation. JITC selected the voice engineering lab as a partnering facility to evaluate a variety of UC voice and data products and services. JITC distributed testing is performed in collaboration with DISA, and the other services, to provide the technical solutions necessary to migrate Defense Switched Network (DSN) services to assured service Voice and Video over IP (VVoIP) unified capabilities. The voice systems IPT is a key element of the JITC distributed test lab group directly supporting DISA's efforts to provide joint service UC interoperability.

The voice systems IPT uses its end-to-end secure communications expertise and sophisticated laboratory to create high-fidelity simulations of Navy and joint communications architectures, allowing evaluation of an array of supporting and interrelated technologies for JITC-approved products testing.

These special voice assets also play a key role in furthering the Navy's interests in rapid technology transfer research and development for a variety of IP-based technologies, such as Assured Services-Service Initiated Protocol (AS-SIP), Voice over Secure IP (VoSIP), and other secure real-time services. This concept is illustrated in Figure 1. The voice engineering lab's continuing efforts ensure the ability of the DISN and DoD service infrastructures to supply prioritized and protected voice, video and data transmissions, including proposed Navy and joint communications architectures.

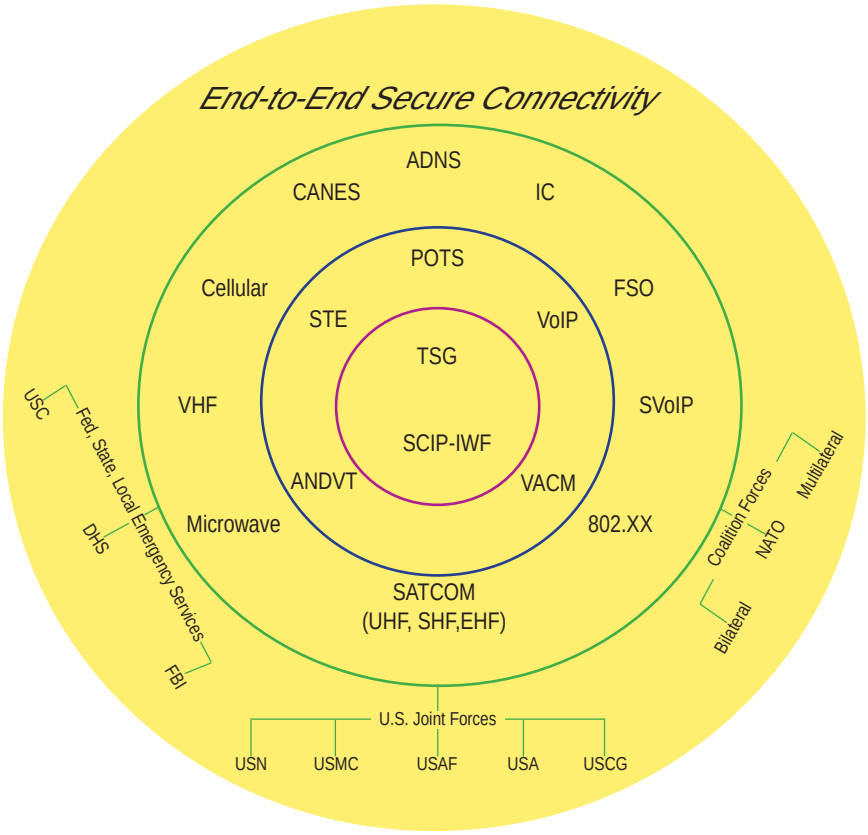


Figure 2. SPAWARSYSCEN Atlantic's voice systems integrated product team (IPT) provides secure voice end-to-end connectivity for Navy, joint, coalition and national agencies with a variety of communications capabilities.

Defense Red Switch Network

SPAWARSYSCEN Atlantic's voice systems IPT is also the Navy lead for DRSN engineering and technical support. DRSN is a DISA-managed Joint Staff telephony system used as the primary national command authority voice network, providing global secure services to the president, Secretary of Defense, Joint Chiefs of Staff, combatant commanders and selected agencies, with command and control secure voice and voice conferencing capabilities. Figure 2 illustrates the DRSN range of services and customers of the voice engineering lab.

SPAWARSYSCEN Atlantic provides on-site technical support personnel for five Navy shore sites, as well as DRSN installation, and engineering support, testing, and training for DRSN sites and other DoD activities.

The SPAWARSYSCEN Atlantic voice systems IPT provides the Department of the Navy (DON) with capability-driven and sustainable solutions, leading the way to ensure naval compatibility with future DoD unified capabilities and assured services. As the primary point of contact for DON enterprise-wide voice communications, the IPT successfully helped steer Navy voice communication away from legacy (channelized and stovepiped) to more modernized, net-centric solutions.

The IPT's ISEA and sustainment efforts are essential to the Navy's voice systems operators and directly support global operations. Its tireless pursuit of modernized and practical voice solutions have helped the Navy transition from serial-based, legacy telephony systems into modern, IP-based naval voice communication networks, a vital link in the transition process to the Navy and DoD's net-centric Global Information Grid.

The voice systems IPT's expert advocacy continues to provide acquisition managers and Program Executive Officer (PEO) C4I leadership the technical foundation necessary for informed Navy enterprise voice decisions. CHIPS

Nick Werner is the SPAWARSYSCEN Atlantic voice systems IPT technical writer.

DON EMPLOYEE CHALLENGES USE OF UNAUTHORIZED DoD "FORM"

By Steve Muck

The Department of the Navy is working to eliminate the unnecessary collection of Social Security numbers (SSNs) to protect your personally identifiable information (PII). The SSN is ubiquitous and one of the key data elements used to commit identity fraud. The DON has embarked on a plan to reduce the use of the SSN by eliminating it where it is not needed or replacing it with another unique identifier (e.g., the Department of Defense identification number/Electronic Data Interchange-Personal Identifier (EDI-PI)) associated with an individual's name.

The following is a recent success story that highlights the actions an individual took to challenge the use of a form that appeared to be an unauthorized collection of PII. It is very likely that business processes within your organization are repeating a scenario similar to this. This success story should serve as a reminder to all that only approved collections of PII are authorized.

The command security manager approached his command's privacy official presenting what appeared to be a routine form and asked if it was an authorized collection of PII. The privacy official noted that the form had a Privacy Act Statement at the bottom of each page, but did not appear to be an approved DoD form because it was lacking a form number. The command staff was sensitized to the use of unauthorized forms as part of the DoD/DON SSN Reduction Plan; therefore, several staff members were reluctant to provide the information because it asked for full name, full SSN, and other PII to be used for controlled space access.

The DON privacy official contacted the DoD forms manager who agreed that the form did not appear to be official. The DoD forms manager then contacted the head of the security office responsible for the form, who is now in the process of either eliminating the form or making it an official standard form (SF) or Defense Department (DD) form. To make the form official it must be reviewed by the DoD forms manager and DoD privacy official. If PII is collected on the form, a Privacy Act Statement (PAS) must be created. If SSNs are collected on the form, there must be an approved justification that cites one of 12 valid exceptions ("Approved Use Cases for Systems Collecting SSNs" available at www.doncio.navy.mil/ContentView.aspx?ID=1833) that allow its continued use. The approved justification is an auditable record and must be signed by a flag or Senior Executive Service member, or "By Direction" authority. The forms review process is the same for all DON controlled forms.

Bravo Zulu to the personnel who alerted their privacy official that there may be a problem with PII collection using what appeared to be a routine form. Personnel should challenge any form that collects PII, does not have an official form number, and an attached Privacy Act Statement. By properly managing official forms, exposure and use of PII will be greatly reduced, and commands will be compliant with existing privacy laws and regulations. CHIPS

Steve Muck is the DON privacy team lead.

By JPEO JTRS Strategic Communications

JTRS SRW Network Manager Successfully Completes Format Qualification Test

Enterprise Business Model stimulates competition and increases innovation

The Joint Program Executive Office (JPEO) for the Joint Tactical Radio System (JTRS) Network Enterprise Domain (NED) announced the successful completion of the formal qualification test (FQT) of the Soldier Radio Waveform Network Manager (SRWNM) with multiple JTRS radios Jan. 28, 2011. Completion of the SRWNM FQT is a significant milestone in delivering an enterprise-wide network planning and management capability for JTRS radios.

SRWNM enables planning for heterogeneous SRW networks consisting of SRW-capable radios from multiple vendors, generating presets for the radios in the plan, downloading presets to the planned radio nodes, and then monitoring the planned operational SRW network. SRWNM is a key component of the JTRS Enterprise Network Manager (JENM) which provides tactical network management products for all JTRS radios. JENM enables planning, instantiation, management and over-the-air reconfiguration of tactical networks comprised of software defined radios from multiple vendors, greatly simplifying network planning and operations compared with using separate management products provided by each qualified radio vendor.

In addition to providing SRW planning and management for JTRS radios under development on government contracts, such as the Ground Mobile Radios (GMR) and Handheld/Manpack/Small Form Fit (HMS) programs, the SRWNM development and FQT included robust planning and management capabilities for the Harris Corp. AN/PRC-117G and ITT Corp. Soldier-Rifleman Radio. Both of these radio products are being developed by leveraging the JTRS Enterprise Business Model, which allows radio developers access to JTRS software capabilities for integration into their products, without using government contracts and funding.

The JTRS Enterprise Business Model is designed to stimulate competition, increase innovation and reduce government costs through software reuse while simultaneously speeding development and fielding of tactical networking capabilities. Inclusion of radio products developed under the JTRS Enterprise Business Model in the SRWNM FQT represents a unique government and industry partnership to aggressively deliver advanced tactical networking capabilities to joint warfighters. Successful completion of the SRWNM FQT with these products included validates the JTRS Enterprise Business Model effectiveness and illustrates its ability to foster a competitive environment in the defense communications and networking industry. All SRWNM and JENM releases are also made available on the JTRS Information Repository to other authorized users within the Department of Defense and industry.

JPEO JTRS Announces Approval of COALWNW Operational Requirements

Introduction of software defined radio programs with partner nations spurs requirements for interoperability

In June 2009, nine nations (Australia, Finland, France, Germany, Italy, Spain, Sweden, the United Kingdom and United States) agreed to jointly develop a wideband networking waveform to enable tactical interoperability among coalition forces. This waveform is known as the Coalition Wideband Networking Waveform, or COALWNW, (pronounced Coal-Win).

The JPEO JTRS announced in January 2011 the approval of the operational requirements document (ORD) underpinning the COALWNW specification. The ORD represents the consolidated and prioritized operational requirements of the nations participating in the COALWNW international agreement and is intended to support potential future development of a common, interoperable waveform. This milestone is an important step toward achieving enhanced interoperability and communication between the United States and coalition partners.

Enhanced interoperability among coalition partners is an essential requirement on the modern battlefield, with multinational coalitions becoming the norm for conducting military operations in hot spots around the world. The COALWNW tactical networking capability will allow coalition partners to exchange secure wideband voice, data and video between each nation's software defined radios in land, air and maritime domains. These capabilities will significantly contribute to improved coordination, shared situational awareness, reduced chance of fratricide, and secure provisioning of effects across multinational boundaries.

The COALWNW capability will be designed, developed and tested using a three-phased approach: (1) waveform specification; (2) waveform development; and (3) interoperability testing. During the first phase, the participating nations have developed a single set of operational requirements that will underpin the COALWNW specification. To evaluate and baseline these requirements, the nations performed a comprehensive

requirements definition process that included an analysis of current waveform developments.

When waveform development begins in the second phase, COALWNW will be delivered incrementally with increased functionality incorporated in later increments. In this manner, developmental risk can be effectively managed and early deployment of initial capability can be achieved. The first increment will focus on delivering interoperability within the ground environment, inclusive of many maritime and air support assets. A working group, comprised of members from the nine COALWNW nations, is studying alternatives to determine the best acquisition strategy for the initial increment. Member nations expect that other nations will join the COALWNW effort for development of the first increment.

A key enabler to the COALWNW capability is the introduction of software defined radio programs within the partner nations. In a software defined radio, the software defines the communication characteristics of the radio, and software waveforms may be reused and ported onto different radio hardware similar to computer applications. Once developed, the intent is to port COALWNW onto the various nations' software defined radio hardware hosts, thus ensuring coalition interoperability through a diverse range of platforms.

MIDS JTRS Receives Limited Production 2 Approval

Terminals slated for Navy's F/A-18E/F Super Hornet, Air Force's EC-130H Compass Call and RC-135 Rivet Joint

The Multifunctional Information Distribution System Joint Tactical Radio System (MIDS JTRS) terminal was approved for Limited Production 2 procurement. The Acquisition Decision Memorandum was signed Jan. 31, 2011, by Under Secretary of Defense for Acquisition, Technology and Logistics Dr. Ashton B. Carter.

"The MIDS JTRS Limited Production 2 decision is another major accomplishment for the MIDS program and the JTRS enterprise and advances the program one step closer to full production and the initial operational capability (IOC) milestone," said Navy Capt. Scott Krambeck, MIDS program manager.

The MIDS program is one of five major acquisition category (ACAT) 1D programs within the JTRS enterprise. MIDS provides interoperable, affordable and secure tactical data link and programmable networking technologies and capabilities for the joint, coalition and international warfighter. MIDS JTRS is a software defined networking terminal that is not only National Security Agency (NSA) certified with the Link 16 waveform, but is also equipped with Link 16 Enhanced Throughput and Link 16 Frequency Remapping.

The MIDS JTRS terminal has demonstrated continued maturity over the past year, and with the successful completion of this Limited Production 2 decision, the MIDS JTRS program has reached another significant objective on its path to delivering the advanced networking capabilities into the hands of the warfighter. The MIDS program office is now authorized to allow MIDS JTRS to enter into a second limited production of 42 terminals for the Navy's F/A-18E/F Super Hornet, as well as the Air Force's EC-130H Compass Call and RC-135 Rivet Joint.

Krambeck added, "While we still have some additional MIDS JTRS testing to conduct prior to full production and IOC, I am extremely pleased with the progress the team is making, the new trails we are blazing, and the lessons learned that we are sharing with our JTRS teammates. The outstanding government and industry MIDS JTRS team continues to advance and demonstrate JTRS technology and soon the warfighter will benefit. I am anxious to get MIDS JTRS operating in the fleet." CHIPS

The Seawater Antenna

By Holly Quick

Space and Naval Warfare Systems Center Pacific (SSC Pacific) high frequency antenna designer, Daniel Tam, developed an innovative device that uses the magnetic induction properties of salt in seawater to create a very high frequency (VHF) antenna. The patent-pending seawater antenna, recently coined the Electrolytic Fluid Antenna, was on display at the SPAWAR exhibit at AFCEA West 2011, Jan. 25-27 in San Diego.

Conference attendees were fascinated by Tam's demonstration of the seawater antenna as he, and SSC Pacific scientists P. Michael McGinnis and Lu Xu, eagerly discussed the advantages of the seawater antenna. A continuous line of spectators watched as Tam, McGinnis and Xu demonstrated how to use a jet of seawater as a communications antenna.

Tam combined water and sodium chloride to replicate seawater and pumped it into a plastic enclosed tube. The tube was then placed inside a current probe made of a ferrite magnetic core hooked to a water pump creating the jet of water. The magnetic field in the probe induced a current that spread via the salt in the seawater.

Standing approximately five feet from Tam, McGinnis spoke into a portable radio while his message was transmitted to Tam using a VHF signal. The signal transmission was possible because of the principle of magnetic induction, which uses ion conduction instead of the electron flow that is used in regular, metallic antennas.

The width and length of the water stream projected from the Electrolytic Fluid Antenna determine bandwidth and frequency capabilities. An 80-foot high stream could transmit and receive from two to 400 megahertz (MHz) with a relatively small onboard footprint.

The Electrolytic Fluid Antenna can transmit and receive HF, VHF and ultra-high frequency (UHF) signals and has been tested at a receiving range of more than 30 miles. A typical Navy vessel has 80 metallic antennas that could theoretically be replaced with only 10 Electrolytic Fluid Antennas of varying heights and streams to cover the same frequencies.

"The advantage of the seawater antenna is that we no longer have topside real estate restrictions. We can place the antenna anywhere along the deck of the ship," Tam said.

As the use of wireless communication continues to grow, an increasing number of antennas are required to support data transmission, and many conditions limit available space for antenna placement. The Electrolytic Fluid Antenna could decrease the footprint for antennas in situations where shipboard space is scarce by decreasing the need for metallic antenna structures.

The Electrolytic Fluid Antenna can be turned off when not in use, with no unsightly obscuring views, and even allow ships to avoid radar detection by adversaries. The system could be used portably as an emergency antenna for watercraft, potentially powered by battery, solar panel or manually with a foot pump.

The technology could possibly be used on land with salt-supplemented water, replacing large unsightly antenna towers with fountains. Another use for a seawater antenna could be as an emergency antenna system for watercraft.

Electrolytic Fluid Antenna Facts

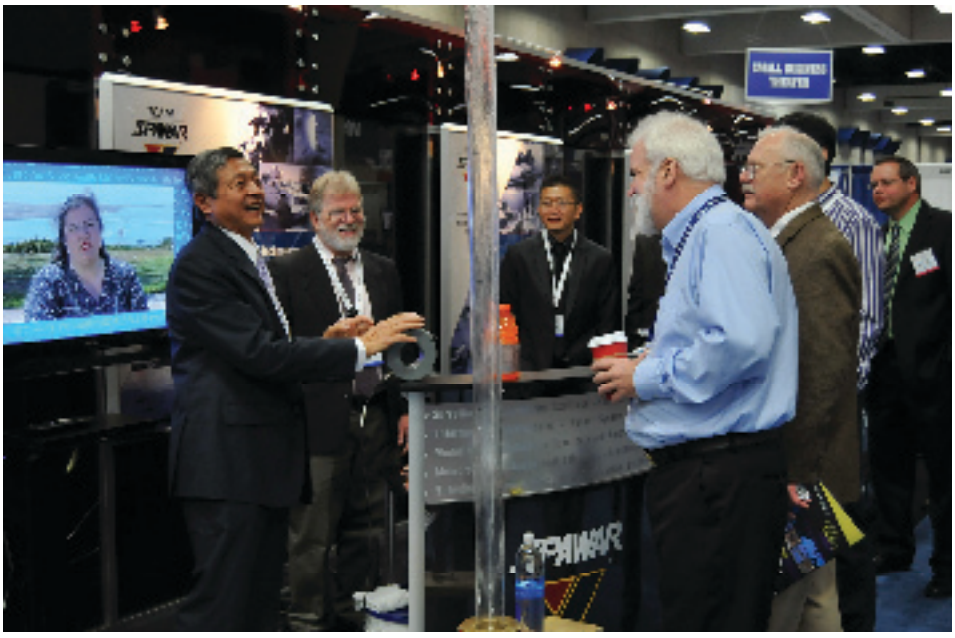
- Sends and receives HF, VHF and UHF signals.
- Frequency range is based on the height of the water stream:
  - o HF – 70 to 80 feet;
  - o VHF – 6 feet; and
  - o UHF – 2 feet.
- Transmits and receives from 2 to 400 MHz.
- Capability to turn jet stream on and off.
- Consists of only a stream of saltwater, a current probe made of magnetic coil, an antenna signal cable, and a plastic tube (if indoors or in an area with extreme wind).

In the future, Tam said the technology will be able to use the salt solution in human bodies to turn body parts into communications antennas.

"My vision for the future for Navy warfighters is to design a small antenna using your own finger as an antenna element. For women, I can design earrings, a necklace and a bracelet. For men, a necktie and a belt," Tam said.

Using human body parts as communications antennas will give warfighters a winning edge by dramatically reducing the weight they have to carry. CHIPS

Holly Quick is a contributor to CHIPS and supports the public affairs office of SPAWARSYSCEN Atlantic. Claire Dobransky from the SSC Pacific Technology Transfer Office contributed to this article. For more information, contact the SSC Pacific public affairs office at (619) 553-2725.



SPAWARSYSCEN Pacific scientists, Daniel Tam, P. Michael McGinnis and Lu Xu, demonstrate the Electrolytic Fluid Antenna at West 2011 in San Diego, Calif. The antenna can transmit HF, VHF and UHF signals. Photo by Rick Naystatt/SPAWAR A/V specialist.

Developing a New Model for Maritime Tactical Information Dominance

By Capt. Danelle Barrett

In an orchestra, each musician produces exquisite music independently and relies on the conductor to synchronize its effort to achieve a sum greater than its parts. As the Navy moves toward an environment where information dominance has the potential to surpass traditional combat power to achieve operational effects, a new conductor is needed to manage the information cacophony in the tactical environment.

In the same way the conductor synchronizes the efforts of an orchestra, the information warfare commander (IWC) is key to leveraging the tactical advantages of the new information landscape to improve assimilation of information, standardize procedures and use transformational technologies to revolutionize operations. The role of the IWC must be refined within this reality to achieve national strategic, operational and tactical outcomes.

To this end, the Chief of Naval Operations tasked all Navy admirals and vice admirals to take part in the implementation of information dominance in a letter issued March 20, 2011 (3800, Ser NOO/S010I) and to report their progress within the next few months. Each tasking names specific commands to take the lead for each area of responsibility. A few of the CNO's directives include: the development of doctrine and requirements at the operational level of war (OLW) to support information dominance; develop a plan and scope for tactics, techniques, and procedures (TTPs) to support information dominance; develop a plan to integrate vigorous, information-intensive training into the Fleet Response Training Plan (FRTP); and develop an approach for dominance environment experimentation.

Currently, information dominance is the squeaky violin of the maritime orchestra, not harmonized for maximum effectiveness. Establishment of the Information Dominance Corps (IDC) in 2009, which combined intelligence, information warfare (IW), information professional (IP) and oceanography officers into one restricted line warfare community provides an opportunity to implement a new IWC construct afloat that improves the use of information as a main operational battery. A senior IDC captain should be that information conductor for the strike group.

The Tactical Information "Conductor"

The role of a strike group IWC in tactical operations requires a revised framework that incorporates both non-kinetic and transformational operational capabilities with tactics, techniques and procedures in a significantly more sophisticated manner than what is done today. With proper direction, and a sustained effort to improve integration of the currently disaggregated information batteries, harmonization will improve speed and accuracy of decision making, shared situational awareness, and the ability to achieve desired operational effects. The IWC should be the conductor providing that reality.

Over the years, the IWC position was filled by officers with varying degrees of expertise. In the past, the IWC function fell under the command and control, communications and computers (C4)/IW department, led by an 0-6 submariner. In some strike groups, the IWC was the commanding officer of the carrier or other ship without an assigned warfare commander role. Regardless of who had the job, the primary focus was on the pillars of Information Operations (IO) most germane in the maritime environment: tactical military deception, electronic warfare, and computer network operations, specifically computer network defense. In the last five years, N6 and IW billets have decoupled on most strike groups with an IP captain in charge of the C4/N6 department and an IW commander working for the IWC. Recently, some strike groups have designated a senior IP officer as the IWC, retaining the same traditional IO focus, but missing the opportunity to create the tactical information conductor.

The legacy Napoleonic staff structure on strike groups is not agile or responsive enough to achieve the tight integration needed to advance information power, particularly using transformational non-kinetic capabilities. Each department provides information support in its respective specialized, or stovepiped areas, to multiple strike group warfare commanders. In the best circumstances, information "seams" are discovered and course corrected during the planning phases, but seams often emerge at later stages, like during a brief to the commander, or in the most unfortunate cases, during execution.

Since the strike group staff already has the resident expertise representing each core competency of the IDC (several IPs, IWs, intelligence and one oceanography officer), a logical and effective first step is to align their efforts under the direction of the information warfare commander. The IWC, as supporting commander, would coordinate with other warfare commanders to ensure their requirements are met by these experts, prioritizing their activity based on commander's guidance. Conversely, depending on the mission and operational requirements, the IWC may be a supported commander for strike group assets and capabilities by other warfare commanders.

Beyond closer integration of the key tenets of information dominance, increased emphasis on use of new technologies and influence operations can revolutionize tactical operations. The responsibility of the IWC must evolve beyond the traditional maritime IO, so that the battlespace is viewed through a new optic. Specific future tasks for the IWC are:

• Creatively combining oceanography, meteorology, hydrography, bathymetry, intelligence, communications and information operations to achieve desired operational effects. A comprehensive analysis of information from these disciplines aligned to support the commander's critical information requirements, mission planning, execution and post operational assessments, would address questions important to mission success such as: how are sensor data and other information across all IDC disciplines combined into actionable intelligence for decision makers? Likewise, the threat posed by enemy capabilities in all of these areas must be critically assessed to identify exploitable vulnerabilities.

• Integration of the "Fifth Domain" ["Learning to Operate in Cyberspace," by Rear Adm. William Leigher, Proceedings, January 2011] of cyberspace operations into planning and mission execution. Maintaining situational awareness of command and control infrastructure requires the IWC to predict, identify and mitigate threats. Threats may be environmental, enemy-imposed or self-induced. The IWC would lead the development and execution of exercise plans to operate in a satellite denied or bandwidth reduced environment and would manage the tactical electromagnetic spectrum to ensure uninterrupted command and control of forces.

• Employment of non-kinetic capabilities for influence operations

nested in the larger joint task force and theater strategic communication efforts. This involves close coordination with other warfare commanders to include non-kinetic strikes (leaflets, psychological operations broadcasts, etc.) into the air tasking order and larger battlespace.

• Institutionalize a sustained and purposeful knowledge and information management effort to standardize practices for quality, expeditious information exchange and reuse. The focus should be on improving sharing and synthesis of information among the composite warfare commanders (air, surface, subsurface and strike), and removal of barriers to information sharing internal to the strike group and with external entities including coalition partners. Lastly, there should be an iterative refinement of the strike group battle rhythm to improve speed and accuracy of decision making.

• Leverage transformational technologies, such as social networking tools, for information sharing even in bandwidth limited situations, and unmanned vehicles (UV) for improved situational awareness, kinetic and non-kinetic strike, and communications relay for sustainment of command and control links.

While some of these functions are performed in an ad hoc manner in the fleet today, the harmonization of their effects is not always deliberate, planned and measured to adequately gauge effectiveness, and best practices are not institutionalized. Lessons continue to be observed and relearned. While there are many operational tasking messages promulgated (i.e., the OPTASK IW, Communications, Chat, Information Management, Link, etc.) to address specific elements of the information domain, they are not always comprehensive or fully coordinated. For example, has the OPTASK Communications properly accounted for frequencies used for UVs to prevent interference? Does the OPTASK Information Management include provisions to exchange time-critical products, like imagery or oceanography products, with bandwidth disadvantaged units including coalition partners? How does the strike group disseminate tasking for implementation of strategic communications themes and messages? The IWC should ensure alignment of these tasking orders and institutionalize best practices.

The IWC should also direct the assessment of an adversary's ability to integrate those same information disciplines. For example, does the intelligence preparation of the battlespace account for the enemy's ability to synchronize its information, or are there vulnerabilities that could be exploited to friendly advantage? The IWC should ensure this type of analysis translates to operational plans and targets of opportunity.

Looking to the Future: Unmanned Vehicles in Maritime Operations and Influence Operations

The Navy is increasingly employing aerial and subsurface UVs for persistent maritime intelligence, surveillance and reconnaissance, signals intelligence, support to mine warfare, strike and targeting operations, and for undersea environmental sensing and mapping. Systems used or planned include the Unmanned Carrier Launched Airborne Surveillance and Strike (UCLASS) and unmanned undersea vehicles (UUV). Use of UVs will significantly complicate the information battlespace without a deliberate strategy for managing sensor feeds and information capabilities. The IWC, at the forefront of developing strategy, would implement tactics, techniques and procedures to leverage transformational capabilities.

For UVs to be a true game-changer for tactical operations, they should be multimission capable with some platforms organic to the strike group. As new UV capabilities with global reach evolve, operational commanders can improve joint sharing of these rare assets with tactical commanders, adding to the UV cluster of resources available for maritime operations. Organic strike group UVs could be rapidly deployed or redirected by the IWC, in coordination with the other warfare commanders, to deny adversaries a tactical advantage. Ideally, multimission capable, modular carrier-based unmanned aerial vehicles (UAV), with different packages, could be managed by the IWC to perform various functions: ISR platforms to track vessels of interest, an electronic warfare package to jam enemy sensors, or as aerial communications nodes to extend high data rate communications beyond the horizon. When this capability exists in the future, the IWC would orchestrate their use in operations. Additionally, as interoperability issues between UUVs and existing fleet platforms are resolved, the IWC should understand how to incorporate sensor data from those platforms and use it for executing operations.

A second game-changer for the IWC is the optimized use of strategic communication, including influence operations. Strategic communication starts at the top with the president and National Security Council, who provide doctrine assisting Navy and joint planners in nesting their actions, themes and messages into the higher level influence campaign. There is a tight link between the diplomatic and information elements of national power at the strategic level, and an equally strong link between strategic communication, public affairs and information operations at the operational and tactical levels.

Working with the joint task force and numbered fleet staff, the IWC would ensure that the message sent is the right "non-kinetic fire" for the target audience, is received in a manner that will have the desired impact, and can be measured to validate the effectiveness of both the message and the delivery mechanism. As the IWC coordinates, plans and executes influence operations at the tactical level, nontraditional communications media, such as social networks and microblogging, should be included. Intelligence preparation of the battlespace should consider social network targets with the same level of scrutiny and effort applied to kinetic targeting.

On the tail end, the IWC can improve processes for influence operations battle damage assessment (BDA), conducted with the same rigor used to assess a kinetic strike. The IWC would ensure that the command and control pieces of strike group influence operations are synchronized across all lines of operations and that the plans developed are worked in close coordination with higher authorities. Strategic, operational and tactical plans must be in lockstep, with clearly identified desired effects for strategic communication, including maritime tactical influence operations, to avoid sending conflicting messages to an adversary.

Information is the new game-changer for friendly and enemy forces alike. Maintaining information superiority will provide the tactical advantage for success. Key to this becoming reality is to redefine the IWC role with an IDC officer as the new conductor in operations standardizing techniques, tactics, procedures, doctrine and training across the fleet. CHIPS

Capt. Barrett is an Information Dominance Corps officer with two previous carrier strike group tours.

Enterprise Software Agreements

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

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

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

For more information on the ESI or to obtain product information, visit the ESI website at 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: 23 Mar 15

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: 13 May 11 (Please call for extension information.)

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

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.

The BPWin/ERWin products are now available from the C-EMS2 contract on page 62. The C-EMS2 contract number is listed below.

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

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

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

Database Management Tools

Microsoft Products

Microsoft Database Products – See information under Office Systems on page 65.

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. See information provided on page 66.

Contractors:

Oracle Corp. (W91QUZ-07-A-0001); (703) 364-3110

DLT Solutions (W91QUZ-06-A-0002); (703) 708-8979

immixTechnology, Inc. (W91QUZ-08-A-0001); Small Business; (703) 752-0628

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

TKC Integration Services, LLC (W91QUZ-09-A-0001); Small Business; (571) 323-5584

Ordering Expires:

Oracle: 30 Sep 11
DLT: 01 Apr 13
immixTechnology: 26 Aug 11
Mythics: 18 Dec 11
TKCIS: 29 Jun 11

www.esi.mil

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: See the information provided on page 66 concerning the Navy Oracle Database Enterprise License under Department of the Navy Agreements.

Sybase (DEAL-S)

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

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

Ordering Expires: 15 Jan 13

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

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

Enterprise Application Integration

Sun Software

Sun Products – Provides Sun Java Enterprise System (JES) and Sun StarOffice. Sun JES products supply integration and service oriented architecture (SOA) software including: Identity Management Suite; Communications Suite; Availability Suite; Web Infrastructure Suite; MySQL; xVM and Role Manager. Sun StarOffice supplies a full-featured office productivity suite.

Contractors:

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

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

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

Ordering Expires: 24 Sep 12

Web Links:

Sun Products
www.esi.mil/agreements.aspx?id=160
Commercial Data
www.esi.mil/contentview.aspx?id=160&type=2
Dynamic Systems
www.esi.mil/contentview.aspx?id=162&type=2
World Wide Technology
www.esi.mil/contentview.aspx?id=161&type=2

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; (703) 752-0641 or (703) 752-0646

Ordering Expires: 03 May 11 (Please call for extension information.)

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

VMware

VMware – Provides VMware software and other products and services. This BPA has been designated as a GSA SmartBUY.

Contractor: ***Carahsoft Inc.*** (W91QUZ-09-A-0003)

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

Ordering Expires: 27 Mar 14

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

Enterprise Management

CA Enterprise Management Software (C-EMS2)

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

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

Ordering Expires: 22 Sep 12

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

Microsoft Premier Support Services (MPS-2)

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

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

Ordering Expires: 31 Mar 11 (Please call for extension information.)

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

NetIQ

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

Contractors:

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

Northrop Grumman – authorized reseller

Federal Technology Solutions, Inc. – authorized reseller

Ordering Expires: 05 May 14
Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

Planet Associates

Planet Associates Infrastructure Relationship Management (IRM) Software Products – Provides software products including licenses, maintenance and training for an enterprise management tool for documenting and visually managing all enterprise assets, critical infrastructure and interconnectivity including the interdependencies between systems, networks, users, locations and services.

Contractor: ***Planet Associates, Inc.*** (N00104-09-A-ZF36); Small Business; (732) 922-5300 ext. 202
Ordering Expires: 01 Jun 14
Web Link: www.esi.mil/contentview.aspx?id=143&type=2

Quest Products

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

Contractors:
Quest Software, Inc. (W91QUZ-05-A-0023); (301) 820-4889
DLT Solutions (W91QUZ-06-A-0004); (703) 708-9127
Ordering Expires:
Quest: 29 Dec 15
DLT: 01 Apr 13
Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

Enterprise Resource Planning

Oracle

Oracle – *See information provided under Database Management Tools on page 61.*

RWD Technologies

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

Contractor: ***RWD Technologies*** (N00104-06-A-ZF37); (410) 869-3014
Ordering Expires: Effective for term of the GSA FSS Schedule
Web Link: www.esi.mil/contentview.aspx?id=150&type=2

SAP

SAP Products – Provide 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 Links:
SAP
www.esi.mil/contentview.aspx?id=154&type=2
Advantaged
www.esi.mil/contentview.aspx?id=155&type=2
Carahsoft
www.esi.mil/contentview.aspx?id=156&type=2
Oakland
www.esi.mil/contentview.aspx?id=157&type=2

Information Assurance Tools

Data at Rest (DAR) 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 to include approved U.S. thumb drives. All products use cryptographic modules validated under FIPS 140-2 security requirements and have met stringent technical and interoperability requirements.

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

Service component chief information officers (CIO) are developing component service-specific enterprise strategies. Accordingly, customers should check with their CIO for component-specific policies and strategies before procuring a DAR solution.

The DON CIO issued an enterprise solution for Navy users purchasing DAR software. See the information provided on page 66 under Department of the Navy Agreements. The Department of the Army issued an enterprise solution for Army users purchasing DAR software. See the information provided on the Army CHESS website at https://chess.army.mil/ascp/commerce/contract/FA8771-07-A-0301_bpaorderinginstructions(2)_ARMY.jsp. As of this printing, the Air Force has not yet provided a DAR solution.

Mobile Armor – ***MTM Technologies, Inc.*** (FA8771-07-A-0301)
McAfee – ***Rocky Mountain Ram*** (FA8771-07-A-0302)
Information Security Corp. – ***Carahsoft Technology Corp.*** (FA8771-07-A-0303)
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)
Checkpoint – ***immix Technologies*** (FA8771-07-A-0307)
SPYRUS, Inc. – ***Autonomic Resources, LLC*** (FA8771-07-A-0308)
WinMagic, Inc. – ***Govbuys, Inc.*** (FA8771-07-A-0310)
CREDANT Technologies – ***Intelligent Decisions*** (FA8771-07-A-0311)
Symantec, formerly GuardianEdge Technologies – ***Merlin International*** (FA8771-07-A-0312)
Ordering Expires: 14 Jun 12 (If extended by option exercise.)
Web Link: www.esi.mil

McAfee (formerly Securify)

McAfee – 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. McAfee 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: 31 May 11

Web Link: www.patriot-tech.com/contract-vehicles/gcv-dodesi.html

Symantec

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

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

Ordering Expires: 31 May 11

Web Link: www.immixgroup.com/contract-vehicles/federal/esi/symantec

Symantec Antivirus:

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 websites:

NIPRNET site: https://patches.csd.disa.mil

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

Websense (WFT)

Websense – Provides software and maintenance for Web filtering products.

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

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

Ordering Expires: 31 Aug 11

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

Xacta

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

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

Ordering Expires: 24 Sep 14

Web Link: https://esi.telos.com/contract/overview/default.cfm

Lean Six Sigma Tools

iGrafx Business Process Analysis Tools

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

Contractors:

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

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

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

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

Ordering Expires: 31 Jan 14

Web Links:

Softchoice
www.esi.mil/contentview.aspx?id=118&type=2
Softmart
www.esi.mil/contentview.aspx?id=117&type=2
SHI
www.esi.mil/contentview.aspx?id=123&type=2

Minitab

Minitab – 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: www.esi.mil/contentview.aspx?id=73&type=2

PowerSteering

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

Contractor: ***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: www.esi.mil/contentview.aspx?id=145&type=2

Office Systems

Adobe Desktop Products

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

Contractors:

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

CDW Government, LLC (N00104-08-A-ZF34); (703) 621-8211

GovConnection, Inc. (N00104-08-A-ZF35); (301) 340-3861
Insight Public Sector, Inc. (N00104-08-A-ZF36); (443) 306-7885
Ordering Expires: 30 Jun 12
Web Links:
Adobe Desktop Products
www.esi.mil/agreements.aspx?id=52
Dell
www.esi.mil/contentview.aspx?id=53&type=2
CDW-G
www.esi.mil/contentview.aspx?id=52&type=2
GovConnection
www.esi.mil/contentview.aspx?id=33&type=2
Insight
www.esi.mil/contentview.aspx?id=54&type=2

Adobe Server Products

Adobe Server Products – Provides software licenses (new and upgrade), maintenance, training and support for numerous Adobe server products including LiveCycle Forms; LiveCycle Reader Extensions; Acrobat Connect; Flex; ColdFusion Enterprise; Flash Media Server and other Adobe server products.
Contractor:
Carahsoft Technology Corp. (N00104-09-A-ZF31); Small Business; (703) 871-8503
Ordering Expires: 14 Jan 14
Web Link: www.esi.mil/contentview.aspx?id=186&type=2

Microsoft Products

Microsoft Products – Provides licenses and software assurance for desktop configurations, servers and other products. In addition, any Microsoft product available on the GSA schedule can be added to the BPA.
Contractors:
CDW Government, LLC (N00104-02-A-ZE85); (888) 826-2394
Dell (N00104-02-A-ZE83); (800) 727-1100 ext. 7253702 or (512) 725-3702
GovConnection (N00104-10-A-ZF30); (301) 340-3861
GTSI (N00104-02-A-ZE79); (800) 999-GTSI ext. 2071
Hewlett-Packard (N00104-02-A-ZE80); (978) 399-9818
Insight Public Sector, Inc. (N00104-02-A-ZE82); (800) 862-8758
SHI (N00104-02-A-ZE86); (732) 868-5926
Softchoice (N00104-02-A-ZE81); (877) 333-7638
Softmart (N00104-02-A-ZE84); (800) 628-9091 ext. 6928
Ordering Expires: 31 Mar 13
Web Link: www.esi.mil/agreements.aspx?id=173

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 websites listed below to obtain the GIG segmented version of the software. You may not use the commercial version available from the August Schell Red Hat download site.

If you are not sure which version (commercial or segmented) to use, we strongly encourage you to refer to the websites listed below for additional information to help you to make this determination before you obtain the software from the August Schell Red Hat download site (or contact the project manager).

GIG or GCCS users: Common Operating Environment Home Page
www.disa.mil/gccs-j/index.html
GCSS users: Global Combat Support System
www.disa.mil/gcssj

Contractor: ***August Schell Enterprises*** (www.augustschell.com)

Download Site: http://redhat.augustschell.com
Ordering Expires: (Please call (703) 882-1636 for information about follow-on contract.)
All downloads provided at no cost.
Web Link: http://iase.disa.mil/netlic.html

Red Hat Linux

Red Hat Linux – Provides operating system software license subscriptions and services to include installation and consulting support, client-directed engineering and software customization. Red Hat Enterprise Linux is the premier operating system for open source computing. It is sold by annual subscription, runs on seven system architectures and is certified by top enterprise software and hardware vendors.
Contractors:
Carahsoft Technology Corporation (HC1028-09-A-2004)
DLT Solutions, Inc. (HC1028-09-A-2003)
Ordering Expires:
Carahsoft: 09 Feb 14
DLT Solutions, Inc.: 17 Feb 14
Web Link: www.esi.mil

Operating Systems

Apple

Apple – Provides Apple Desktop and Server Software, maintenance, related services and support as well as Apple Perpetual Software licenses. These licenses include Apple OS X Server v10.5; Xsan 2; Apple Remote Desktop 3.2; Aperture 2; Final Cut Express 4; Final Cut Studio 2; iLife '08; iWork '08; Logic Express 8; Logic Pro 7; Mac OS X v10.5 Leopard; QuickTime 7 Pro Mac; and Shake 4.1 Mac OS X. Software Maintenance, OS X Server Support, AppleCare Support and Technical Service are also available.
Contractor: ***Apple, Inc.*** (HC1047-08-A-1011)
Ordering Expires: 10 Sep 11
Web Link: 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: 31 May 11 (Please call for extension information.)
Web Link: www.disa.mil/contracts/guide/bpa/bpa_sun.html

Research and Advisory BPA

Research and Advisory Services BPAs provide unlimited access to telephone inquiry support, access to research via websites and analyst support for the number of users registered. In addition, the services provide independent advice on tactical and strategic IT decisions. Advisory services provide expert advice on a broad range of technical topics and specifically focus on industry and market trends. BPA listed below.

Gartner Group (N00104-07-A-ZF30); (703) 378-5697; Awarded Dec. 1, 2006

Ordering Expires: Effective for term of GSA contract

Authorized Users: All DoD components. For the purpose of this agreement, DoD components include: the Office of the Secretary of Defense; U.S. Military Departments; the Chairman of the Joint Chiefs of Staff; Combatant Commands; the Department of Defense Office of Inspector General; Defense Agencies; DoD Field Activities; the U.S. Coast Guard; NATO; the Intelligence Community and Foreign Military Sales with a letter of authorization. This BPA is also open to DoD contractors authorized in accordance with the FAR Part 51.

Web Link: www.esi.mil/contentview.aspx?id=171&type=2

Department of the Navy Agreements

Oracle (DEAL-O) Database Enterprise License for the Navy

On Oct. 1, 2004 and May 6, 2005, the Navy established the Oracle Database Enterprise License, effective through Sept. 30, 2013. The enterprise license provides Navy shore-based and afloat users, to include active duty, Reserve and civilian billets, as well as contractors who access Navy systems, the right to use Oracle databases for the purpose of supporting Navy internal operations. Navy users in joint commands or supporting joint functions should contact the NAVICP Mechanicsburg contracting office at (717) 605-5659 for further review of the requirements and coverage.

This license is managed by the Space and Naval Warfare Systems Center (SPAWARSYSCEN) Pacific. 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: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

Data at Rest Solutions BPA Navy Agreement only

The DON CIO has issued an enterprise solution for Navy users purchasing DAR software. Visit the DON CIO website 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 ESI website at www.esi.mil/contentview.aspx?id=131&type=2. Procurement of other DAR solutions for Navy users is prohibited.

Navy Enterprise BPA for DAR Users:

Mobile Armor – ***MTM Technologies, Inc.*** (N00104-09-A-ZF30)

Web Link: www.esi.mil/contentview.aspx?id=131&type=2

NEED HELP?

CONTACT THE PROJECT MANAGERS BELOW FOR ASSISTANCE

PROGRAM MANAGER
HANK INGORVATE

ORACLE (DEAL-O) NAVY PROJECT MANAGEMENT
JEFFREY HO

MICROSOFT PRODUCTS
TERRY SAMPITÉ

IGRAFX, RESEARCH AND ADVISORY BPA, SAP
NINA DIEP

ADOBE DESKTOP PRODUCTS, ADOBE SERVER PRODUCTS, ENTERPRISE APPLICATION INTEGRATION, SUN SOFTWARE
SUSAN ELLISON

MINITAB, POWERSTEERING, RWD TECHNOLOGIES, PLANET ASSOCIATES
THAO VU

MTM TECHNOLOGIES NAVY PROJECT MANAGEMENT
LAUREN JOHNSON

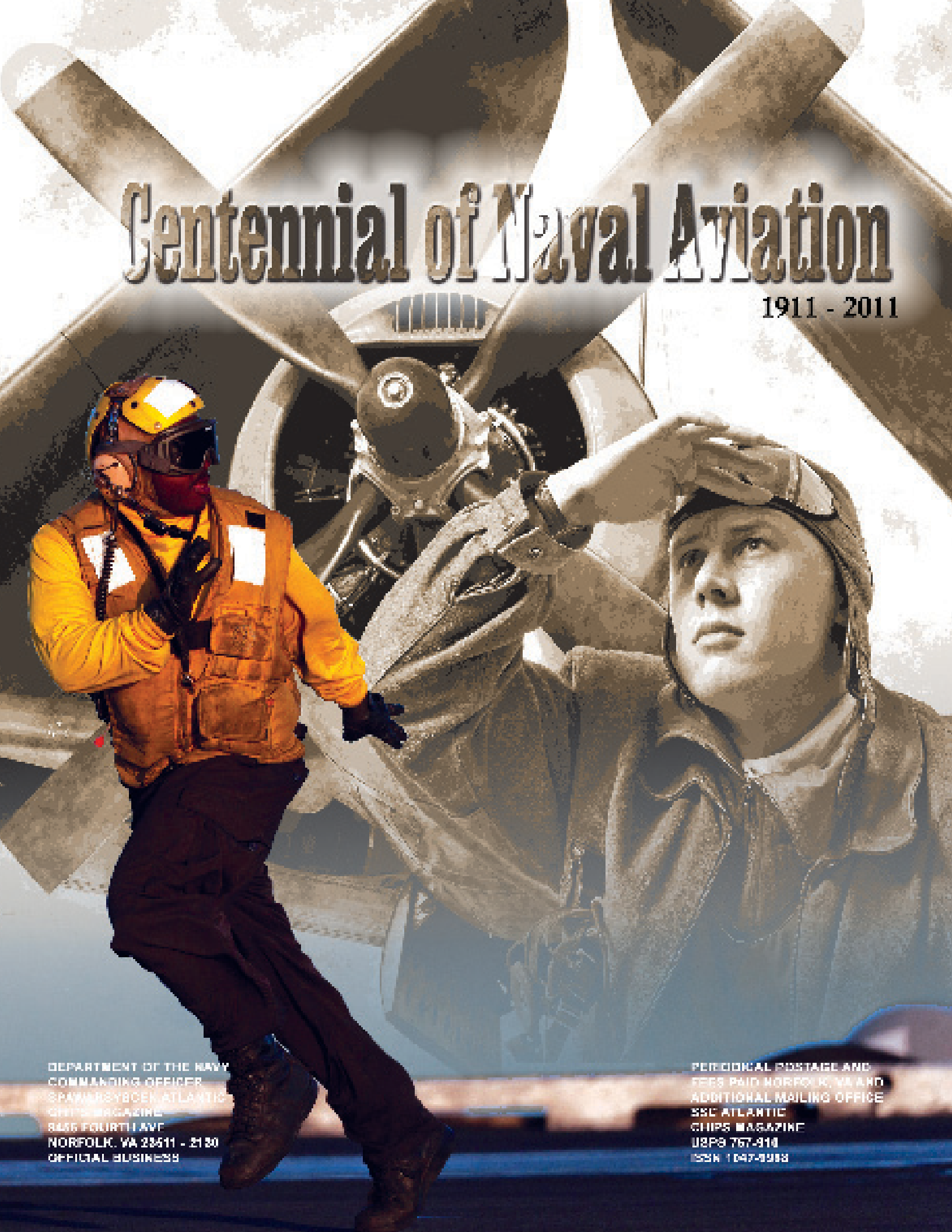
ALL ENTERPRISE CONTRACT INFORMATION HAS BEEN CONSOLIDATED UNDER
WWW.ESI.MIL
FOR YOUR TECHNOLOGY NEEDS

WWW.CHIPS.NAVY.MIL

WWW.DONCIO.NAVY.MIL

ENTERPRISE COST $AVINGS ARE JUST A CLICK AWAY

VISIT OUR E-COMMERCE SITE - WWW.ITEC-DIRECT.NAVY.MIL



DEPARTMENT OF THE NAVY
COMMANDING OFFICER
SPAWARSYSCEN ATLANTIC
CHIPS MAGAZINE
8456 FOURTH AVE
NORFOLK, VA 23511 - 2130
OFFICIAL BUSINESS

PERIODICAL POSTAGE AND
FEES PAID NORFOLK, VA AND
ADDITIONAL MAILING OFFICE
SSC ATLANTIC
CHIPS MAGAZINE
USPS 767-910
ISSN 1047-9988