

CHIPS
magazine



JUL-SEP
2006

J T R S

Joint Tactical Radio System

R E L O A D E D



***Dedicated to Sharing
Information • Technology • Experience***

CHIPS Jul-Sep 2006

Department of the Navy
Chief Information Officer
Mr. David Wennergren

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

Space & Naval Warfare Systems Center Charleston
Commanding Officer
Captain Red Hoover



Senior Editor
Sharon Anderson

Assistant Editor
Nancy Reasor

Web support: Tony Virata and Bill Bunton
DON IT Umbrella Program

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

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

Submit article ideas to CHIPS editors 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 Charleston, 9456 Fourth Ave., Norfolk, VA 23511-2130, or call (757) 444-8704; DSN 564. E-mail address: chips@navy.mil; fax (757) 445-2103; DSN 565. Web address: <http://www.chips.navy.mil/>.

Disclaimer: The views and opinions contained in CHIPS are not necessarily those of the Department of Defense nor do they constitute endorsement or approval by the DON CIO, DON IT Umbrella Program or SPAWAR Systems Center Charleston. The facts as presented in each article are verified insofar as possible, but the opinions are strictly those of the individual authors.

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) 444-8704, DSN 564.

Contents

- 4 Editor's Notebook**
- 5 From the DON CIO Dave Wennergren**
- 6 The Joint Tactical Radio System – Reloaded**
A CHIPS "exclusive" with JPEO JTRS Dennis Bauman
- 10 Interview with Deputy Commander U.S. Second Fleet Rear Adm. David O. Anderson**
- 12 U.S. Second Fleet - the Fleet Lead in JEFX 06**
- 16 Interview with Vice Adm. Keith Lippert**
Director Defense Logistics Agency
- 20 Adobe Contract News**
- 21 N - STAR - the quest for America's future scientists and engineers**
- 24 Growing Technology Leaders**
- 25 Calling All High School Students ... to a Science Fair**
- 26 Department of the Navy IM/IT Community Update**
The DON CIO provides guidance on the occupational codes and parenthetical specialty titles for the IM/IT civilian workforce
- 28 Crunching Computers**
- 29 DON CIO Personnel Recognized for Superior Government Service**
- 30 Interview with Carmela Keeney**
Executive Director SPAWAR Systems Center San Diego
- 33 DON CIO Provides Tools for Information Accessibility**
DON CIO releases the second edition of its Section 508 Self-Help Toolkit
- 34 DON CIO Issues FISMA Guidance**
- 35 Sailors Warned of VA Data Compromise**
- 36 Combined Endeavor**
Combined Endeavor links 41 NATO and Partnership for Peace nations together with advanced technology
- 38 Naval Computer and Telecommunications Station Far East Wins CITE Award as "Best NCTS"**
- 39 Communicating from the field with the Australian Army**
U.S. Pacific Command's Standing Joint Forces Headquarters participates in Exercise Vital Prospect with the Australian Defense Force
- 42 Training Navy Employees to Protect Data at Home and on the Road**
- 44 ShipShape - Interview with Lt. Cmdr. Jim McGowan**
Nutrition Programs Manager
ShipShape is the BUMED-approved weight management program for active duty Sailors. Put down that PDA and get moving!

- 46 Investing in the Navy's Future
CVN 21 - the Navy's 21st century aircraft carrier program
- 48 DON CIO IM/IT Conference Draws Diverse Audience
- 49 Information Warriors Train Aboard USS Tarawa
- 50 The Lazy Person's Guide to Navigating the Internet
- 53 Under the Contract



U.S. Navy Journalist 1st Class Jim Bane, Public Affairs Center, Norfolk, Va., takes notes as representatives from the French army are briefed on the features of the new U.S. Marine Combat Operation Center during Exercise Combined Endeavor 2006 at Bauholder, Germany May 12, 2006. Combined Endeavor, a U.S. European Command sponsored multinational exercise representing 41 partner nations, is the largest security cooperation and communications and information system military exercise in the world. U.S. Air Force photo by Airman 1st Class Josie Kemp.



Sailors onboard USS Bonhomme Richard, in San Diego, test systems in the Joint Operations Center in preparation for Trident Warrior 06. TW 06 is the primary FORCEnet Sea Trial exercise. Photo by IS1 Daryl Nicholson.

Save the date! The next Department of the Navy Information Management/Information Technology (IM/IT) Conference is scheduled for Jan. 30 to Feb. 2, 2007, in San Diego, Calif.

Check the DON Chief Information Officer Web site (www.doncio.navy.mil) in the upcoming months for more information.

Features

6
JTRS – Reloaded
JTRS Joint Program Executive Officer Dennis Bauman maps out the strategy for "reloading" JTRS to deliver software-programmable radios that will transform communications for troops on the ground, sea and in the air



10
Interview with Second Fleet Deputy Commander Rear Adm. David O. Anderson
Rear Adm. Anderson talks about the Navy's participation in JEFX 06 and Second Fleet's new maritime operations center



16
Interview with DLA Director Vice Adm. Keith Lippert
Vice Adm. Lippert discusses DLA's initiative to replace critical legacy systems with an ERP solution and best commercial practices



21
N-STAR — Naval Research and Technology for America's Readiness
The Office of Naval Research is leading the Department of the Navy's quest for the next generation of scientists and engineers to serve in the Navy's warfare centers and labs through scholarship programs, science fairs and much more



Editor's Notebook

Due to a schedule conflict, I missed covering the exciting Trident Warrior 2006 series of experiments conducted June 16 through 26 off the southern coast of California and in the Pacific operating area aboard the USS Bonhomme Richard. Previous Trident Warrior exercises focused primarily on optimizing military communications in the fleet and interoperability capability for coalition forces on multiple networks. However, this year's TW also demonstrated a FORCENet "Information Bridge" that allows naval and interagency emergency first responders to exchange information on a near real-time basis.

Participants in this first responder command and control team included Sailors, Marines and Coast Guardsmen along with the California Governor's Office of Emergency Services and several local municipalities. TW 06 provided a tool for all the participants to coordinate data sharing with federal, state and local participants, a capability deficiency revealed during Hurricane Katrina.

"The benefits to our nation's capability to organize and respond to a crisis will be immediate from the work done during Trident Warrior 2006," said Cmdr. Tony Parrillo, director of the exercise. "We have already been tasked to integrate several of our procedures and technologies to help the East Coast prepare for the 2006 hurricane season."

TW06 is not an isolated event. There is ongoing work across the Department of the Navy and Defense Department to share information and work seamlessly with coalition partners, humanitarian organizations, local, state and federal government agencies — and international agencies. The need is paramount, and DON and DoD leadership are committed to breaking down barriers to information sharing. From "Combined Endeavor" to "Communicating from the field with the Australian Army," you can read about some of these strategic initiatives in this issue of *CHIPS*.

Joint Staff Director for Command, Control, Communications and Computer Systems (J6) Lt. Gen. Robert Shea recently said, "We are moving from the need to know — to the need to share."

Let's do our part to be part of this transformation.

Welcome new subscribers!

Sharon Anderson



FC2 Rhodeback troubleshoots the Knowledge Wall system with FC3 Wilson, FC3 Tripp and FC3 Stevens onboard USS Bonhomme Richard (LHD 6), in San Diego, Calif., in the Joint Operations Center in preparation for Trident Warrior 06. TW 06 is the primary FORCENet Sea Trial exercise, co-sponsored by Naval Network Warfare Command and Space and Naval Warfare Systems Command. It exploits advanced technology concepts to provide the warfighter with information superiority over an adversary for superior decision-making and execution capability in the battlespace. Photo by IS1 Daryl Nicholson.



French Army Sgt. Cedric Marquet and Adjudantochef Stephane Garnung strip cables for telephone connection with Spanish forces during Combined Endeavor 2006 on Lager Aulenbach in Baumholder, Germany, May 13, 2006. U.S. Air Force photo by Airman 1st Class Josie Kemp.

Left, Ramona Waters of U.S. Joint Forces Command Joint Experimentation Directorate and Cmdr. John Hearne from Naval Network Warfare Command at the DON IM and IT Conference May 2006 in Hampton, Va. Heane led a discussion titled "Knowledge Management Fleet Perspective" during the conference. Go to page 48 for more information about the conference. Go to the DON Chief Information Officer Web site at www.doncio.navy.mil to download DON IM and IT Conference presentations.



Transformation at Home and Abroad

A recent Wall Street Journal article pointed out that “idea life cycles are shrinking. From the 1950s to the 1970s, it typically took more than a decade for interest in an idea, measured by press mentions, to peak. By the 1990s, that interval had shrunk to fewer than three years.”

The article served as a pointed reminder that the time available to us to successfully implement information technology (IT) solutions and embrace new ideas is constrained by:

- The ever increasing pace of new technology development
- The time available to garner senior leadership support in an environment where military personnel and political appointees have relatively short tenures, and
- The apparently short attention span that we have as a society for new management theories and ideas.

If we are emotionally and organizationally prepared to take advantage of new approaches and work toward truly meaningful change, opportunities abound across the Navy and Marine Corps team.

The Quadrennial Defense Review (QDR) provides a wonderful leverage point to adapt dramatic improvements in information management. The QDR includes a clean focus on making organizations more “horizontal,” moving to portfolio management processes, creating common data structures, providing access to authoritative information sources, emphasizing the flow of knowledge and aligning to enterprise-wide solutions.

The day-to-day application of Lean Six Sigma is another path to implement important process changes and improvements. The Secretary of the Navy has made clear his commitment that Lean Six Sigma be embraced across the Department, and has repeatedly pointed out how its adoption will (1) improve efficiency, (2) improve quality, (3) improve safety, and (4) increase employee satisfaction.

As IT professionals, we are called to champion these change opportunities. The successful use of information management and IT to improve our warfighting and support processes has never been more important. Around the world, in challenging environments, the importance of successful information leadership is viewed as crucial to an organization’s success. Even in Iraq, where the new government has such a daunting imperative to rebuild the nation, the use of IT is recognized as a crucial enabler.

Recently, I have had the honor to work with U.S. Air Force Brig. Gen. Gary Connor and his team from the Multi-National Force-Iraq in their support to the Iraqi government in implementing a successful IT governance structure and implementation plan. Similar efforts are ongoing in Afghanistan and other nations dealing with complex rebuilding efforts. These governments share a recognition that “getting IT right” is worth a significant commitment of time and personal effort.

The imperative is no less urgent here, as we work to achieve the transformational vision of our Secretary of the Navy, Chief of Naval Operations and Commandant of the Marine Corps.

Dave Wennergren



DEPARTMENT OF THE NAVY - CHIEF INFORMATION OFFICER
W W W . D O N C I O . N A V Y . M I L

The Joint Tactical Radio System – Reloaded

The Joint Program Executive Officer Joint Tactical Radio System (JPEO JTRS) outlines an incremental approach to build software-programmable radios that will transform communication capabilities for troops on the ground, sea and in the air ...

By Sharon Anderson and Steven A. Davis

Dennis Bauman, JPEO JTRS, has the chartered financial, technical and directive authority to oversee development of JTRS through low rate initial production. He is the only Joint PEO that reports directly to a senior decision-maker in the Office of the Secretary of Defense; Bauman's boss is Ken Krieg, the Under Secretary of Defense for Acquisition, Technology and Logistics.

Bauman is using this authority to deliver JTRS communications capabilities to the warfighter at realistic cost, schedule and technical risk.

It should also be noted that Bauman is "dual-hatted." He is the Navy's PEO for Command, Control, Communications, Computers, Intelligence and Space programs.

Four Goals

"Reloading" JTRS is all about completing four strategic goals Bauman set for the program last spring: (1) Assess the status of the total program; (2) Develop and gain approval for realistic requirements and a budget going forward; (3) Implement an acquisition strategy to achieve the requirements within budget and; (4) Create an enduring "joint" organization that balances Service equities with DoD enterprise needs.

The JPEO's priority was to complete the first two goals in the

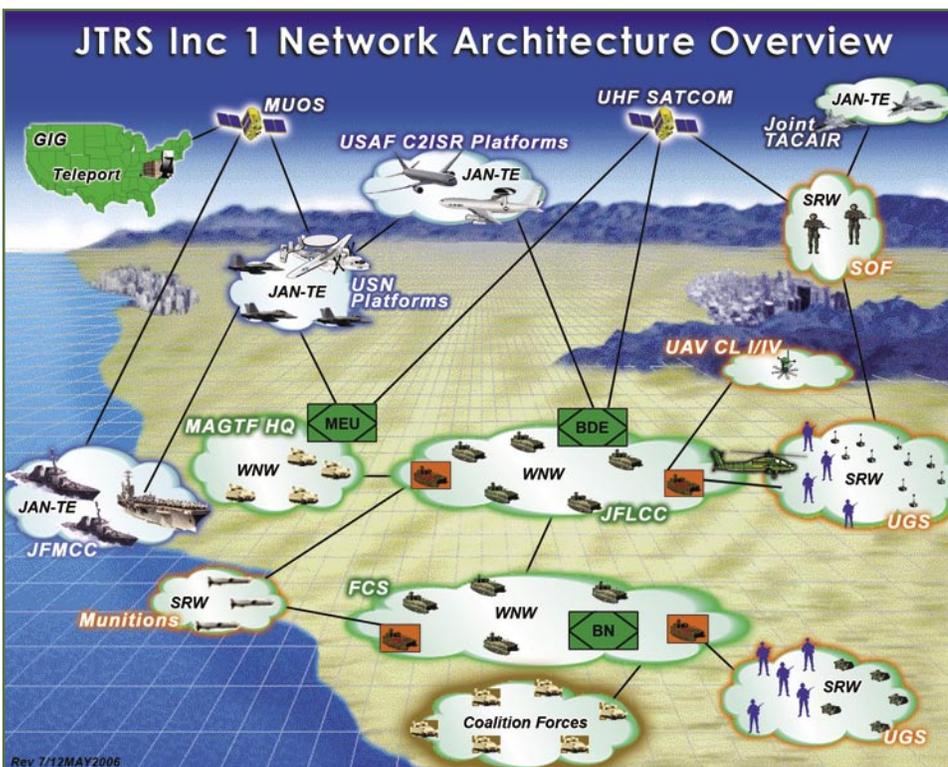
first year. Appointed JPEO in March 2005, he completed the second goal by mid-March 2006 with a Joint Requirements Oversight Council Memo signed by the Vice Chairman of the Joint Chiefs of Staff. The memo "locks in" — sets — realistic requirements funded in the President's FY 2007 Budget.

Bauman continues to move aggressively to complete the final two goals for the program. Under Secretary Krieg signed direction at the end of March 2006 approving the "Increment 1" development strategy for JTRS. Increment 1 is a significant change to an earlier acquisition strategy plagued by reported "requirements creep." Increment 1 reduces from 32 to 9 the number of waveforms for JTRS radios. It also reduces from 26 to 13 the number of form factors, and reduces the number of channels in some form factors.

Dennis Bauman on "What is JTRS? Why is it important?"

The transformational efforts of DoD's architecture depends on the information infrastructure called the Global Information Grid (GIG). Without a capability like JTRS, the GIG's transformational networking would halt at the command center level, unable to extend to the actual mobile warfighters. Figure 1 illustrates JTRS Increment 1 Network Architecture Overview.

JTRS is critical to serving as the last tactical mile connecting the warfighter on the ground into the networking capabilities that are delivered through the GIG. Under the newly revised requirements, budget, and schedule established for the program, JTRS will provide the mobile, ad hoc networking capability that is essential to realizing DoD's transformational goals for the warfighter.



"Neither the JPEO nor the DoD has given up on the full set of requirements for JTRS. Increment 1 is what we're going to deliver with the funding in the FY 2007 President's Budget, understanding that there will be subsequent Increments delivered later," Bauman said.

Lastly, Bauman is proposing a governance, or decision-making model, to create and sustain a truly joint organization. The goal is to address individual Service requirements for mobile ad hoc networking with an enterprise approach to acquisition and engineering practices that would enable effective leveraging of efforts across the JTRS product lines.

The governance model is moving forward. Under Secretary Krieg testified to the House and Senate Armed Services Committees April 5, 2006, citing JTRS as the pilot program he will use to streamline the decision-making process for

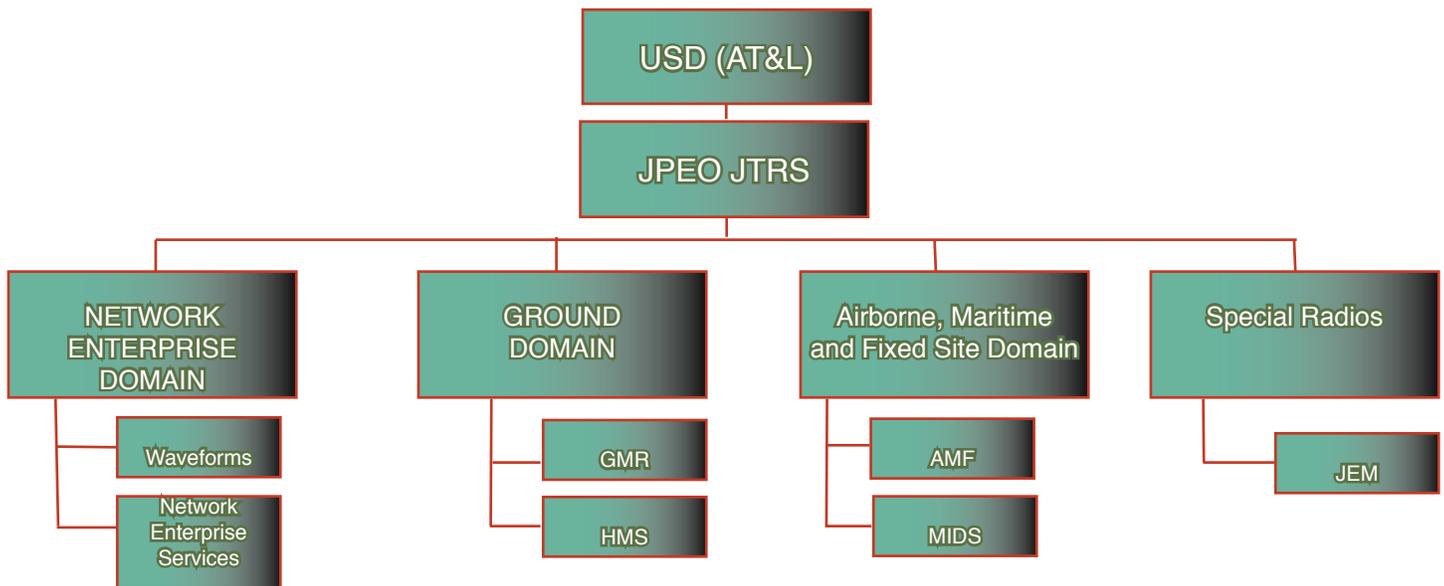


Figure 2. JTRS Organizational Structure

major weapons programs. The February 2006 Quadrennial Defense Review Report highlighted how the JTRS restructuring exemplified a collaborative approach between the joint warfighter acquisition and resource communities. The Report called for other joint programs to follow this collaborative approach.

Assessing the Status of the Total JTRS Program

In April 2005, the Joint Program Executive Officer technical and engineering staff began an assessment of the program with an extensive group of independent subject matter experts to take a close look at the JTRS product lines. The JPEO's major findings indicated that the program's requirements had fundamentally changed.

"When JTRS started, it was to be a legacy radio replacement program. Over time it had changed into a mobile, ad hoc networking capability to accomplish DoD's transformational goals. The requirements changed significantly without a corresponding adjustment in the budget or the acquisition strategy," Bauman explained.

Secondly, there were information assurance challenges when transitioning from legacy radio replacement to a mobile networking capability. The National Security Agency (NSA) took a closer look at the vulnerabilities of mobile, ad hoc networking in a mobile ground unit, which had the potential to fall into the hands of an adversary.

The NSA recommended signifi-

cant changes to the security vulnerability requirements of the architecture. Unfortunately, these recommended changes for mitigating vulnerabilities increased cost and schedule. Contractors had already delivered engineering development models under architecture requirements that differed from the NSA recommendations.

In July 2005, the JPEO reported to senior DoD leadership the research and development price tag alone for the current JTRS program would total \$6 billion.

"That was an unacceptable high cost to the DoD leadership, and they directed us to complete capability trade-offs over August. We needed to deliver on meaningful warfighter requirements. However, we needed to deliver capability with moderate cost, schedule and technical risk," Bauman said.

Setting Requirements and a Realistic Budget

The JPEO, working with the Joint Staff, provided a number of trade-offs in 14 functional areas across all JTRS radios and waveforms. The Joint Staff, working as liaison with the Combatant Commanders, relayed how much trade space could be "negotiated" within each functional area.

In August 2005, the JPEO teamed with the Joint Staff, Services, NSA, JTRS program managers, and the OSD staff, to meet the Services' most pressing needs for networking capabilities with affordable options using trade space. The result of that collaboration was an agreed-to set of options for the JTRS program.

There was also consensus on threshold JTRS requirements, the highest priorities for the Services, for developing and fielding an initial mobile ad hoc networking capability.

In November 2005, Bauman briefed senior DoD leadership on the set of options for the JTRS program. The DoD leadership selected the option to develop transformational waveforms with selected Service high-priority legacy waveforms.

What is a waveform?
A waveform is the entire set of radio and/or communications functions that occur from the user input to the radio frequency output and vice versa. JTRS waveform implementation consists of a Waveform Application Code, Radio Set Devices and Radio System Applications.
 Originally, there were 32 JTRS waveforms which have since been reduced to the following 9.

- Wideband Networking Waveform (WNW)
- Soldier Radio Waveform (SRW)
- Joint Airborne Networking-Tactical Edge (JAN-TE)
- Mobile User Objective System (MUOS)
- SINCGARS
- Link-16
- EPLRS
- High Frequency (HF)
- UHF SATCOM

The FY 2007 President's Budget funds this \$4 billion development option for transformational network capabilities and Service high-priority waveforms, including the Wideband Networking Waveform, Soldier Radio Waveform, and Joint Airborne Networking-Tactical Edge.

Strategy to Achieve Requirements Within Budget

Implementing an acquisition strategy at the JPEO level means overseeing program execution in FY 2006 and a near-term execution strategy for FY 2007. The JPEO wants to tie both to an underlying business philosophy to execute the JTRS program with an enterprise approach that has four key elements:

✓ **Government Purpose Rights (GPR):** This is GPR for enterprise elements such as software, enabling reuse and application across the JTRS product lines. A key part of the GPR approach is use of the JTRS Information Repository that provides a "home" for posting application program interfaces (APIs); GPR source code; and documentation and models associated with JTRS software products.

The goal is to have the artifacts mentioned above available for use by other JTRS programs. The Repository will be available to industry vendors to maximize code reuse and portability. Currently, there are more than 3.5 million lines of code in the Repository, including 15 waveforms and two operating environments/core frameworks. The Repository is absolutely vital as the program focuses more intensely on interoperability across the respective warfighting domains.

✓ **Open Systems Architecture Approach:** This approach focuses on an overarching systems engineering model that will direct the performance, design specifications and standards for operation of the system. This includes enterprise-wide networking and an information assurance architecture where feasible.

The JPEO is pursuing an open systems architecture based on the Software Communications Architecture (SCA) that includes a set of defined JTRS APIs.

What is a form factor?

A form factor is the linear dimensions and configuration of a device, as distinguished from other measures of size.

The initial 26 form factors were reduced to the following 13.

- Ground Mobile Radio (GMR)
- Multifunctional Information Distribution System for JTRS (MIDS-J)
- Manpack
- Handheld
- Airborne, Maritime and Fixed Site Small Airborne (AMF-SA)
- AMF-MF (Maritime/Fixed Site)
- Small Form Factor A&H (for Intelligent Munitions Systems and Unattended Ground Sensors in the Future Combat System)
- SFF B, C and I (for Ground Soldier Systems)
- SFF D (for Aerial Systems)
- SFF J (for Networked Missile Launcher System in FCS)

✓ **Moderate- to Low-Risk Acquisition Programs:** One of the fundamental tenets of the JTRS restructure was to ensure program managers moved their respective programs from high to at least moderate risk, employing an incremental development approach. This also includes more stringent oversight of program costs, and frequently scheduled assessments of technical and schedule risks.

✓ **Broaden Industry Involvement and Maximize Competition:** Throughout the JTRS restructure the JPEO organization actively looked, and continues to look at existing technology to leverage commercial-off-the-shelf and government-off-the-shelf opportunities where appropriate. This encourages new ideas and technologies from a diverse set of industry sources.

Creating an Enduring Joint Organization that Balances Service Equities with DoD Enterprise Needs

The March 31, 2006, acquisition decision memorandum signed by Under Secretary Krieg contributes significantly to the JPEO's goal for a lasting joint organization. The memorandum directs replacing the former "Clusters" that had become separate disjointed programs with the centrally managed domain program management offices illustrated in Figure 2. The plan structure is comprised of three JTRS domains shown in Table 1.

"This new organizational approach gets us away from the original Service-centric approach to developing this joint capability, facilitating a more enterprise approach to things like systems engineering, common service implementations and gateways that cut across the warfighting domains. This organizational construct will increase our ability to effectively and efficiently develop and field joint capability and provides the basis for effective resource management and governance processes," Bauman explained.

In terms of joint resource management, the Joint Program Executive Officer is centrally managing the RDT&E efforts for the JTRS enterprise in the outyears – FY 2007 and beyond. Once the JTRS program funding plan is approved, JPEO has full control

Table 1. The JTRS Domains

Ground Domain	Ground Mobile Radio (GMR) (formerly Cluster 1) - Support requirements for Army and Marine Corps Ground Vehicular platforms Handheld/Manpack/Small Form Factor (HMS) (formerly Cluster 5) - Support requirements for JTRS handheld and manpack units and forms suitable for integration into platforms requiring a Small Form Fit radio
Airborne, Maritime and Fixed Domain	Airborne, Maritime and Fixed Site (AMF) - Support requirements for airborne (including rotary wing), maritime and fixed station platforms for all Services Multifunctional Information Distribution System–JTRS (MIDS-J) - Migrate the current MIDS-Low Volume Terminal to MIDS-JTRS compliance producing the next generation data link and communication terminal for joint and coalition tactical platforms
Network Enterprise Domain	Waveform Program Office - Responsible for waveform development, cryptographic equipment applications, architectural integrity of JTRS, gateways and common network services
Special Radio Systems	JTRS Enhanced Multi-Band, Inter/Intra Team Radio (MIBTR) (formerly Cluster 2) - Managed by Special Operations Command - Support requirements for handheld radios for the Army, Navy, Marine Corps and Air Force Special Operations Forces

of those funds in the year of execution. This allows the JPEO to address funding priorities within the enterprise to the greatest extent possible and better support individual program stability.

“Going forward in FY 2007, my office will directly receive the total JTRS RDT&E allocation from the Army Budget Office under a single program element. I then will be empowered to oversee execution, providing me with instantaneous visibility into fiscal status for all JTRS developmental efforts. Again, this streamlined resource management process is vital while managing enterprise efforts across the Services and warfighting domains,” Bauman elaborated.

The authority and responsibility for the procurement and sustainment of software-programmable radios reside with the individual Services who will determine unit quantities. Quantities will not be finalized until the results of the Program Objective Memorandum for 2008 are released and the Services’ input into the Future Years Defense Program are known. In the meantime, a detailed independent unit cost estimate is currently being conducted.

In addition to effective resource management processes, the JPEO is charting an innovative approach to program governance. “DoD has come under some scrutiny as of late in terms of how we, as a DoD enterprise, manage our acquisition programs,” Bauman said.

The Defense Acquisition Performance Assessment report, the Quadrennial Defense Review, various Government Accountability Office reports, as well as an independent JTRS assessment conducted by the former Air Force Chief of Staff Gen. Larry Welch earlier this year, have all highlighted the concerns with respect to the defense systems acquisition process and its inability to effectively control costs and deliver capability on schedule.

“Last summer, Secretary Krieg challenged me to come up with some ideas on how we can more effectively govern and manage joint programs. We did some in-depth studies; we looked hard at the lessons learned in earlier reports and presented a revised governance process to senior DoD leadership in February 2006. As part of our recommendations, we advocated using JTRS as a pilot for a revised governance process,” Bauman explained.

The JPEO provided DoD senior leadership with core principles and key attributes that support a more streamlined approach to joint program governance. These principles and attributes are based on proven corporate models that drive industry.

In principle, executives must have freedom to responsibly drive the enterprise forward to meet the strategic direction. Overly burdensome restraints to this freedom have a high potential to negatively impact schedule, cost and risk. In accordance with their chartered responsibilities, executives need to be empowered to aggressively execute to agreed-to requirements. The governance process must also provide for effective accountability commensurate with the degree of executive freedom exercised.

An optimum governance process must be able to make the quick

decisions while balancing enterprise and stakeholder equities against the strategic direction. Effective oversight is achieved through effective communications and collaboration, resulting in an agile, efficient, and less onerous process.

“The streamlined process I proposed should increase the speed of decision making while still honoring the interests of the various stakeholders — in effect, it empowers a true Joint Program Executive Officer as intended. More importantly, it gets the right capability at the right time into the hands of our warfighters,” Bauman concluded.

The JTRS governance process, though approved by DoD senior leadership, is not “written in stone” nor will it be applied to every joint program. “Based on some of the feedback from our stakeholders, we are working some of the details of the process,” Bauman added.

JTRS and the Army’s Future Combat System

JTRS will provide the Army warfighter with new, secure capabilities, which include the transmission and receipt of real-time information through voice and text, as well as the ability to stream live video/audio, draw/share maps, and allow video/audio conferencing.

The revised JTRS strategy fully supports the fielding of the GMR and HMS radios and their fit into the Army’s Future Combat System. The FCS is an integrated suite of technology components that are part of the Army’s transformational process to become a lighter, more agile force. The technology components will be dependent on JTRS for mobile networking, which is essential to the success of FCS.

The JPEO is taking an enterprise approach with FCS, adopting a moderate risk posture and specific business philosophies about government purpose rights of the software and competition in production on the hardware.

“We are synchronizing our program with the FCS and meeting the schedules that the Army has for Spinout 1, which is the first implementation of FCS. We consulted the Army and the FCS program. When I say ‘we,’ I am really talking about the big ‘We’ that includes the Joint Chiefs of Staff, Joint Staff Director for Command, Control and Communications, and the Joint Staff Director for Force Structure, Resources and Assessment. The Army and the FCS staffs have been an integral part of defining the requirements for Increment 1,” Bauman said.

“We talk weekly, if not daily, with Maj. Gen. Charles Cartwright, Program Manager Future Combat Systems, who is my counterpart on FCS, and we have people collocated between our two programs working this very closely because we recognize the key dependency of FCS on the JTRS program,” Bauman added.



For more information about the JPEO JTRS, go to the Space and Naval Warfare Systems Command (SPAWAR) Web site at <http://spawar.navy.mil> and click on the JPEO JTRS program seal. CHIPS

Interview with Deputy Commander U.S. Second Fleet R

CHIPS asked Deputy Commander, U.S. Second Fleet, Rear Adm. David O. Anderson to explain the importance of the Navy's participation in the Joint Expeditionary Force Experiment 2006 (JEFX 06) and Second Fleet's recently created Maritime Operations Center during a tour of the MOC April 24, 2006.

Rear Adm. Anderson: First of all, Second Fleet has been working hard, at least the last two years, to get more integrated not only into the joint world with the other Services, but also with our coalition and NATO partners worldwide, and most importantly with the interagency piece. In the last six to nine months we have started getting some incredible traction.

We realize that 2nd Fleet has a key role in the security of the nation as we develop a joint, coalition and interagency solution to the maritime challenges of homeland defense. To that end, we have stood-up our Maritime Operations Center - Experimental (MOC-X) as a viable and relevant warfighting capability to rapidly field and test both equipment and tasks that can then be replicated in all the numbered fleet MOCs.

JEFX is an exercise that is providing us a venue to work through some of the operational level planning challenges as well as highlighting the tactical TTPs (tactics, techniques and procedures) and CONOPS (concept of operations) of working with other Services and agencies. The end result will be another major step toward the Chief of Naval Operations' goals for maritime domain awareness.

In the last couple of weeks, we have had several of the numbered fleet commanders visit 2nd Fleet. We want to make sure as we model new processes and capabilities within Navy, we share best practices so all of our Maritime Operations Centers develop in parallel. We are extremely focused in our efforts to not be working in a 'stove-pipe' but to constantly be communicating with other commands working similar issues.

Probably the most important aspect of exercises like JEFX 06 is what we do with lessons learned after the exercise. Or simply put, 'so what?' Take for example Maritime Dynamic Targeting. In the past, we have seen both gaps and overlaps between maritime, land and air components. This is extremely evident in the Time Sensitive Targeting cell of the JFACC (Joint Force Air Component Commander).

As all components are continually developing faster and more lethal capabilities, we need a way to update the processes we use to prosecute these targets. This exercise has allowed us to work real world, challenging scenarios to define for all components the best practices to effectively and efficiently prosecute these targets.

CHIPS: *What is Maritime Dynamic Targeting?*



Deputy Commander, U.S. Second Fleet, Rear Adm. David O. Anderson in the MOC April 24, 2006.

Rear Adm. Anderson: Maritime Dynamic Targeting is the process of prosecuting a time-sensitive target in the maritime environment. Navy has done this for years, but now we are working to do it in the joint arena where the JFACC and JFLCC (Joint Force Land Component Commander) have visibility on what we're doing. This is extremely important due to the command and control of who owns the assets available to strike, and who is controlling those assets when you need them.

When we see a new target pop up, do we have the processes and relationships built to immediately identify and prosecute it with the best platform available and in concert with the JTF (Joint Task Force) commander's desired effects? Do we have the common TTPs of all components to work together in each other's area of responsibility to do so as efficiently as possible? These are some of the things exercises like this give us.

CHIPS: *You mention coalition and other agencies a good bit. Why is it so important that the Navy works with them in the maritime domain?*

Rear Adm. Anderson: You have heard the CNO talk about a 1,000 ship Navy. What does that mean? Does it mean he wants to have 1,000 ships in the U.S. Navy painted gray with U.S. Sailors on them? Not at all. What we want to be able to do is build an operating maritime picture that is worldwide using coalition and joint partners so that whoever has the sensor, whoever identifies the ship, can then put it all into one truly worldwide common operating picture that we can tap into.

For instance, the U.S. Coast Guard has a fantastic picture of the maritime domain out to about 12 miles. We have worked with them to develop our common operating picture to include all they offer. What we are endeavoring to do now is to make sure we are not playing what we call the 'catcher's mitt.' If something bad is coming into this country on a ship, whether it is off the

Rear Admiral David O. Anderson

coast here in Norfolk, in Hawaii or anywhere else — we want to know about it long before it gets that close. This requires that we fuse our intelligence and sensors with many other agencies and countries worldwide, so we know before it is actually loaded on the ship.

Federal agencies and all the Services have been working on this. The lane where 2nd Fleet has responsibility, working for U.S. Northern Command through U. S. Fleet Forces Command, is where we are concentrating our efforts. Those efforts have included building new relationships outside of DoD.

Vice Adm. Mark Fitzgerald, Commander, Second Fleet, now has written memorandums of understanding or direct liaison with the State Department, FBI and NCIS (Naval Criminal Investigative Service). We do a lot bilaterally with the United Kingdom and Canada.

This has allowed us to develop many new ways of identifying and solving problems and then sharing them within Navy lifelines with the other numbered fleets as well as with many other organizations outside of the Navy.

CHIPS: How do you operate with first-responders like state and local agencies where these personnel don't report to the military?

Rear Adm. Anderson: Here in Tidewater we have several different city municipalities that each has a maritime police capability. At the Joint Harbor Operations Center (JHOC) that the Coast Guard runs in Hampton Roads, they are constantly working to solve command and control issues like you describe. If a suspect ship is observed by the Norfolk Police Department, the Norfolk Police know who they report to and what to expect. The same is true for Virginia Beach and all the others.

This gives the visibility needed to ensure every agency knows what it is expected to do, who is in control, and then allows the Coast Guard to coordinate efforts. This is something that is happening right now.

CHIPS: How has Second Fleet's mission changed in the last few years to help fight the war on terror?

Rear Adm. Anderson: Second Fleet has four major objectives. The first one is certification for all the carrier strike groups, surface strike groups and expeditionary strike groups before they are deployed. We don't train them anymore. We have subordinate commands that do their training. However, Vice Adm. Fitzgerald is the final authority to certify a CSG, SSG or ESG as combat ready. That's still our bread and butter.

The second mission objective we have is to be able to have our staff function as a Joint Task Force commander. The third one is to be the Joint Force Maritime Component Commander (JFMCC) much like you saw with Hurricane Katrina. Katrina gave us a chance to validate the new staff structure we had to develop to be able to serve these new mission objectives of JTF or JFMCC.

This new command structure is what we call a distributed staff. We have a small portion of our staff that is trained, manned and equipped to forward deploy at any time. Then through reach-back, we can increase our work capacity by having portions of the required work completed by the bulk of our staff that remains in the headquarters. We are constantly developing the skill sets our people need to effectively operate this way and improving the hardware needed to support them.

The fourth major objective for Second Fleet is in our NATO command, the Combined Joint Operations from the Sea Center of Excellence that we stood up last year.

CHIPS: What about the federal agencies that can't work on our networks, like SIPRNET, because of the security classification requirement. What will be the communication method?

Rear Adm. Anderson: I will give you two answers to that. First of all, the Joint Interagency Task Force South (JIATF-S) in Key West, Fla., has been up and running for a number of years, primarily focusing on the drug trade. You will have a watchfloor, like in our MOC, with an FBI agent seated next to a CIA agent, seated next to a Navy officer, who is seated next to a Coast Guardsman, seated next to an Airman seated next to a Dutch officer — and they are all internally set up on their own equivalent of SIPRNET.

Let's say that I want to see data in the FBI agent's database, which may entail opening an active criminal investigation in our country. There are serious reasons the FBI would not want me to have access to that system, just like we have reasons that we don't want people to be able to get into SIPRNET.

What JIATF-S has done is establish the protocols they need to be able to share only the needed information. We may not have complete visibility to their entire database, but we can glean out what we need at any time. That's one way we are going about it.

We have also started working creative ways to cordon off portions of SIPRNET and to make more systems interoperable. NETWARCOM (Naval Network Warfare Command) has been working very hard to help provide us the tools we need to meet our operational requirement and yet still ensure we have the proper level of security in our systems.

Let me give you an example. Last year, the USS Theodore Roosevelt (CVN 71) Strike Group had a Spanish ship in their battle group. During their Joint Task Force Exercise (JTFE), we invited a rear admiral from the UK to come over with his entire staff and serve as our JFMCC.

So, we had a U.S. JTF Commander, Vice Adm. Fitzgerald embarked on USS Iwo Jima (LHD 7), with a UK two-star serving as the JFMCC in our headquarters in Norfolk, tasking the CSG commander onboard Theodore Roosevelt, who had, as one of the key ships in his command, a Spanish ship. We had four different systems on live chat, and all were able to communicate throughout the exercise.

By Sharon Anderson

I went down to the British commodore's stateroom on USS Iwo Jima one evening because he came to my stateroom and said, 'You have to come see this!' He had four screens up with live chat going from us aboard Iwo Jima to the UK commander in Norfolk on this releasable SIPRNET, down to the Theodore Roosevelt Strike Group, over to the Spanish ship Alvaro de Bazán (F101). We were doing live chat for four different systems all at one time.

Those are some of the things that NETWARCOM has helped us work through. A lot of the time, the problem is not hardware but specific protocols and getting the authority to interoperate.

Are we there yet? No. Have we identified where we need to get to? Yes, we have. And we are getting there a lot faster than anybody anticipated at this point. All players, whether it is FBI, whether it is the State Department, the UK as a NATO partner, whether it is the Spanish government as a coalition partner — everybody understands — and everybody is trying to move toward that.

We just have to continue to adapt and do the hard detail work. But it is work that is making our country a safer place everyday.

CHIPS: Is there any final comment you would like to leave us with today?

Rear Adm. Anderson: I firmly believe that one of the most important things we have to get better at across not only DoD, but all of the other agencies, is explaining to the American people what we are doing to make their military more effective in the 'Long War' that is GWOT (global war on terror). How we are making America a safer place.

The Goldwater-Nichols Act was designed to make DoD become joint and interoperable. The operations in Grenada proved to us years ago that the Services didn't even have radios that could talk to each other. We have matured dramatically since those days and are indeed interoperable today.

Interoperable is nothing more than ensuring my people and equipment works with your people and equipment. This is important, but it is not good enough any more. We need to get to the point where we are truly interdependent, which means I cannot do my job without you, and you cannot do your job without me.

This level of coordination demands trust and an in-depth understanding of every players' strengths and weaknesses. We need to get to this point not only within DoD, but within the other government agencies as well. What you are going to see here today is how Second Fleet is making this concept a reality today. *CHIPS*

For more information about U.S. Second Fleet, go to <http://www.secondfleet.navy.mil/>.

The Joint Expeditionary Force Experiment 2006 is the sixth in a series of U.S. Air Force biennial highly focused, multinational, multi-Service military experiments. JEFX supports multi-functional exploration, spiral development and rigorous assessment of initiatives in the areas of command and control, space, information management, combat forces, mobility, combat and logistics support, and homeland defense. The Main Experiment (MAINEX) executed April 18-28, 2006.

JEFX 06 is the first experiment to leverage the integration efforts of experimentation and link them directly with test and evaluation to prepare the Combined Air and Space Operations Center (CAOC) weapon system for expedited operational fielding.

The goals for this experiment are to better integrate CAOC processes, expand the use of data links, extend networks linking operational and tactical levels of execution, and improve coordination processes for collecting, fusing and disseminating information in support of homeland security and defense.

"JEFX 06 is a true experiment. It is Air Force directed," said Second Fleet science adviser, Tom Forbes. "Navy plays in JEFX to interoperate, to be interdependent with the Air Force on the same operational level. We experiment with the latest and greatest in technology. We take away lessons learned, and we make recommendations as to what to do with the 'so what' after we have finished with the experiment and the analysis work. Do we accelerate production or do we let it mature more in the laboratories and industry floors before we turn it over to the warfighters?"

The Navy portion of JEFX 06 is sponsored and led by the Naval Network Warfare Command (NETWARCOM), the operational agent for the Navy's FORCENet program under Sea Power 21. Second Fleet is the overall fleet lead for JEFX 06.

STIMS

The Navy Warfare Development Command (NWDC) coordinates the Sea Trial component of the Sea Power 21 vision, the Navy's experimentation program. The Sea Trial Information Management System (STIMS) for concept development and experimentation, developed by the NWDC, is an interactive, secure database located on the NWDC SIPRNET Web site (nwdc.navy.mil/stims). STIMS serves as the central library of initiatives, events and projects to manage Sea Trial events and related activities, as well as to support cataloging all experimentation.

After the experiment, the evaluation process includes the appropriate Fleet Collaborative Team, the operational agent, and ultimately the Sea Trial Executive Steering Group. STIMS is also the repository of analysis and assessment documents that are linked to Sea Trial experimentation proposals and initiatives.

The Experiments

Each of the Navy's four JEFX 06 initiatives has its own STIMS unique identifier, Forbes explained. The objective of STIMS No.

Get Lead in Joint Expeditionary Force Experiment 2006



Tom Forbes, Second Fleet science adviser.

2042, Global Hawk Maritime Demonstrator (GHMD)/Maritime Domain Awareness (MDA), is to explore the processes, procedures, systems and time lines for GHMD to support and provide maritime operational and intelligence data to maritime homeland security/maritime homeland defense (MHLS/MHLD) nodes across military components in support of specific maritime domain awareness surveillance requirements.

The GHMD system will also be used to further develop long endurance unmanned aerial vehicles (UAV) concept of operations (CONOPS) and tactics, techniques and procedures (TTP).

The Naval Air Systems Command (NAVAIR) acquired two Global Hawk aircraft as part of the GHMD project administered by the Program Executive Office for Strike Weapons and Unmanned Aviation (PEO(W)) and its subordinate Program Management Office for Unmanned Aerial Vehicles (PMA-263).

The Navy is committed to buying a high-altitude, long-endurance unmanned air system, according to Forbes. The Navy's plan is to use the unmanned air system as a surrogate for the procurement plan. The experiment used simulation testing due to delays in delivery of the first air system to the Patuxent River Naval Air Station. One test flight of about two hours duration was conducted during the experiment; however, it was not a data collection flight for purposes of the experiment.

"The first airplane will probably show up around 2012. The Air Force had already developed Global Hawk as a part of an advanced concept technology demonstration. Navy decided if we are going to buy into a program like this, a unique, revolutionary airplane that flies for a long time (a day and a half, perhaps) at high altitudes so it is not interfering with commercial aircraft, we ought to learn how to operate it before we develop the procurement program," Forbes said.

The air system consists of Synthetic Aperture Radar (SAR), Ground Moving Target Indicator (GMTI), maritime surveillance and Inverse SAR Radar. The Global Hawk came with existing Air

Force sensor software, which the Navy modified. The Air Force model was optimized for land search and surveillance. But the boundary conditions are different between land search and water search. In the land environment, the only thing that is moving is the target, but over water, the ocean surface is moving continuously, but targets do not move rapidly. ISAR records the echo signals of moving targets such as ships and displays the unique characteristics that make them different from land targets.

"We added a maritime surveillance mode for the radar maritime target acquisition that results in dots or target locations on the common operating picture. We added Inverse Synthetic Aperture Radar, known as ISAR. It is good over water because it cancels out the background of the water's movement; it only looks at the characteristics associated with ships in the ocean—pitch and roll and yaw. As the ship moves, it reveals itself and its characteristics over an ISAR picture," Forbes said.

Electronic Support Measures is essentially an electronic vacuum cleaner that sucks up electronic emissions from the targets and provides line of bearing information to the ground station. This is a unique Navy package that is in the air system. It downlinks information to the ground station called the Tactical Auxiliary Ground Station (TAGS), which is paired with the Mission Control Element (MCE) at Patuxent River, Md.

A tremendous amount of data are sorted at the TAGS, according to Forbes. Individual tracks are nominated to the Naval North Fleet East, which is Second Fleet's name in its homeland security/homeland defense role to U.S. Northern Command. Imagery from the ISAR radar and/or electro-optical or IR (infrared) sensors go to the Office of Naval Intelligence, Fleet Imagery Support Team and National Maritime Intelligence Center in Suitland, Md., where imagery analysts examine the data and provide associations between the analyzed imagery and the target.

"We pair the two together and nominate those tracks to a common operating picture, provide that to U.S. Fleet Forces Command and from there they are disseminated over the GCCS-M (Global Command and Control System – Maritime) transport path," Forbes said.

Imagery is also sent to the Coast Guard Maritime Intelligence Fusion Center located at Dam Neck, Va., which may send the picture to Coast Guard Headquarters. USNORTHCOM and the Joint Force Maritime Component Commander (JFMCC) North, which is Fleet Forces Command, provide a picture to the CAOC at Nellis Air Force Base, and up to the Pentagon.

"We are looking at how we integrate the products from that air system with other sensors and database information so that we can positively locate, characterize, identify and persistently track candidate vessels in the maritime domain," Forbes said.

The Navy is working with the Coast Guard because certain sections of Titles 10 and 14 preclude members of the Army, Navy, Air Force or Marine Corps from direct participation in law enforce-

ment activities. Some of those law enforcement activities would include interdicting vehicles, vessels and aircraft; conducting surveillance, searches, pursuit and seizures; or making arrests on behalf of civilian law enforcement authorities. The Coast Guard is not restricted from acting in this regard.

“We are looking to be able to sort the suspect vessels from all the rest and then have the ability to disseminate that information, not only among Navy stations and resources, but provide that information to interagencies, Coast Guard, FBI and other agencies that might be interested, including U.S. Customs and Border Protection,” Forbes said.

In the Maritime Dynamic Targeting (MDT), STIMS No. 2041, and Time Sensitive Targets (TST) piece, the Navy wants to develop the process by which maritime forces prosecute MDT and TST. This experiment provided the opportunity and means to focus technology development for marine command and control and targeting to speed up targeting capability. The experiment also was an opportunity for input into the development of JFMCC command and control, targeting and fires doctrine, and TTP.

Maritime Dynamic Targeting objectives include testing joint interoperability, timeliness and accuracy, and appropriateness of response. MDT demonstrated the interoperability, interdependence and connectivity between the Combined Forces Air Component Commander, the Combined Forces Commander, the Joint Task Force Commander and Second Fleet using the same software suite that the air component uses at Nellis Air Force Base, called the CAOC Common Client.

Cross component collaboration means that when the Air Force or the Navy develops a target, it becomes available for anybody to execute a strike on that target.

“For Maritime Dynamic Targeting we have developed a CONOPS, and we have refined that through spirals. We have refined the standard operating procedures to the point where we are now. It seems to be working well, so well that the Air Force has adopted the same kind of processes and procedures in its operations center at Nellis Air Force Base,” Forbes said.

Tactical IP Networks, STIMS No. 2040, and Link 16, STIMS No. 2039, presented the concept of the airborne network evolving from voice-based command and control at the operational level to a more complex network of data shared in many forms by many users. Machine to Machine (M2M) targeting using Link 16 is a legacy system that constituted the backbone of Navy experimentation in JEFX 04. Further experimentation is needed to enhance Blue Force situational awareness and improve the Navy’s ability to receive and transmit imagery and conduct Digital TST.

A desired outcome of this part of the experiment is that imagery using the J16.0 message and targeting data can be transmitted through the current infrastructure with acceptable latency and that the images are of sufficient quality to reduce the kill chain time to execute.



The Global Hawk unmanned aircraft.

Airborne Tactical Internet Protocol (Tac IP) experimentation allowed the exploration of maturing technologies that have the potential to significantly enhance information flow around the battle space. JEFX 06 employed Tactical Targeting Network Technology to investigate Tac IP networks potential use and role within net-centric operations.

“Tactical IP Network takes the ground-based, terrestrial IP networks that you are familiar with and puts them in the air. Now you have airplanes interoperating over an IP network at high bandwidth, with high data rates that we heretofore have not been able to do,” Forbes said. “Link 16 experiments with non-traditional intelligence, surveillance and reconnaissance by passing imagery back and forth.”

Anybody on the ground that has access to the IP network and the cockpit can send imagery, messages, chat or Voice-over-IP. Having received the images, the pilot can identify the target on the ground, execute a strike, take an image of the target with the on-board equipment, send it to the CAOC, and there is almost immediate results on the bomb damage. The success story here is high bandwidth in the cockpit and rapid transmission of tactical data.

“Whoever puts eyes on a target, transmits this information through the network to the CAOC. Then one or more of the applications in the MOC nominates the strike through the Battle Management Command and Control (BMC2), whether it is an E2 Hawkeye or an AWACS, and that is passed to an F-15 E1, a special aircraft made by Boeing,” Forbes said.

The Boeing F-15 E1 is special because it allows the installation of two different types of operational flight software; one is the actual release, and the other can be used for experimentation.

The Maritime Operations Center

While Forbes provided details about the experimentation, watchstanders in the MOC were participating in the exercises as events unfolded. In the cubicle marked “ISR OPS” Cmdr. Mark Hottendorf and Operations Specialist Senior Chief Kevin Albright were using IWS, or InfoWorkSpace, an interactive virtual environment that allows geographically dispersed teams to collaborate and share information in real-time.

“We use a couple of tools that are under development to update what is going on when we are trying to get approval. It could be

U.S. Air Force Maj. Jim “Irish” Kockler, from Air Combat Command, is the project officer for Maritime Dynamic Targeting testing at 2nd Fleet. He helps develop tactics, techniques and procedures.



dropping bombs on a target or denying airspace to someone, or getting ships or aircraft from one place to another,” Hottendorf said.

The software tested called WEEMC, or Web Enabled Execution Management Capability, is the interim name for a new system that will be called JADOCs-NC or Joint Automated Deep Operations Coordination System – Net Centric. It allows coordination between different levels of the command structure to agree on courses of action. When the board signals green across all levels of command, it means that the course of action has been approved and units are assigned to execute the order.

“Basically, we are concerned with the maritime component, which are the ships and the aircraft that are operating at sea. There is also a Land Component Commander, which is Army and an Air Component Commander, which is Air Force. We have cross-coordination between those component commanders, and that’s also done via this tool as well,” Hottendorf said.

Coordination across levels of command takes mere seconds, but evaluating operational options may be more complicated.

“The decision on the courses of action may take several minutes. We may have to consult with the JAG, the Judge Advocate General, concerning the rules of engagement and collateral damage estimates. Once we have discussed those courses of actions, the actual approval takes a matter of seconds,” Hottendorf said. “In this experiment we are taking some of the older doctrine and putting a new spin on it. We are developing new tactics, techniques and procedures and using these tools to help develop new doctrine.”

New technology does not drive the need for new doctrine; it only enhances it, according to Albright. “The tool helps the process go faster. The people in different areas and at Nellis are coordinating off this same tool.... It is like a relay race; someone starts off the process and then hands the baton to the next person.”

“Technology is enabling us to do things at a quicker rate, but we still need to make sure that if we do something that quickly that we do not have friendly fire, and we do the proper thing and still allow the commanders on the field to take the initiative to do



Cmdr. Mark Hottendorf (right, foreground) and OCS Kevin Albright using InfoWorkSpace, a real-time virtual environment for information sharing.

what they need to do without reaching down and micromanaging,” Hottendorf said.

JEFX consists of three spiral events, in addition to MAINEX. Spiral 1 is essentially a technology demonstration of the command and control tools or “initiatives” where warfighters can provide feedback to the developers. The developers use the feedback to modify the tools or initiatives before Spirals 2 and 3.

During Spirals 2 and 3, the warfighters, manning an operationally representative combined air operations center, use the initiatives and systems, assess them for their operational utility and submit desired changes. The ultimate aim of the experiments is to accelerate development to get capabilities into the hands of warfighters faster.

The only U.S. Air Force member in the MOC, Maj. Jim “Irish” Kockler, is the Second Fleet project officer for Maritime Dynamic Targeting. Kockler said he was excited about MDT test results.

“Things are going better than I expected. After Spiral 3, as far as the Maritime Dynamic Targeting is concerned, we accomplished what we wanted to accomplish during MAINEX the last time we got together. Now we are advancing the football down the field a little more during this MAINEX. We are doing a good job. ‘Dr.’ Forbes thinks the same way. I do not think we came into this to write a Tactical Memorandum on this process, but I think that is going to be the end result,” Kockler said.

Maj. Kockler helps 2nd Fleet develop tactics, techniques and procedures. Lessons learned during this experiment may become part of Navy doctrine, according to Kockler.

“Someone else will take our lessons learned and put those into a document. For example, Naval Warfare Development Command has written the concept of operations, and we are employing the work that they have done and are experimenting with it. They will make changes based on how we perform, and it ends up being a Navy Tactical Memo.”

CHIPS

Interview with Vice Admiral Keith Lippert

Director Defense Logistics Agency



Vice Adm. Keith Lippert

The Defense Logistics Agency (DLA) is a U.S. Department of Defense (DoD) agency. The DLA Director reports to the Under Secretary of Defense for Acquisition, Technology and Logistics through the Deputy Under Secretary of Defense (Logistics and Materiel Readiness). DLA provides worldwide logistics support for the missions of the military departments and the unified combatant commands under conditions of peace and war. It also provides logistics support to other DoD components and certain federal agencies, foreign governments, international organizations, and others as authorized.

A major initiative underway is Business Systems Modernization (BSM), a project that will replace DLA's mission critical legacy systems with a new enterprise architecture based on COTS software and best commercial practices.

For the second time in three years, DLA's Information Operations Directorate received a CIO 100 Award, presented annually by International Data Group's CIO magazine. DLA is being recognized for its eWorkplace program, a single portal for knowledge management, work processes and collaboration across the entire agency. CHIPS asked DLA Director Vice Adm. Lippert to talk about DLA's transformational technology initiatives, mission and vast customer base March 27, 2006.

CHIPS: What is the Business Systems Modernization initiative?

Vice Adm. Lippert: First, I would like to spend a moment making sure that you understand what DLA is. It is important that you put into perspective the size of the organization and mission. DLA is responsible for providing logistics support and services throughout the Department of Defense. It is a joint command, which means we have military assigned from all the military services, and we, in fact, do support all the military services.

Our total workforce is more than 20,000, of which about 500 are active duty military. Thus the largest part of our overall staffing is our civilian workforce, many of whom have a great deal of overall DoD logistics experience and a number of whom work directly with our customers.

"If we were on the Fortune 500, we would be No. 50 in sales — above the Intel Corp."

- Vice Adm. Keith Lippert

We run this agency like a business. We get very little direct appropriated funding to run DLA. We are primarily funded via the Defense Working Capital Fund, so we add a cost recovery rate, as a necessary form of 'overhead' added to the cost of the supplies that we provide, and use it to pay my salary, the other 20,000 plus civilian and military salaries, utilities, other costs to source, acquire and distribute material, and so on.

In fiscal year 2001, we were a \$17 billion corporation as reflected in our sales to our customers. This year we project to be a \$35 billion corporation. Business has doubled in five years. We're meeting the demand, providing services and support with fewer people than we had five years ago, and at a significantly reduced cost recovery rate.

We provide 95 percent of the services' repair parts, and 100 percent of the services' subsistence, fuels, medical, clothing, textiles, and

construction and barrier materials. We also run a large worldwide warehouse distribution system. We run a property disposal and re-utilization system.

We provide the Defense Logistics Information Service that catalogs all the parts used in DoD and by NATO. We run a hub at the Defense Automatic Addressing System Center that routes the vast majority of DoD's logistics transactions. We run a Defense document automation and production operation. That's just to give you an idea of some of the things that we do.

We get 54,000 requests for material a day on average. We award 8,200 contracts a day. If we were on the Fortune 500, we would be No. 50 in sales — above the Intel Corp. We have 26 worldwide distribution depots, anywhere from Korea to Kuwait. We are located in 48 states and in 28 countries.

So, when we implement something like our Business Systems Modernization, it is a major endeavor when put in our large and worldwide support context. The system that we are replacing, which we refer to as our legacy system, was designed in the 1960s. It was implemented in the 1970s, and it probably should have been replaced in the late 1980s. It is written in COBOL, and it is a dinosaur. When it was implemented, it was state-of-the-art. It still does a remarkably good job of providing worldwide support, but it does not have the functionality that we need right now.

This agency tried five different times to start projects to replace this legacy system. This is our sixth attempt — and we are going to be successful this time. The backbone of BSM's enterprise resource planning (ERP) is systems software and related embedded business processes from SAP. We use Manugistics for our demand-planning module. Overall, BSM is about a \$750 million project.

The project was started in 1999 in terms of defining the concept. We went to a live concept demonstration of much of BSM's functionality in summer 2002 with limited items and numbers of users

at first. We took 155,000 of our 5.2 million items and put them under this solution.

Prior to that concept demo, we trained people not only in the system itself but also in change management. Every employee performing inventory management related functions within DLA had used the legacy system for his or her entire professional life at DLA. During the concept demo, we took that familiar system away, and employees had to do everything differently.

We trained, and we measured progress, and after an extensive training period and selection of the first people that would use the system, we went live. The challenges were not only the change management issue, but also the fact that we were in the midst of a war and supporting warfighters around the world. We did not have a margin of error to slip. So there was added pressure to make sure that the system was effective right from the start.

While it was effective overall, we had a lot of problems to resolve in the BSM concept demo phase. Despite all our careful planning, we were much too optimistic in assuming we could bring this complex system to maturity in a three to six-month concept demo period.

It ultimately took two years to get the system stabilized and to add some additional planned functionality to it. During that two-year period it was not always clear that the light was at the end of the tunnel. Once we got past that, we started rolling out the rest of our 5.2 million items. We have about \$8 billion of our sales in this ERP solution as of April 2006. By December 2006, we will have the majority of the 5.2 million items up and operational involving \$18 billion in sales.

One of the benefits that we expect to achieve from this system is a reduction in customer wait time because the system operates on a real-time basis as opposed to the batch mode process of the legacy system. We expect to see reduced operating costs because the system is much more efficient than the legacy system associated with it. We expect to see savings in inventory because we will require less inventory. This is because of the data integrity that the system requires, and the demand forecasting and customer and supplier collaboration techniques it has.

The new system requires reorganization of related processes and functions at our Defense supply center buying activities, which we call Inventory Control Points, and changing job roles and descriptions to incorporate the best business practices of the private sector while also incorporating those best practices that remain truly unique to military logistics support.

DLA has never been able to pass a chief financial officer's compliance audit (as is true for most of the DoD). So another of the benefits that we expect to achieve is that DLA, in FY08, will be able to pass that audit for the first time. The ERP solution is a major contributor to that.

The only other thing that I would say is that if, in fact, any organization, I do not care if it is public or private, wants to implement an ERP solution, there has to be a commitment from the leadership. It is not just a commitment; it is a passion to get this thing done. If the

*Commander
Defense Supply
Center Richmond,
Va., Rear Adm.
Mark Heinrich
discussing the
Business System
Modernization
program with
employee
Taneesha
Goodrich July
2005. BSM*



replaced a COBOL-driven legacy program designed in the 1960s with enterprise resource planning software.

passion to do this is not there, the system will fail. When you see the statistics of the various companies that have tried, it bears out the fact that there has to be a commitment on everyone's part.

Another thing that I would reinforce is, 'You have to train, you have to train, and you have to train' to make sure that the system can be implemented successfully. If we had chosen a strategy, which you could call a 'big bang,' which means that we had thrown everything into BSM at one time, we would have failed miserably. We would have probably put support to the warfighter at risk.

Certainly, a lesson learned for anyone is that an incremental approach is the best. As you move to an ERP solution, you learn and adjust. You take another bite out of the apple, and you keep on going until you are finally operational.

CHIPS: The Integrated Data Environment (IDE) will provide a DoD ebusiness information exchange service, which will enable common interactive business practices across the military services, agencies and their trading partners. How will the IDE work?

Vice Adm. Lippert: This is a goal that the DoD has had for years. The idea behind it is to ensure that regardless of where warfighters are, when they query the supply system, they know what the asset profile is or when the contract is due in. Warfighters want to know if we have what they need, and where the material is in the transportation system as it arrives in the theater.

One of the major lessons learned in Operation Desert Storm in the early '90s was that we had a huge buildup of material there, literally mountains of material, because the warfighter was ordering materials repeatedly to make sure he (or she) had them on hand. It gets back to trust in the supply system and its ability to produce what is required. If asset visibility tools had been in place in Desert Storm, we would have had a more cost-effective supply chain providing materials for our warfighter. That is why this initiative is so important.

We have implemented the newest version, which we literally call 'Asset Visibility' that is part of the IDE effort. Warfighters can query into AV and get the required data that they need, not only from DLA but also from the military services, and can utilize the data in readiness planning. This new version of AV creates some executive summary

level charts that help from a management perspective and also allows us to access our BSM effort.

I have been to Kuwait several times, and one of the frustrations of the warfighters is that they have to go from personal computer to personal computer to tap into various databases so they can get all the information. It would be nice if they could sit at one PC and get the information that they need. To help, DLA and USTRANSCOM (U.S. Transportation Command) are joining together to converge our IDE system with USTRANSCOM's GTN (Global Transportation Network) system, which provides the transportation tracking link into one source so the warfighter can find not only basic asset visibility but also the transportation status. This is a major step forward for us.

The next step, beyond converging IDE with GTN, is to expand IDE's scope within DLA to better integrate all of our DLA logistics data. Subsequently, we plan to help DoD pursue an Enterprise Integrated Data Environment, which would enable faster and more accurate sharing of logistics information from the military services' databases via a Web browser, including data in their ERP replacement systems and their current legacy systems, to help provide the full across-DoD asset and transit visibility that is so important for future logistics support to the warfighter.

CHIPS: DLA is a champion of knowledge management practices. Can you talk about some of the projects in this area?

Vice Adm. Lippert: I put this under the umbrella of communications. DLA has more than 20,000 people around the world. Communicating is a difficult process. You have read that you have to communicate everything seven times to get the message through. Anything that we use to help in communicating and overall knowledge sharing is very important to us. We implemented a common tool called 'eWorkplace.' The intention is for it to be used throughout the entire DLA enterprise.

We also have worked hard on metrics, which we use throughout the organization for anything that we do, to measure to see if, in fact, the tool is being utilized and then to link it into our strategic and business plans, our Balanced Scorecard, which are all part of our strategic effort. This is to make sure that everybody realizes our objectives; this is why eWorkplace is so important.

eWorkplace is an enterprise portal; it is a common base for delivery of all information within DLA. At the first of this year, we had over 52,000 logins to the system, which is a 30 percent increase in growth since August 2005. One of the things it does is greatly reduces the amount of bandwidth used to send multiple briefing copies to potential users by e-mail. Instead, we provide a link to the file on eWorkplace. This also reduces the number of copies that need to be stored on individual PCs and helps ensure everyone is referring to the current version.

We do get feedback from people who feel it can be used in a better way, and we try to make adjustments accordingly. We have gone more and more to teleworking, and in a telework environment, things like eWorkplace become important tools to make sure that teleworking is a successful effort.

CHIPS: What is the eBusiness/eCommerce initiative?

Vice Adm. Lippert: This is something that is important for us as we look to the future. Although the terms 'eBusiness' and 'eCommerce' only came into common use in the mid-1990s, DLA has really been involved in this approach for the last 40 years. When DoD standardized logistics transactions throughout the Department, it became part of our Defense Automatic Addressing System. In recent years, we have greatly increased our leverage of the Internet to enable much more extensive use of commercial standards and to provide faster support overall.

The related effort that I am most interested in now is 'DOD EMALL.' We have been running EMALL for the Department of Defense. Basically, EMALL allows a DLA customer to log in to the EMALL Web site (www.emall.dla.mil) and access a series of catalogs to order material using a DoD credit card and to arrange transportation for the materials to be delivered.

The idea for EMALL was started in the late 1990s. Initially, it did not have much business. We built it and nobody came, as opposed to 'build it and they will come.' We spent a lot of time at DLA marketing EMALL and making sure customers knew what the capabilities are and what it could do for us.

In FY02, our sales were about \$6 million out of the \$17 or \$18 billion worth of business that DLA was doing. It grew to \$60 million in FY03, and we completed last year at \$500 million. The number of customers has increased from 13,000 to 26,000. We have about 1,200 catalogs from various sources on it now, and I continue to see this growing as we look into the future.

Many of our big customers are organizations like the naval shipyards that have found EMALL helps fill their requirements. We have even expanded use to the Department of Homeland Security.

CHIPS: DLA has such a large customer base, is it possible to standardize business processes and technology across DoD and federal agencies?

Vice Adm. Lippert: Impossible. There are too many unique applications and missions for that ever to be a goal. But there are clearly certain areas that we can work on in terms of better standardization. The transaction system that I mentioned is basically the same regardless of who the customer is. Where we have areas where it appears that standardization can be done, we certainly focus on that, such as our successful standardization of warehousing operations that support all of DoD, and in our logistics data projects such as the IDE/GTN convergence that I talked about earlier.

DLA inventory manages most of the 5.2 million items that I have mentioned. As we continue to manage all of these items, it leads to standardization. To explain, they are mostly consumables, many of them commonly used across DoD — items that are either consumed, such as food or fuel, or are disposed of when no longer useful, like certain clothing items or various spare parts and general use items.

This contrasts with items that are used for awhile and then repaired or refurbished for reuse, commonly called Depot Level Repairables.

DLRs are often warehoused by DLA but are inventory managed by each of the military services. The Base Closure and Realignment Commission gave us some opportunities to do additional standardization, including applying common procurement practices to buy DLRs in the amounts determined by the services' inventory managers.

So where we can, we try to take advantage of standardization, but there is never going to be one standard way to do all of this.

CHIPS: You sound so passionate about serving DLA customers. Do you consider the services DLA provides to be part of DoD's weapons systems?

Vice Adm. Lippert: They absolutely are from many aspects! First, when you manage 95 percent of the consumable items that DoD uses, it is obvious that we are engaged with the weapon systems around the world. In all my travels since I have been here, one experience has always stuck out in my mind to emphasize the importance of DLA's missions and our role in weapons systems support.

As we were expanding our role into Kuwait, the Army sent some of its divisions from Korea into theater and they brought their equipment with them. In Kuwait, the Army was bringing some of its tanks up to higher readiness levels, and as I was going around and looking at all the maintenance effort that was going on, one of the groups put out in front of a tank all of the DLA items that they were using for the readiness improvement to the tank. It really brought home the importance of the mission that we have in providing supply and piece part support to make sure these weapon systems are geared to do what they do.

The second piece of it is that we are getting more and more into information services in terms of asset visibility and the systems we can bring to make it easier on the maintenance people and warfighter to support readiness.

The third piece of this whole thing is that we have, in the last several years, positioned our people forward with the warfighters. We have DLA people with our major combatant commanders and also our major customers. They actually deploy with them as they go into theater. We have a significant presence in Southwest Asia right now, in Iraq, and certainly in Kuwait and Afghanistan. DLA is central to the entire mission of the Department.

CHIPS: U.S. forces in Iraq and Afghanistan have commented enthusiastically about the quality and variety of food in the dining facilities. Is DLA responsible for providing the fresh food items?

Vice Adm. Lippert: We are involved in awarding the contracts for the food in all these areas. We call these contracts 'Subsistence Prime Vendor Programs.' They started in the continental United States. It is an interesting concept; we do not put the food in our warehouses. We have a prime vendor that we requisition through, and the prime vendor will go to various contractors and suppliers in its network. This method provides our customers the opportunity to pick the brands and types of food that they want to use. The selection opportunities are great. It's done in a timely manner, and I do not have to put all this material in my warehouse.

We have expanded that concept overseas. In Southwest Asia, we

have a company that does the primary work, which we call PWC (Public Warehousing Co.) Kuwait. PWC Kuwait provides the food for that area. I have been there, have tasted the food, and they do a great job.

CHIPS: Are there any other DLA initiatives that you would like to tell our readers about?

Vice Adm. Lippert: There are a lot of things going on including focusing on the human capital side of our business. As we have done corporate climate surveys over time, in addition to the communications effort that I talked about throughout the agency, it became apparent that while DLA was doing a good job overall in performing its missions, there were concerns within the workforce that one of the things we needed to work on was further enhancing the professionalism of our management team.

Most of the promotions that we did in the DoD civilian workforce were based upon technical expertise. We had not spent much time training those who had been promoted in terms of leadership and management. We have a major effort going on within the DLA to ensure that our workforce is also up to world-class standards in terms of leadership and management skills. CHIPS

IDE/GTN Convergence

Enhanced materiel visibility is among the benefits customers can expect from a new program management partnership recently announced by U.S. Transportation Command and the Defense Logistics Agency. The partnership will integrate defense supply chain, logistics, transportation and distribution-related data and information technology services. A new program office has been established to unify logistics/distribution/transportation visibility efforts between DLA's Integrated Data Environment (IDE) initiative and USTRANSCOM's Global Transportation Network (GTN) program, with the goal of eliminating redundancy, streamlining access to data and optimizing resources.

The convergence of the two programs will provide common integrated data services to assist development of applications that will give combatant commands, the military services, DoD, and other federal agencies a cohesive solution to manage supply chain, distribution and logistics information. Convergence will provide a single point of systems data integration within and between DLA and USTRANSCOM and other systems; ensure consistent access to common, authoritative logistics data; and provide business rules and reliable information for DLA and USTRANSCOM and their customers.

To smooth the integration process, both programs have been placed under a single program executive officer, David Falvey, at DLA. The program manager is Army Lt. Col. Pat Flanders at USTRANSCOM. Flanders is currently leading a 90-day technical analysis to evaluate and recommend the best approach to deliver these capabilities. After the analysis, the DLA/USTRANSCOM team will jointly develop the strategy for delivering the necessary data sharing and systems to provide this needed end-to-end capability.

More information about USTRANSCOM is available at www.transcom.mil/.

DLA is the one source for nearly every consumable item, whether for combat readiness, emergency preparedness or day-to-day operations. More information about DLA is available at www.dla.mil/. CHIPS

Adobe Contract News

The Department of the Navy Information Technology (DON IT)

Umbrella Program of contracts announces four newly awarded

Blanket Purchase Agreements for Adobe products ...

By Steve Thompson

Four new Blanket Purchase Agreements (BPAs) provide both new and upgrade software licenses for Adobe products. These agreements also provide Adobe software upgrade plans, formerly known as maintenance agreements. The BPAs include software licenses formerly known under the Macromedia product brand. Products include: Acrobat (Standard and Professional); Photoshop; Encore; After Effects; Frame Maker; Creative Suites; Illustrator; Flash Professional; Dreamweaver; Cold Fusion; and other Adobe products.

The awardees are CDW-G, Softmart, ASAP and Softchoice.

A change in Adobe licensing will affect a user's ability to purchase upgrade plan coverage for legacy products. Without purchasing upgrade plan coverage, customers will not be eligible for free version upgrades.

From May 1 through Nov. 1, 2006, all Defense Department customers that own Adobe and Macromedia legacy software licenses will be able to purchase a new upgrade plan — if the customer's software licenses are at current shipping versions. The first six months of the new Adobe agreement will be the only opportunity to cover (maintain) legacy Adobe products even if customers currently have maintenance plans.

Customers that do not take advantage of this limited time offer will have to purchase an upgrade license (if available) or repurchase a new license for the Adobe product to obtain the latest Adobe versions.

After the first six-month period, upgrade plans can only be purchased for new and upgrade licenses — and only at the time of a new license purchase.

Products may be purchased through the ITEC Direct storefront (<http://www.itec-direct.navy.mil>). Customers can make direct purchases using the government credit card; contact software product managers and obtain customer service; browse our product line; review policy notices; and access small business contracts.

Contractors:

ASAP (N00104-06-A-ZF33)
Small Business (800) 248-2727, ext. 5303

CDW-G (N00104-06-A-ZF34)
(703) 621-8211

Softchoice (N00104-06-A-ZF35)
Small Business (703) 480-1957

Softmart (N00104-06-A-ZF36)
Small Business (610) 518-4192

These BPAs expire May 31, 2008. Go to page 53 for a complete list of contracts and points of contact for assistance.

For more information, go to the DON IT Umbrella Program Web site: <http://www.it-umbrella.navy.mil/contract/enterprise/adobe-esa/index.shtml>. CHIPS



Savings Under the Umbrella

The DON IT Umbrella Program assists the DON and DoD in making efficient use of IT dollars. It is a business strategy that aggregates customer requirements for volume discounts on the products and services that Defense customers need most.

As a key component of the DoD Enterprise Software Initiative (ESI), the Umbrella Program fulfills the Navy's duties as the executive agent for office automation tools, enterprise resource planning (ERP) software and enterprise application integration software.

ESI product agreements include: the entire Microsoft product line; Section 508 tools; Adobe; Oracle; Novell; TOWER Software; Business Objects' Crystal Reports and Crystal Enterprise; Telelogic; NetIQ; Symantec; Quest Software; Red Hat Linux; WinZip; Gartner research and advisory services; and much more.

But the DON IT Umbrella Program is more than just a convenient way to order hardware, software and services, it is a business model that yields optimal pricing and preferred terms and conditions for widely used commercial-off the-shelf (COTS) software.

Refer to Defense Acquisition Regulation Supplement (DFARS) Subpart 208.74 for policy and procedural guidance. The recent reissue of the Defense Acquisition System Policy (DoD 5000 series) mandates the leveraging of, and coordination with, the DoD Enterprise Software Initiative when the use of commercial IT is considered viable.

Finally, relevant provisions of the DoD Chief Information Officer Guidance and Policy Memorandum of July 26, 2000, may also be incorporated into software directives and instructions.



N-STAR

NAVAL RESEARCH — SCIENCE & TECHNOLOGY FOR AMERICA'S READINESS

The quest for
America's future
scientists and
engineers

By Sharon Anderson

Naval Research — Science and Technology for America's Readiness, or N-STAR, is a program within the Office of Naval Research. Its purpose is the development of the next generation of Navy scientists and engineers to ensure that the Department of the Navy maintains a leading edge in warfighting technologies for national defense.

To this end, N-STAR director, Bob Kavetsky, said the Office of Naval Research, under the leadership of Chief of Naval Research Rear Adm. William Landay, in cooperation with the Navy's warfare centers, is developing a suite of programs that the Navy hopes will result in bringing on board 4,000 new scientists and engineers over the next 10 years.

Background

According to ONR, the N-STAR program combines vital efforts to replenish the anticipated loss of federal science and technology (S&T) employees who will reach retirement age in the next 10 years. One effort involves generating student interest in science and engineering fields and recruiting these students for service in the Navy's labs and warfare centers.

The Office of Personnel Management estimates that 60 percent of the federal government's workforce will be eligible to retire over the next 10 years and that 40 percent will likely retire. Competition between government agencies and private industry for the shrinking pool of newly graduating engineers and scientists is expected to be keen. According to ONR, agencies that are unprepared to replace retiring employees will find themselves in a bind when they see their intellectual capital walking out the door.

"The next 10 to 15 years could be a golden age for the mass transfer of corporate knowledge from our existing population of 'greybeards' and technical experts to the next generation of scientists and engineers coming into the system," Kavetsky said. "NASA has paid the price by letting a lot of its corporate smarts go out the door. The Department of Energy ran into this same problem with its nuclear weapons programs, so the Navy is not unique in this regard."

According to ONR, there are about 22,000 scientists and engineers in the DON, of which about 4,000 of whom are card-carrying members of the S&T community. These are professionals who perform basic and applied research.

Up to half of these civilian scientists and engineers are eligible to retire in the next several years and with fewer U.S. students graduating with advanced science and engineering degrees, a crisis in replacing these employees is anticipated — unless decisive action is taken now.

"They are in my view, the pointy end of the spear, the intellectual spear. They are the ones that interface with the universities and know what is happening in global research arenas. In my view, they are a critical piece of the whole naval research enterprise," Kavetsky said.

Launching N-STAR

By engaging personnel from the naval warfare centers in active outreach programs, N-STAR has been effective in introducing young people to the benefits and joys of careers in Navy research. According to ONR, it is important to let young scientists and engineers know that there are challenging opportunities in the Navy, where they can have the flexibility and satisfaction of performing independent research — with a chance to serve their country.

A few years ago, ONR, under the N-STAR program, initiated a scholarship program between the National Science Foundation (NSF) and the Navy. The NSF/N-STAR Civilian Service scholarship program, or NNCS, targets recruiting efforts at juniors and seniors in college and graduate students. The students receive fellowship money and incur a service obligation as civil service employees in a naval research and development (R&D) center.

While it may seem ironic that young people are not drawn to these areas of study since today's teenagers and young adults are plugged into mobile electronic devices like never before, Kavetsky said their knowledge of the science that makes these devices possible is superficial at best.

"In my opinion, children are using those devices like toys and at the toy level. When you want somebody to get excited about science or engineering, you have to work deep into those fields. Children today are just scratching the surface. Even at the high school level, and in early college, these students are shallow in their understanding of the enabling technology. They are whizzes at how to apply it because of their quick reflexes. But our kids are 'wired' because we have given them neat toys not because they have an appreciation of the underlying science," Kavetsky said.

Recognizing this paradox, ONR began looking at engaging student interest in science and technology at a younger age by forming partnerships with local and state government, and academic leaders, which led to an outreach program with schools and universities in Virginia.

The Virginia Demonstration Project

The commonwealth of Virginia joined with ONR to expand the N-STAR program to reach students at the middle school level in 2004.

Far right, middle school students brief their Navy civilian engineer mentor, Homar Rivera, a branch head from NSWC Dahlgren, about their robotics project at a Virginia Demonstration Project event at the Fredericksburg, Va., Exposition Center. The VDP event attracted about 1,700 students April 13, 2006. Left photo from l to r: N-STAR Director Bob Kavetsky, Chief of Naval Research Rear Adm. William Landay and VDP Director Bob Stiegler.



Left photo from l to r: N-STAR Director Bob Kavetsky, Chief of Naval Research Rear Adm. William Landay and VDP Director Bob Stiegler.

Virginia entered into the program when staffers from Virginia Republican Sen. John Warner's office became interested in N-STAR through a brief given to Congress by National Science Foundation staff. Sen. Warner's office provided \$1.8 million in the Navy's S&T budget in fiscal year 2005 for the Virginia Demonstration Project. In FY 2006, Sen. Warner's office provided an additional \$2.1 million.

The VDP was launched in partnership with one of the premier research and development centers in the Navy, the Navy Surface Warfare Center (NSWC) in Dahlgren, Va. About 35 Dahlgren scientists and engineers work with middle school teachers and students. In 2005, Dahlgren staged a summer camp for about 100 students. NSWC engineers and scientists provide mentorship and help to students. A portion of the VDP funds are assisting three NSWC employees obtain doctoral degrees.

Doctoral degrees are going to be the level of expertise needed to play in the global S&T arena, according to Kavetsky.

"One of the unique things that has happened by design, is that NSWC doctoral candidates act as role models to the students. These Ph.D. candidates are newer at Dahlgren and relate better to middle school students than somebody my age," Kavetsky said.

Other key partners in the Virginia Demonstration Project's success are Dr. Eugene Brown, a professor of mechanical engineering at Virginia Polytechnic Institute and State University, and VDP program director, Bob Stiegler, a retired Dahlgren engineer. They put a strong team together which included partnership with the College of William and Mary and school systems in Stafford, King George and Spotsylvania counties.

This year about 1,700 students from Spotsylvania, Stafford and King George County middle schools, in addition to the Dahlgren DoD middle school, participated in the VDP. Two summer camps are also planned at NSWC in Dahlgren. Each camp can accommodate about 100 students.

According to Kavetsky, igniting children's interest in science and technology at the middle school level has been a fascinating experience with some unexpected results.

"When you are in middle school, math problems have a fixed answer. What we have seen in our program is when you get a real working engineer in the classroom with the middle school teacher, showing the students that the problems that we are working on are not in the textbook and do not necessarily have pat answers, or they have multiple answers sometimes creates a spark with students," Kavetsky said.

The inspiration to drawing student interest has been in showing students real-world problems and challenging them to find practical solutions.

"The problem set students chose last year was how do you use unmanned surface, undersea and air vehicles to address the world's landmine problem. When Bob Stiegler, VDP program director, told me they had chosen that topic, I looked at him like he must have gone crazy. But he told me the teachers and students picked that problem because they had found that the largest population worldwide affected by landmines is children," Kavetsky said.

"The children in middle school saw that for their compatriots in other countries this was a big deal. What the children have seen is that there is a whole world of problems to which we do not have textbook answers. The teachers have seen children show some interest in their studies. That is what the program is all about — exciting the students about science and mathematics studies," Kavetsky said.

Students worked in project teams of six to eight, which was a fundamental ingredient to success, according to Kavetsky. Students used creativity and their knowledge of other subjects such as English and art to complete their projects.

"Somebody had to write up project reports, others had to make displays. They did not all have to become 'technology weenies' because they could use other skill sets in executing the project," Kavetsky said.

The Navy would like to duplicate this success in every other state where it has a presence, such as where the R&D centers are located, but according to Kavetsky, the program is scalable across DoD. "We have already been in discussions with the Office of Secretary of



Defense about how to expand something like this DoD-wide. ONR R&D centers across the Navy bring a mass of scientists and engineers to draw from. They all live in communities, so it is easy to link them up with their local school systems," Kavetsky said.

The VDP is open to all students from participating schools. There are no prerequisites or entry fees.

"One of the aspects of the program that I am excited about is that this program is not just for the gifted and talented — it is designed for all children. We are making this a regular part of the school day. This is not an after school activity that students sign up for voluntarily. Our push is to get all children to some degree exposed to this and some children really excited about it," Kavetsky said.

Knowledge Transfer

The N-STAR program manages about \$15 million a year of In-house Laboratory Independent Research (ILIR) money that is sent from ONR to the technical directors of the major naval warfare centers. Those technical directors pick the projects in which their centers will be engaged. In FY 2002, ONR launched the In-house Applied Research (IAR) piece of N-STAR with \$4 million of applied research money.

Kavetsky calls the money "seed corn" for new research topics that focus on specific mission areas. For example, NSWC Dahlgren performs basic research in the areas of combat systems and chemistry-biology. The Naval Undersea Warfare Center in Newport, R.I., performs research in submarine technology. At NSWC Indian Head, Md., energetics scientists work with explosive molecules.

ONR teams new junior level scientists and engineers with a seasoned employee to start the transfer of corporate knowledge to the next generation. There are about 20 IAR projects that team three or four junior level people with a senior level scientist.

Shaping Future Leaders

Instead of just focusing on research work, N-STAR built a leadership component into the NSF/N-STAR Civilian Service scholarship program last year. The students, who are from the top universities in the country, step away from their studies for three days to do a self-assessment about their careers.

Initially, they went to the workshop wondering what they were doing there and, in many cases, their advisers were not happy about them attending, since it entailed three days away from their research work. But it was a valuable experience, according to Kavetsky.

"They saw in dealing with our people at NSWC Carderock how you apply some of what their graduate studies are all about. They appreciated the time to reflect on their own careers and their future leadership roles in our S&T community," Kavetsky said.

Communications Outreach

There is also a formal communications component for the N-STAR program, which encompasses newsletters, symposiums and program Web sites.

The N-STAR flagship publication is *STARLINK*, which contains pro-

gram highlights and research initiatives across the naval warfare centers and labs. *STARLINK* is available online at <http://www.nstarweb.com/enewsletter.html>.

N-STAR is also reaching out to naval officers in all designators.

"In the Navy, other than medical officers, there are roughly 42,000 naval officers, of those, 119 have doctoral degrees. Everybody has the perception that the Navy is the technology service. I am not so sure that is the case. The Air Force has more than 1,000 Ph.D.s in its officer corps. One of the things we decided in our N-STAR program is that we needed our future naval officers to have an appreciation of science and technology," Kavetsky said.

To showcase naval S&T careers and their importance to the future of the Navy, 70 leading scientists and engineers from NSWC Dahlgren led a three-day conference for the midshipmen of the U.S. Naval Academy last year. The conference was a win-win proposition for both the midshipmen and their instructors who began to form relationships with NSWC scientists and engineers.

"We have gotten unbelievably positive feedback from our scientists and engineers who enjoyed interfacing with the students at the Naval Academy. They are bright students and ask a lot of good questions. The Naval Academy faculty appreciated it because it makes their jobs easier in showing students at the university level how to apply calculus, chemistry and physics to problems... Our scientists can explain how the sonar transducers on Navy submarines work. It was a valuable exercise," Kavetsky said.

N-STAR plans to take the technology conference to the Naval Postgraduate School this year to naval officers who are working on advanced degrees.

"We are trying to make sure that at the end of the day our naval officers have an appreciation of what technology is doing for them in a military sense and that they have formed some relationships with our science and engineering community across the Navy. That is what we are here for, to support them. Having them know where that energetic molecule came from is a healthy thing to do," Kavetsky said.

Few would argue that the economic power of the United States and its military might are built on a robust science and technology community, which includes U.S. universities, Defense Department and government labs, and high tech industry.

"You are seeing India and China graduating increasing numbers of students with S&T degrees, and we want to ensure we have a robust supply of U.S. citizens earning engineering and science degrees," Kavetsky said. "We need to encourage children at a young age to become interested in science and mathematics." CHIPS



For more information about N-STAR go to <http://www.nstarweb.com/> or phone (703) 696-4126. CHIPS

Growing Technology Leaders

VDP leads seventh graders on the road to math and science professions

By John Joyce, NSWC Dahlgren Division Corporate Communications

Sen. John Warner, R-Va., told about 1,700 middle school students that they are the future of the country at the Virginia Demonstration Project (VDP) Exposition in Fredericksburg, Va., where students were showcasing their scientific achievements.

“America is falling behind,” Warner said, “as we train 70,000 scientists and engineers this year, China graduates 600,000 scientists and engineers. We need a wake-up call, and you are sending that wake-up call.”

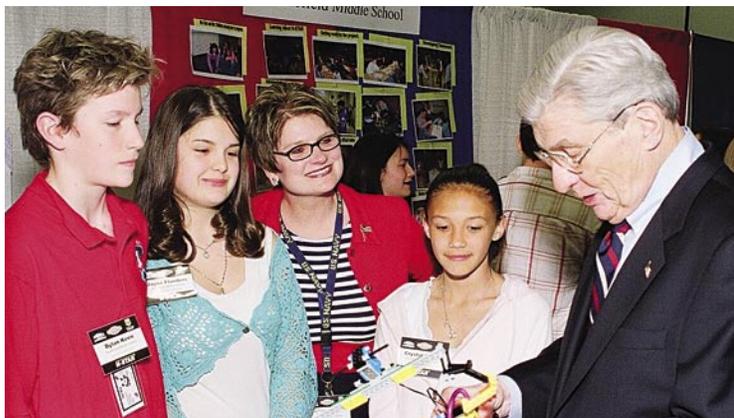
The VDP is a part of the N-STAR (Naval Research — Science and Technology for America’s Readiness) program, which was launched in 2004 by the Office of Naval Research (ONR). It was initiated to show young students that careers in math, science and engineering are fascinating, fun and socially relevant.

“There are worlds of problems waiting for you to solve,” said the Chief of Naval Research Rear Adm. William Landay. “You have discovered that engineering is really a lot of fun when you can get your hands on it,” said Landay, who is also the Assistant Deputy Commandant of the Marine Corps for Science and Technology.

Conceived as a multi-year, state-wide outreach effort involving high schools, middle schools and community colleges, the VDP is in its first phase and is limited to middle schools in King George, Stafford and Spotsylvania counties. The VDP program uses the science and engineering staff of the Naval Surface Warfare Center (NSWC) Dahlgren Division as mentors to the students and teachers.

A host of military and civilian leaders joined Sen. Warner and Rear Adm. Landay April 13 to commend the students and endorse the VDP program that gave the students an opportunity to work in their classrooms side-by-side with Navy scientists and engineers on technological projects designed to solve today’s problems.

“The students were outstanding in their presentations and in tying the technology to real-world environmental issues,” said VDP program director Bob Stiegler, a retired engineer from the NSWC Dahlgren Division. “It is evident by the level of the speakers and the number and level of those in attendance, that the project has a



broad base of support. And not just in words, but through active support of the leadership on all levels – Sen. Warner’s office, ONR, NSWC Dahlgren, the county school districts and the universities.”

The VDP Expo confirmed for attendees, including NSWC Dahlgren Division Commanding Officer Capt. Joseph McGettigan, Fredericksburg Chamber of Commerce officials, King George, Stafford and Spotsylvania county middle school principals and school board members that a new generation of Americans can indeed make the world better and assist in national security efforts armed with math and science skills.

Students, working in teams of six to eight, used robots, computers, Microsoft PowerPoint presentations and movies they wrote, narrated and produced to explain their creative solutions to save lives, clean oil spills and clear mines from land and water.

“This is the American dream – developing things to make people’s lives better,” McGettigan said. “When we give these kids a problem, there’s a lot of excitement as we watch their enthusiasm in solving it with a skill and technical savvy they didn’t have before.”

One way VDP generates the interest of students in math and science is through their teachers. The program provides middle school teachers with opportunities to team with scientists and engineers from the mentor-rich environment at the naval warfare centers.

“We were able to see science and engineering in real jobs doing real things for all of us,” said Dr. Jean Murray, Superintendent of Stafford County Public Schools. “Our students learned more than science and math. They have learned about creativity and problem solving, and how to learn by sharing information.”

VDP common themes featured robotics problems that were integrated into four subject areas: math, science, language arts and civics. “N-STAR definitely changed my mind,” said Kaitlin McDonough, an H.H. Poole Middle School seventh-grader, after giving a brief about how to clean up an oil spill and protect coral reefs and marine life. “Before our project, I saw math as just numbers.”

Mentors from NSWC Dahlgren, approximately 35 scientists and engineers, shared real-world experiences to shape positive perceptions about math and science among students preparing for high school. “Although this program was developed to encourage young people to consider careers in technical fields, working with these young minds reinvigorated me and made me more appreciative of my work,” said Bruce Copeland, a Strategic and Weapon Control Systems Department engineer, who mentored students at Chancellor Middle School.

“With all the reports about the inability of young people to concentrate on a single task, it was enlightening to see the focus and intensity of purpose that some of the young men and women could bring to bear on solving a complex problem. It improves my outlook for the future of our nation,” Copeland said.

Chairman of the Senate Armed Services Committee, Sen. John Warner, R-Va., and participants of the VDP Exposition in Fredericksburg, Va., April 13, 2006.

VDP's ultimate goal is to establish educational outreach programs at other Navy research and development centers throughout the country. The initiative could eventually expand beyond the Navy and evolve into a national demonstration project encompassing all the Defense Department laboratories in a sustained effort to secure the long-term competitiveness of America's science and technology workforce by hooking more students on math and science at an earlier age.

"After approaching this problem from a practical aspect, our students have a clearer understanding of what public policy is and can see themselves in the future as citizens who have an active part to play in public policy," said H. H. Poole Middle School civics teacher Nancy Vitale.

For more information about the Virginia Demonstration Project, go to the N-STAR Web site at <http://www.nstarweb.com/>.

CHIPS

Calling All High School Students ... to a Science Fair

By Sharon Anderson

The Naval Science Awards Program is a U.S. Navy and Marine Corps program that encourages America's students to develop an interest in science and engineering. NSAP recognizes the accomplishments of eligible students at regional and state science and engineering fairs, and the International Science and Engineering Fair (ISEF).

The Office of Naval Research sponsors NSAP for the Department of the Navy. The ONR executes and promotes science and technology programs of the naval services through universities, government laboratories and nonprofit and for-profit organizations.

The Navy and Marine Corps participate each year in more than 425 regional, district and state science and engineering fairs in which high school students exhibit their projects. Qualified experts drawn from local Navy and Marine Corps activities serve as judges, with subsequent presentation of prizes to successful competitors.

Each year the ONR participates in the ISEF, administered by Science Service. Nearly 1,200 high school students, in grades 9 through 12, representing over 500 science, math and engineering fairs affiliated with Science Service, display their research projects and vie for hundreds of special awards. At the ISEF, the ONR selects one winner in each of the 14 scientific disciplines, three students from any category who have projects deemed to have particular naval relevance, and one two-person team to receive an \$8,000 undergraduate scholarship, payable at \$2,000 per year.

Nineteen students were named "Naval Science Award Winners" at the 2006 ISEF in Indianapolis, Ind. The fair, held May 7-12 at the Indiana Convention Center, provided students with a diverse learning experience. Katherine Hesterman Newcomb, a Navy Reservist and microbiologist/medical educator who has been a Navy ISEF judge

since 1989, said she enjoys the students' enthusiasm and continues to be impressed by how hard they work on their projects.

"The projects become more sophisticated and specialized with each year. A greater percentage of students, have access to research laboratories in which to carry out their work and, overall, the mentoring seems to improve each year. This contributes to increased difficulty in judging, with the necessary time limitations. Although people often find this hard to believe but, if you ask any of the judges, you will hear that the complexity of a number of the projects is often at a master's or doctoral level," Newcomb said.

In addition to naval scientific areas, other project categories included the behavioral-social sciences, botany, environmental science, medicine and health, space science and zoology. The Navy hopes the fairs will excite the students' interest in science or engineering so they will pursue advanced degrees in these areas.

Midshipman 2nd Class Craig Wright, a three-time competitor in the science fairs and now a Navy ISEF judge, said participating in the fairs helps students decide on a career path.

"I can personally attest to the significance that the science fair played in my life. Researching and competing in the fair challenged my mind more than any other program I ever engaged in. Now a midshipman at the U. S. Naval Academy, I accredit a large amount of my success at the academy to what I learned through the science fairs," Wright said.

The fairs also give students a chance to talk with other students and discover new fields of study.

"Participating students realize it is an excellent venue to meet other students with similar interests, to meet mentors working in the field, to learn of opportunities for internships, and to learn of the variety of job opportunities involving science. Seeing other projects often sparks ideas for their own research. For their friends who have not participated, they can see the positive impact this experience has, and may pique their interest to also become involved," Newcomb said.

Wright agreed that participating in the fairs opens new horizons for students. "I was able to investigate a wide variety of scientific disciplines without the fear of committing to a single subject. Now in college, I have a good idea of my interests and am pursuing a degree in aerospace engineering."

Naval Science Awards are open to high school students in grades 9 through 12 who are citizens or permanent residents of the United States or its territories at the time of their selection.

According to Newcomb, just attending a science fair is a memorable experience. "I believe that anyone who attends the ISEF cannot help but be impressed at these young scientists' work and dedication. To use one of their expressions, 'It is awesome!'"

For more information contact the NSAP program manager at (703) 696-4111 or NSAP_help@onr.navy.mil.

CHIPS



The 2210 Classification

The 2210 IT Specialist occupational code, developed through a partnership between the Federal CIO Council and the Office of Personnel Management, has 11 parenthetical specialty titles. Workforce identification becomes complicated because the implementation of the 2210 standard is inconsistent, demonstrated by the fact that only 57 percent of 2210s have a specialty title identified in the Defense Civilian Personnel Data System (DCPDS).

As personnel transition under NSPS, they will be required to identify at least one primary specialty. A combination of two specialty titles are allowed if they are of significant importance to the position (e.g., Applications Software/Systems Analysis). The concept of “generalist” will no longer apply. Given the wide spectrum of functions and the multi-specialist nature of the occupational code 2210, parenthetical specialty titles are crucial to conducting workforce planning.

A comparison shows that there are marked differences between the information reported in the biennial IM/IT workforce skills assessment survey conducted in 2004 and data from DCPDS. DCPDS and survey data are highlighted in Figure 1. These differences reinforce the importance of ensuring appropriate specialty title identification.

Organizations should ensure the parenthetical specialty titles for

Table 1. DON IM/IT Civilian Community Occupational Codes and Parenthetical Specialty Titles

Occupational Codes	Parenthetical Specialty Titles
2210	IT Specialist, IT Project Management
2210	IT Specialist, Policy and Planning
2210	IT Specialist, Security
2210	IT Specialist, Systems Analysis
2210	IT Specialist, Applications Software
2210	IT Specialist, Operating Systems
2210	IT Specialist, Network Services
2210	IT Specialist, Data Management
2210	IT Specialist, Internet
2210	IT Specialist, Systems Administration
2210	IT Specialist, Customer Support
2203 (0332)	Computer Operator
2204 (0335)	Computer Technician
1550	Computer Scientist
1421	Archives Technician
1420	Archivist
1412	Technical Information Specialist
1411	Library Technician
1410	Librarian
0394	Communications Technician
0392	Telecommunications Technician
0391	Telecommunications Specialist
0390	Telecommunications Equipment Operator

Information alert for employees in the IM/IT career fields

Over the last several months, the Department of the Navy Information Management/Information Technology (IM/IT) Integrated Process Team (IPT) has been working behind the scenes in support of the ongoing implementation of the National Security Personnel System (NSPS). During this process, several IM/IT community issues were identified.

The Deputy Assistant Secretary of the Navy (Civilian Human Resources) tasked each of the 21 civilian community leaders to develop standard position descriptions (PDs) in support of NSPS. The DON Chief Information Officer (CIO) serves as the DON IM/IT Civilian Community Leader, and under DON CIO leadership, the IPT has completed general PDs in preparation for the transition to the NSPS.

Background

With the help of subject matter experts and a human resources specialist from the Office of Civilian Human Resources (OCHR), the IPT drafted 48 PDs for the 23 occupational codes and specialties within the civilian IM/IT community. These classifications listed in Table 1, are not descriptive of the full scope of IM/IT work, but they provide a basis for DON-wide civilian community management.

The PDs, drafted by the IPT and awaiting further guidance from OCHR are available for review at <http://www.doncio.navy.mil>. A top priority for effective civilian community management is ensuring that civilian positions are classified accurately. The implementation of competency-based career roadmaps increases the urgency of classifying civilian positions correctly.

As community management matures within the DON, communities will become more engaged in workforce analysis and planning. The goal for all civilian communities is to complete Five Vector Models — the process that will validate competencies, skills and career paths, ultimately impacting recruitment and development — by the end of this calendar year.

those classified in the 2210 occupational codes are correct. This requires personnel and their supporting human resources consultants to become engaged in correcting the titling within the DCPDS.

Command Information Office Personnel

The PD for occupation code 2210, "Policy and Planning," is targeted to civilians performing work within a command information office or performing as a command information officer. The PD aligns to the standard and describes the broad technology management functions that align to command information office functions.

This PD includes a wide range of IM/IT functions such as strategic planning; capital planning and investment control; workforce planning; policy and standards development; resource management; knowledge management; architecture and infrastructure planning and management; auditing; and information security management.

Information Assurance Workforce

Under the IA Workforce Transformation initiative, full-time IA managers and IA technicians will be classified as 2210 occupations with their primary specialty identified as "Security." The PD for this occupation code describes the position of an IA manager and provides a career path option for IA technicians. However, it does not adequately describe the more technical nature of IA technician positions. Therefore, IA technicians should select a secondary specialty from the other specialty titles that are typically related, such as network services or systems administration.

IT Project Manager

Interpretive Guidance for Project Manager Positions, issued August 2003 and available at <http://www.opm.gov/fedclass/PM/CG03-0001.pdf>, provides detailed guidance to address position classification, job evaluation, staffing, qualifications, training, and development for project manager positions.

It also authorizes the title of "IT Project Manager" for the 2210 occupation code in lieu of IT Specialist (*providing two separate, approved titles for the same series*). IT Project Management is the title with the most notable discrepancy in classification. Within the DON, 14.2 percent of the 2004 survey respondents identified IT Project Management as their specialty area, while actual DCPDS data revealed only two people.

2210 Recruitment Announcements

The 2210 occupation code is comprised of 11 parenthetical specialty titles that are functionally diverse. A 2210 series search conducted on USAJobs (<http://www.usajobs.opm.gov/>) April 13, 2006, found 721 announcements; of these 231 were DON announcements and 228 of those were open continuous announcements by geographical location.

The announcements have little detail, combine 10 specialty titles, have grade levels that range from GS-1 to GS-15 and salaries

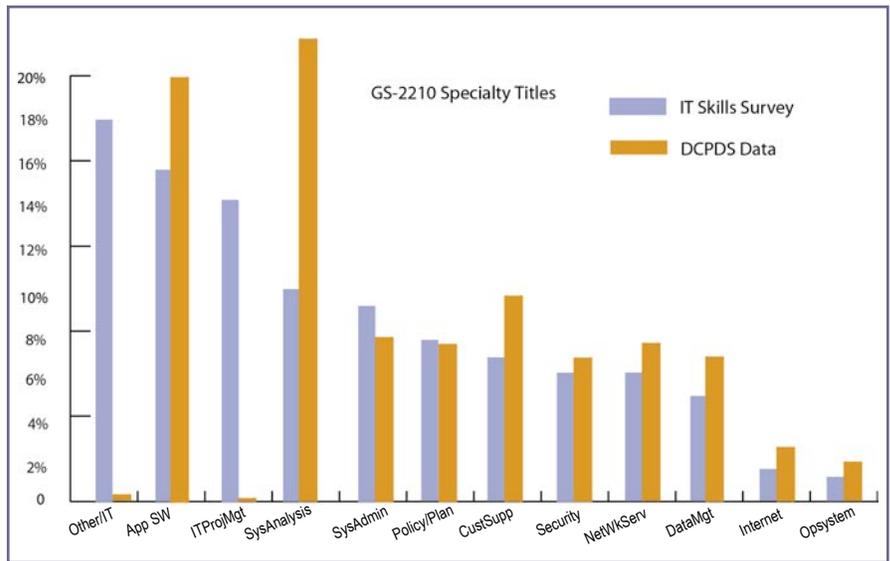


Figure 1. GS-2210 Specialty Titles Reported in the 2004 IT Skills Survey versus Defense Civilian Personnel Data System

that range from \$15,000 to \$115,000. One announcement lists 10 to 50 different geographic recruiting locations.

The announcements were confusing, leaving a potential applicant not sure of what the position entails or where the position is located. It is difficult for an applicant to tell what jobs are actually being advertised — thus creating a barrier to recruiting the best pool of candidates from federal agencies and industry.

The job recruitment area needs further analysis and collaboration with OCHR to make necessary improvements and corrections to the USAJobs Web site. However, within the DON, personnel can access <http://chart.donhr.navy.mil> to easily identify DON job announcements.

The Way Ahead

The DON IM/IT Workforce IPT is continuing its work to improve the DON IM/IT Civilian Community. The IPT seeks your input in order to gain a deeper understanding of the issues and ensure a broad consensus on the best way ahead. Please let your views be heard and provide feedback as we continue to reach out and partner across our community.

Go to the DON CIO Web site for more information at <http://www.doncio.navy.mil/>. CHIPS

DON IM/IT Community Resources

DON IM/IT Virtual Community: Collaborative site for members of the DON IM and IT community. A common access card (CAC) is required to enter the site. If you would like to request membership and participate in this virtual community please use the link below and select the "Apply for Account" button to request access: <https://donimitcommunity.spawar.navy.mil/>.

DON Civilian Human Resources: This site will provide you with timely and useful information on important issues for DON applicants, employees, managers, senior executive staff, and the civilian HR management community. For more information, please visit <http://www.donhr.navy.mil/>.



Computers are everywhere, touching every part of our lives. Home, work, shopping, schools ... You can't go far without hearing the familiar beep of a microprocessor. Uncle Sam uses a lot of electronic equipment too. According to the Environmental Protection Agency (EPA), the federal government buys 7 percent of the world's computers.

But these technological wonders are not designed to last forever. According to the National Safety Council, nearly 250 million computers will become obsolete in the next five years.

The federal government disposes of 10,000 computers every week. That's a lot of electronic trash. What happens to it? According to the EPA, a significant number end up in storage closets, warehouses and landfills, or overseas, where environmental standards are generally lower.

Conservation and Recovery Act (RCRA), Congress directed government agencies to promote recycling by increasing purchases of products containing recovered materials.

Every government agency falls under the Pollution Prevention Act and Executive Order 13101 to recycle and properly dispose of electronic equipment. Guidance is available from the following Web sites:

Pollution Prevention Act – (<http://www.fedcenter.gov/programs/p2/>) signed into law in 1990.

Executive Order 13101 – (<http://www.ofee.gov/eo/13101.htm>), "Greening the Government through Waste Prevention, Recycling, and Federal Acquisition" signed into law in 1998.

DRMS to the Rescue

The Defense Reutilization and Marketing Service (DRMS) is an agency within the Department of Defense and Defense Logistics Agency. DRMS works with the military services to reuse, recycle and dispose of excess material.

There are 89 Defense Reutilization and Marketing Offices (DRMO) located in 17 countries and 37 states on or near military installations. Military units turn-in excess or damaged property, with the proper paperwork, to their DRMO. Excess electronic equipment is redistributed on behalf of Defense agencies by DRMS or sold for reuse by a DRMS contractor resulting in extended life for electronic equipment, thus avoiding or postponing disposal.

Electronics, which cannot be redistrib-

uted or sold, are subjected to de-manufacturing processes that result in some additional reuse and recycling for the remainder of the electronic property. Environmental compliance is assured for Defense Department property, with 100 percent being reused or recycled.

Commercial recycling contractors or Federal Prison Industries perform all of the recycling and disassembly operations. Contracts are awarded under the Governmentwide Acquisition Contracts (GWAC) for Recycling Electronics and Asset Disposition (READ) services.

The contracts provide federal agencies with a dependable method of properly recycling and disposing of damaged or obsolete equipment. Eight companies were awarded contracts January 2005. For DRMS, all de-manufacturing partners are evaluated for technical capabilities and environmental compliance prior to entering into contracts or operating agreements.

Molam International, located near Atlanta, Ga., is one of eight companies recycling electronics for the government. According to company president Nader Nejad, DRMS keeps him busy. "We average 5 million pounds of material every year," Nejad said. "We recycle all of it — including the pallets."

Hazardous materials such as batteries and cathode ray tubes are removed and shipped to specialized recycling centers. The remaining material is shredded into 1 inch pieces and separated. Steel is removed and sent to a scrap metal dealer; plastic is recycled; and precious metals are sent to facilities in Europe where they are recovered.

Computer circuit boards and wiring have copper, gold and platinum in them. These materials can be ground into a fine powder and reused in new computers, according to Nejad.

"Working in partnership with the military services and contractors, the Precious Metals Recovery program recovered more than \$8 million in silver, gold, platinum and palladium in 2005," said John Barrett of the DRMS Precious Metals Recovery program.

According to the National Safety Council, nearly 250 million computers will become obsolete in the next five years.

e-Cycling Guidance

Legislation and presidential direction requiring the purchase of recycled content products have been evolving since 1976, when Congress established a buy-recycled law. In Section 6002 of the Resource



Thousands of old computer circuit boards are collected and shredded, and precious metals such as gold are recovered for future use. Gold flakes like these add up. Working in partnership with the military services and contractors, the Precious Metals Recovery Program has saved the government \$250 million over the past 30 years.

There are opportunities for federal and DoD agencies to save money by participating in the efforts described below.

Reutilization: A military unit that can use equipment turned-in to DRMS is money saved by not buying new equipment.

Transfer/Donation: Equipment donated to federal, state and local agencies saves tax dollars. These agencies will not need to purchase new equipment.

Precious Metals Recovery: Depending on the contract, either the material is sold and the funds returned to the U.S. Treasury, or it is held by DRMS for future use. For example, if a contractor is manufacturing an item that requires gold, the government can provide recovered gold at a reduced cost to reduce the cost of the contract.

Sales: DRMS gets a percentage of the revenues for material sold by its sales agents.

Agencies are required to remove classified information and sensitive data from all equipment prior to disposal. This equipment is not authorized for receipt by DRMS. But if any classified information or labels are discovered by DRMS or any of its agents, the electronics are immediately secured and steps are taken to return the equipment to the original owner for proper declassification procedures.

Sensitive data are slightly different. Only the original data owner can decide what data are sensitive, so the owner must place a certification on each computer stating that the storage media contain no sensitive data, prior to turn-in to DRMS. The DoD owner may choose to erase data,

degauss the storage media or remove the media from the equipment. Equipment without proper certification is rejected and returned to the original DoD owner.

The end of life process, de-manufacturing and recycling, sometimes result in a positive cash flow. At other times, it may be an expense, but expense is justified because all DoD activities achieve environmental compliance and protection of sensitive data in the processing of their electronic equipment through the DRMS de-manufacturing processes.

Please e-Cycle!

Tons of electronic material are saved from landfills and given a second life through recycling. DRMS provides good stewardship of taxpayer dollars and the environment by e-cycling computer components — everything except the beep!

DRMS provides DoD units worldwide with critical disposal services for material no longer needed for national defense. DRMS is responsible for property reuse (including resale), hazardous property disposal, demilitarization, precious metals recovery and recycling program support.

Additional recycling information is available on the Office of the Federal Environmental Executive Web site at <http://www.ofee.gov/eo/strtpln2.htm/>.

For more information about DRMS, visit www.dla.mil/drms/.

Van Williams is with the Battle Creek, Mich., DRMS Office of Public Affairs. CHIPS

DON CIO Personnel Recognized for Superior Government Service

The Department of the Navy Chief Information Officer Dave Wennergren was recognized for his outstanding leadership with a John J. Franke Award. The John J. Franke Award has been given annually since 1999 to recognize individuals who make extraordinary long-term contributions to the federal government. Winners are senior government employees with 15 to 20 years of service, who typically have successfully led enterprise-wide initiatives across a government or Defense agency.

The award is named in memory of John J. Franke, who was director of the Federal Quality Institute at the Agriculture Department and a long-time president of the American Council for Technology (ACT), which sponsors the award. Each year, the award recipient is selected by a committee of the previous awardees.

With the Department of the Navy for 26 years, Wennergren has served as the DON CIO since 2002 and the vice chairman of the Federal CIO Council since January 2006. Wennergren received the award at the ACT/ Industry Advisory Council's annual Change Management Conference June 4, 2006.

John Lussier, Director of Operations, Telecom/Spectrum/Wireless Team Leader was recognized with the Federal CIO Council Leadership Award. The award is presented to federal employees for their outstanding achievements in improving the way government does business through information technology. The award was presented at the Interagency Resources Management Conference (IRMCO) in Williamsburg, Va.

Barbara Hoffman, Investment and Performance Management Team Leader was recognized with the Government Computer News IT Leadership Award. The award recognizes distinguished individuals from federal, state and local governments for their outstanding work in the field of government information technology. The award was presented at the Government Computer News third annual Government IT Leadership Awards Conference in Washington D.C.

CHIPS

Interview with Carmela Keeney

Executive Director, Space and Naval Warfare Systems Center San Diego

Carmela Keeney assumed the top civilian position, Executive Director, Space and Naval Warfare Systems Center San Diego (SSC San Diego) in December 2005. Keeney, a member of the federal government's Senior Executive Service, assumed leadership of an organization of almost 4,000 civilian and military personnel, most of them scientists and engineers, responsible for inventing, developing, engineering, installing and maintaining information technology and systems on Navy ships, submarines and aircraft, and at shore sites.

The Center is the Navy's research, development, test and evaluation, engineering, and fleet support center for command and control, communications, ocean surveillance and the integration of systems that overarch multiple platforms. Increasingly the Center's efforts are for the other Services as well as the Navy, for Defense Department-level agencies like the Defense Advanced Research Projects Agency (DARPA), and for federal non-military agencies like the Department of Homeland Security and the Office of Disaster Preparedness. SSC San Diego's products include information-collection and intelligence systems; communications devices and networks; tactical information processing; knowledge management and decision support tools; and navigation technology.

Each year, the president honors a select group of career federal executives with the President's Rank Award for outstanding leadership, accomplishments and service in some of the nation's most critical federal positions. Keeney was among a distinguished group of federal employees named in the 2005 Presidential Rank Awards for Meritorious Executive in October 2005.

CHIPS: *What are the most critical challenges you have as the executive director?*

Ms. Keeney: We are a full spectrum center here at SSC San Diego, from basic research through operational support. A top priority is developing, fielding and supporting systems to meet today's critical needs. An example of a current high priority area is coalition interoperability. We aren't only worried about today, we are very concerned about the next generation and the generation after next. It is an increasing challenge in our current environment to maintain a balance between today's needs while not losing our focus on basic research and technology development that will lead to transformational capabilities in the future.

One of our priorities is to make sure that we develop and sustain core competencies that are needed to support today's warfighter and the warfighter of the future — that includes maintaining a strong science and technology (S&T) base to ensure we maintain our technological and warfighting edge in the future. A related priority area for us is recruiting and developing the next generation of scientists and engineers that can address these challenges.

CHIPS: *Are you referring to a shortage of S&T skills or funding?*

Ms. Keeney: It is a circular problem, and you definitely need both. We have seen a decline in basic science and applied research over the last two decades. We are working with the Office of Naval Research (ONR) on its basic research and applied research program. We are also working with DARPA. We also need to assess future requirements and train people to meet those requirements because you can't hire new engineers and expect them right away to solve the fleet's immediate and long-term technology challenges.

One of the other challenges is that when we develop a new technological solution, transitioning that innovation into a program of record is difficult and can take many years due to the budget cycle. Gary Wang, who is the chief technology officer for TEAM SPAWAR,



Carmela Keeney

is working on moving things more smoothly from the science and technology arena into a program of record where they can be deployed and sustained. He is engaged with NNFE, the Naval NET-WAR FORCENet Enterprise, in terms of identifying capabilities for the generation after next.

CHIPS: *Are you saying that some of the projects that you are working on are not programs of record yet?*

Ms. Keeney: In the science and technology arena, most projects are not acquisition programs of record. We are talking about the early phases of discovery and invention, which organizations like DARPA and ONR support, the basic science and applied research early phase of the spectrum before you go into engineering development, production, and in-service support.

Sometimes you are working on something like nonlinear dynamics. Nonlinear dynamics is a science and technology area that applies to a whole range of capabilities and systems, including communications and sensors, but it is not a formal program of record.

We have identified several key science and technology areas that we are focusing on. Examples of these include: human-information system interaction in distributed computing environments; dynamically reconfigurable networks; dynamic, nonlinear techniques for communications and signal processing; photonic computation; and fusion of geographically dissimilar source data.

CHIPS: *Are these initiatives just applicable to SSC San Diego?*

Ms. Keeney: These are just a few of the technologies that are applicable to the C4ISR (command, control, communications, computers, intelligence, surveillance and reconnaissance) mission area; that is, C4ISR across the board for both the Navy and joint arena, certainly not just to the Systems Center. They are technologies that would apply to warfighting missions and national capabilities in the future.

Two major focus areas for the center are: maritime domain awareness and supporting the global war on terrorism. In the MDA arena one of the major efforts has been supporting the development and fielding of an integrated AIS solution, an Automatic Identification System for maritime platforms. In the GWOT arena, we are applying S&T technologies to the counter-IED problem, antiterrorism and force protection.

CHIPS: You are looking at the whole spectrum of national security?

Ms. Keeney: Right. The priority area of course is a naval focus but we also look at joint and national level C4ISR. For example, we conducted a technology assessment for the Department of Homeland Security on maritime domain awareness. The results of this study were then shared and briefed to other organizations and agencies including the Navy.

CHIPS: One of the challenges you've had is your customers' understanding of how the Navy Working Capital Fund agencies operate.

Ms. Keeney: The Navy Working Capital Fund is a complicated model that requires us to operate like a business. We establish our labor rates two years in advance and then we recover all of our costs from funding provided by the hundreds of projects that we work on. Whether we are working for the Navy, a joint or federal agency, the organization sponsoring that work pays its share of all of our costs including things like salary, benefits, utilities, comptroller or security services.

All these costs are recovered from the projects that we work on, much like private industry. However, we do not generate any profit. When we do joint work, for example, the Navy has the benefit of leveraging the results and knowledge gained from that work — without having to invest its own resources.

While one of the major disadvantages of the Working Capital Fund is that it is not well understood, there are significant advantages. It forces us to have an excellent handle on all of our costs. Nearly every decision we make addresses cost as a major consideration. There are many drivers, both internal and external, that force us to contain and constantly strive to reduce our costs.

At the center, we use tools like activity-based costing and systems enterprise resource planning (ERP) to help us run the business and manage our costs, so that we can get the most out of every single dollar. We realize that there are very limited resources, so we work hard to deliver the most product and service that we can for the funds that we receive. We always strive to be a good steward of taxpayer dollars. The business model helps us do that.

CHIPS: You are one of the original FORCENet technical directors. Can you talk about that initiative and how the technical director's role has evolved over time?

Ms. Keeney: The FORCENet technical directors stood up in fall 2004, the beginning of FY05. At that time I was the FORCENet technical director (TD) for ISR (intelligence, surveillance and reconnaissance) and IO (information operations). There also are a set of deputy technical directors at SSC Charleston. In FY05, the TDs and deputy

TDs accomplished a significant number of critical things. One of the first things they did, working with SPAWAR 05 and the SPAWAR FORCENet domain chief engineers (CHENGs), was to develop and publish the FORCENet Technical Reference Guide. A critical component of this was communicating this technical guidance to the acquisition community, including all of the Systems Center project managers.

Another major effort was implementing a work shaping and acceptance process for all the SPAWAR Systems Centers. This is a process that helps us evaluate and align our work to ensure it is staffed with the right team, at the right cost. We have baselined all of our ongoing work — and this applies to all Systems Centers: San Diego, Charleston and Norfolk.

Before then we pretty much operated as completely independent entities. Proposals now are vetted, reviewed and approved in advance by senior levels before they are released from any Systems Center. We can be sure that we have the right team, the right laboratory infrastructure and the right competencies from across all the Systems Centers to apply to the problem. We are looking at the type of solutions we want to provide so that we can increase our progress in achieving the FORCENet environment.

As part of that work shaping and acceptance process, we have conducted 23 different classes across TEAM SPAWAR at San Diego, Norfolk, Charleston and Hawaii. The classes provide FORCENet guidance, so in addition to learning how to use the tools, we train on what it means technically to have a proposal that is aligned with FORCENet. We used the FORCENet Technical Reference Guide as part of this training. We have had more than 1,100 people attend the training — project managers and line managers — to help them align their projects with FORCENet objectives.

We also held two major FORCENet engineering conferences with more than 1,000 attendees at each to get the word out to the acquisition community, industry, and any other developer, on how to orient their projects, their work, their systems and their future capabilities with FORCENet.

We are also working on technical authority. We have identified a set of technical authority experts, and the TDs and deputy TDs are supporting the SPAWAR technical authority process for TEAM SPAWAR. As we continue in FY06 with work shaping and acceptance, we are also increasing our focus on technical authority and competency alignment.

CHIPS: Can you talk about the organizational improvements that you are making at the center?

Ms. Keeney: At the center, we have had a culture of continuous improvement for several decades. We are constantly striving to improve our processes and the quality of our products and services. We try to make sure that we are cost-effective, deliver quality products and services and that we meet cost and schedule for our customers.

One example of a proven initiative is our software engineering process improvement initiative for CMM, Capability Maturity Model.

In 2000, we were certified as an organization at CMM Level III for software engineering. We are now working toward the Capability Maturity Model Integration for systems engineering, CMMI Level III certification.

Another area we have been working on is project management. This is a center core competency and a process that we want to continually improve on. We have researched the best practices in industry and across government and have developed a project management guide that identifies best practices to be used on all of our projects.

CHIPS: Are you implementing Lean Six Sigma?

Ms. Keeney: Yes, another area is the use of Lean Six Sigma to reduce costs and improve quality and speed of execution. We have several Lean Six Sigma projects ongoing, internal projects and ones we are working across TEAM SPAWAR, in addition to projects for some of our customers to improve cost, speed and quality of the product.

We also use the Balanced Scorecard tool. We have been using that for four or five years to help with strategic planning and to make sure we have meaningful measures for our strategic goals. We are now applying the Baldrige criteria for performance excellence to ensure that the different improvement efforts we have going on are balanced and integrated and include a strong focus on results, not just the process itself. Malcolm Baldrige served as Secretary of Commerce, and his managerial excellence contributed to long-term improvement in efficiency and effectiveness of government.

CHIPS: Can you talk about the leadership exchange between SSC San Diego and SPAWAR headquarters?

Ms. Keeney: We have had a lot of leadership exchange between the Systems Center and Headquarters. That was one of the byproducts of SPAWAR moving here from Washington, D.C. I think it has been a healthy dynamic. To cite some examples, the current SPAWAR Vice Commander, Rear Adm. Tim Flynn, was previously our commanding officer. The current deputy commander for SPAWAR, Rod Smith, was in my position as the executive director here. Dennis Bauman, the Program Executive Officer (PEO) for C4I and Space and the JPEO for the Joint Tactical Radio System, used to be one of our division heads.

There has also been a lot of movement from the PEO and Headquarters to the Systems Center. Capt. Frank Unetic, our CO now, was a program manager in PEO C4I and Space, and the SPAWAR executive assistant. Gary Wang, our chief technology officer, was the head of one of Headquarters' major departments as a program manager. Tim Smith was a PEO program manager and now heads up our Fleet Engineering Department.

Don Endicott started here, went to SPAWAR's Office of the Chief Engineer, came back and is now the head of our Communications Department. He is also one of the FORCENet technical directors.

We see this as a phenomenon that is likely to continue in the future, and we are working to improve our processes to facilitate a healthy exchange of personnel.

As with most government organizations, we have also seen an increase in retirements. We conducted studies in the 1990s that predicted the bow wave was going to happen for us from 2002 to 2008. We took action years ago to adjust our hiring strategy, and this included a significant increase in reinvigorating our New Professional Program.

For more than five years now we have successfully recruited from some topnotch colleges to provide a major infusion of talent and enthusiasm. It has been a great rejuvenation of our workforce. Given the investment that we are making to develop this generation, we are also watching closely our retention statistics and our metrics — and they are looking good.

One of the issues in San Diego is the cost of living. However, even with the high cost of living, we still have a high retention rate for the personnel we have been recruiting. Part of the reason for this is the challenging and interesting work we are engaged in.

CHIPS: That is something to be proud of because of the shortage of graduates with math, science and engineering degrees, there is a lot of competition from industry for the same graduates.

Ms. Keeney: We make a concerted effort and our leadership is actively involved — project managers, branch heads, division heads and department heads. They go to different universities to bring in topnotch talent. We are very happy with the students we have recruited from various universities and colleges. They are very impressive.

CHIPS: I want to congratulate you on your President's Rank Award in 2005. You talked about technical competencies and your award had a lot to do with your outstanding leadership skills. In addition to developing technical competencies for your workforce, are you also looking at leadership skills?

Ms. Keeney: Thank you. Yes, in the late 1990s, we embarked on another organizational improvement initiative called 'High Performance Organizations.' It includes a network talent model that defines four competencies that every individual should have: technical, management, leadership and team skills. So, if you are an engineer, your technical skill is your engineering skill; if you are a security specialist, the security competency is your primary technical skill, and so on. That is the technical base.

The model also says in addition to having strong technical skills, you need to have strong team skills, management skills and leadership skills. Those are the four basic components. To emphasize this, we included it in our Balanced Scorecard, and we evaluate how we are doing during our performance cycle as part of the performance appraisal process.

We have a vision to be the preeminent provider of integrated C4ISR solutions for the warfighter across Navy and the joint and national community, with our primary focus on integrated C4ISR for the maritime domain. That is our goal: to be C4ISR experts that can address tough national security problems across the spectrum from research and development to acquisition, test and evaluation — across the life cycle.

CHIPS

DON CIO Provides Tools for Information Accessibility

By Nicolle Hackman and Scott Lubow



Leading the effort to provide information accessibility for all Internet users, the Department of the Navy Chief Information Officer (DON CIO) recently released the second edition of its Section 508 Self-Help Toolkit. On the heels of Secretary of the Navy Instruction 5720.47A, which set the standards for Section 508 compliance in 2003, the DON CIO developed the self-help toolkit as a means to assist professionals involved with federal information technology (IT) in making their information accessible to all Internet users.

Since the original release of the toolkit, which was requested by multiple DON organizations, the accessibility and usability of DON Web sites have shown marked improvement.

While other informational Web sites and documents exist, DON CIO's Section 508 toolkit is particularly significant because it is a stand-alone tool that provides practical "how to" information for making IT accessible and, with its military examples, is geared specifically toward the Navy and Marine Corps. Additionally, the toolkit is available on compact disc for personnel who do not have Internet access, for example Navy personnel at sea.

The objective of the Section 508 Self-Help Toolkit is to provide the Department of the Navy and the federal sector with a comprehensive "package" of technical guidance and resources to comply with accessibility requirements for Section 508 of the Rehabilitation Act, as amended.

What is Section 508?

In 1998, Congress amended the Rehabilitation Act (29 U.S.C. 794d) and strengthened provisions covering access to information in the federal sector. As amended, Section 508 of the Rehabilitation Act requires access for people with disabilities to the federal government's electronic and information technology (EIT), unless providing access would constitute an undue burden, defined as significant difficulty or expense.

However, even in cases of undue burden, the information and data on government Web sites must still be provided in a reasonable alternate format to those who request it.

The law covers all types of EIT in the federal sector including Web sites, software, computers, copiers, telephones, fax machines and kiosks. The definition of IT used in Section 508 is consistent with that found in Federal Acquisition Regulation (FAR) 2.101: "EIT is any equipment or interconnected system or subsystem of equipment that is used in the creation, conversion or duplication of data or information."

The goals for Section 508 are to eliminate barriers in accessing information technology and to stimulate the development of assistive technologies for better accessibility. Specifically, it applies to six EIT categories: (1) Software applications and operating systems; (2) Web-based intranet and Internet information and applications; (3) Telecommunications products; (4) Video and multimedia products; (5) Self-contained, closed products, such as copiers, printers and fax machines; and (6) Desktop and portable computers.

In addition, product support documentation and support services, including help desks, must now be accessible.

DON CIO's Answer

DON CIO's Section 508 toolkit provides practical information for each of the six EIT categories in a modular approach and explains and offers solutions for working in each area. In addition to individual modules dedicated to each of the EIT categories, it also features sections for acquisitions, accommodations and accessing additional resources.

The toolkit also offers Web resource links that provide a "one-stop-shop" for accessing a multitude of Web sites that contain information about Section 508 and accessibility. For ease of use, the module is divided into relevant categories including: Government Web Sites, Media Web Sites, University/Research Web Sites, Industry/Vendor Accessibility/Section 508 Web Sites, Useful Web Tools and DON Blanket Purchase Agreements.

What's New

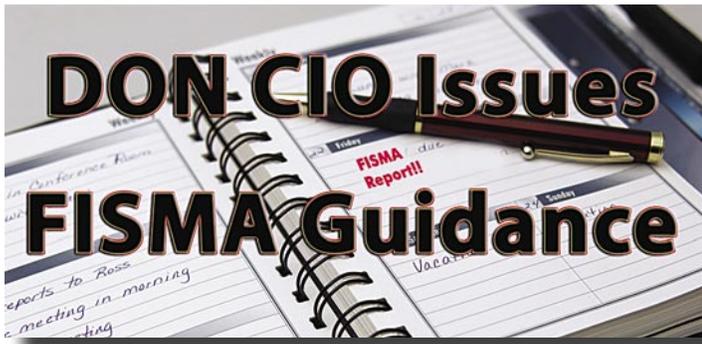
The latest release of the tool adds Microsoft Word, PowerPoint and Adobe portable document format (PDF) modules. These additions provide users with the latest information, guidelines and tips with step-by-step instructions for making documents accessible.

The Word and PowerPoint modules provide information for making files accessible using Microsoft Word and Microsoft PowerPoint. These modules explain key areas such as document structure, templates, styles, forms, tables, and multimedia, as well as how to convert Word documents to accessible PowerPoint and PDF formats.

The PDF module provides information for making new and existing PDF files accessible using Adobe Acrobat versions 6.0 and 7.0. It also explains the inherent issues of image-only PDF files and limitations on the types of files that can and cannot be made accessible. Finally, it offers detailed information on the structure and tags within PDF files and instructions to check the accessibility of PDF files.

The DON CIO remains committed to supporting federal government better business practices and equality in information availability initiatives. The Section 508 Toolkit, which will assist in enabling full Section 508 compliance across the Department, is available on the DON CIO Web site at www.doncio.navy.mil.

Nicolle Hackman, of Burke Consortium, Inc., and Scott Lubow, of Booz-Allen Hamilton, provide Section 508 support to the DON CIO. CHIPS



By Jim Collins

“Each federal agency shall develop, document, and implement an agencywide information security program to provide information security for the information and information systems that support operations and assets of the agency, including those provided or managed by another agency, contractor, or other source...”

– Federal Information Security Management Act of 2002

All federal agencies, including the Department of the Navy (DON), must comply with the provisions of the Federal Information Security Management Act (FISMA) of 2002. Also known as Title III of the E-Government Act of 2002, FISMA requires that each federal agency must provide security safeguards for its information technology (IT) assets.

FISMA Requirements

FISMA mandates that each federal agency report the status of its IT posture to Congress annually. The report must address the adequacy and effectiveness of information security policies, procedures and practices. In addition to the annual report, FISMA requires each agency to conduct an annual independent evaluation of its information assurance (IA) program to determine its effectiveness.

FISMA legislation directed the Office of Management and Budget (OMB) to set standards and oversee FISMA compliance. The DON Chief Information Officer (CIO) coordinates reporting with Navy and Marine Corps activities and sends FISMA reports to the Office of the Secretary of Defense (OSD) Assistant Secretary of Defense for Networks and Information Integration (ASD-NII). The ASD-NII consolidates all Department of Defense data and develops an overall DoD FISMA report for OMB and Congress.

The DON CIO issued DON FISMA Guidance in March 2006 and posted the document on the DON CIO Web site at www.doncio.navy.mil. DON FISMA Guidance provides a foundation for improving the DON's IA posture and outlines courses of action for ensuring compliance with FISMA requirements.

The guidance supports and complements the Secretary of the Navy Instruction (SECNAVINST) 5239.3A, “Department of the Navy Information Assurance (IA) Policy,” which describes FISMA requirements within the DON. It also discusses efforts to improve the DON's overall IA posture, provides metrics to measure specific IA aspects, and includes the DON policy for plans of ac-

tion and milestones (POA&Ms) for correcting information security deficiencies, as required by DON, DoD and OMB policies.

DITPR-DON

The DON variant of the DoD IT Portfolio Registry, referred to as DITPR-DON, serves as a technical database of FISMA assessments, and it maintains the IT system inventory for compliance with Congressional requirements. The Office of the Secretary of Defense uses data from the DITPR to compile reports for internal use and for distribution to OMB and Congress.

The DON uses the DITPR-DON to record the certification and accreditation (C&A) status of Mission Critical (MC), Mission Essential (ME), and Mission Support (MS) DON IT systems and networks. The DON uploads DITPR-DON data into DITPR at least quarterly (March 1, June 1, Sept. 1 and Dec. 1). The ASD-NII uses the data to report DoD FISMA status on a quarterly basis to OMB and annually to OMB and Congress.

The DON CIO submits an annual FISMA report to ASD-NII, which includes data on IT systems and networks, the status of IA training, intrusion incidents, and system/network vulnerability testing. ASD-NII uses each “Defense Agency FISMA Report” to develop its annual FISMA Report to OMB and Congress. Based on OSD's annual FISMA Report, and the evaluation of the DoD Inspector General, Congress then assigns a grade for each agency's information security status.

DON CIO FISMA Guidance

The DON CIO issued the DON fiscal year 2006 FISMA Report Guidance to the DON Navy and Marine Corps Deputy CIOs for forwarding to echelon II commanders, the Marine Corps major commands, and to the Assistant for Administration, Office of the Under Secretary of the Navy (AAUSN), April 21, 2006.

This year, the DON FISMA Report will be due to ASD-NII July 21, 2006. It will include the latest data available from the DITPR-DON as of that date. Since OSD will complete its FY 2006 FISMA Report in September, Sept. 1, 2006 is the last opportunity for the DON to update FISMA data.

Timely and accurate reporting of DON FISMA data to DoD and OMB is essential to demonstrating the DON information assurance posture. OMB requirements to support FISMA may change, so the DON must remain vigilant of the new requirements each year to ensure compliance. For FY 2006, OSD issued new requirements for reaching and sustaining 90 percent or greater full accreditation for systems and networks, referred to as full Authority to Operate (ATO) status.

FISMA Training Requirements

Minimum IA training goals for FY 2006 specify that 96 percent of DON personnel, including contractors, shall complete annual IT security awareness training. This training can be accomplished using the Navy Knowledge Online Web site at <https://www.nko.navy.mil/> or MarineNet at <http://www.marinenet.usmc.mil/>.

For DON personnel, including contractors, with significant IA responsibilities, the DON decrees that 90 percent shall complete

specialized training as specified in DoD Directive (DoDD) 8570.1, "Information Assurance Training, Certification, and Workforce Management" of Aug. 15, 2004, and its associated manual, DoD 8570.01-M, "Information Assurance Workforce Improvement Program."

DON compliance with FISMA requirements ensures that the Department performs due diligence in practicing information assurance, as well as in gathering and reporting data on the security status of its IT systems and networks.

For further information, refer to these previously published FISMA articles available at the *CHIPS* Web links given below.

"The Federal Information Security Management Act of 2002"
– http://www.chips.navy.mil/archives/04_winter/Web_Pages/FISMA.htm.

"FISMA Update" – http://www.chips.navy.mil/archives/05_OCT_DEC/web_pages/FISMA.htm.

Jim Collins is a member of the DON CIO Information Assurance Team.

CHIPS

Sailors Warned of VA Data Compromise

From Chief of Naval Personnel Public Affairs

The Department of Veterans Affairs (VA) announced June 3 that active-duty Sailors may be affected by the theft in May of military personnel data. According to the VA, a duplicate database with data files was stolen from a VA employee's home May 3. While the VA has received no reports that the stolen data has been used for fraudulent purposes, they are asking all veterans to be extra vigilant and to carefully monitor bank statements, credit card statements and any statements relating to recent financial transactions.

Several resources are available for people to go to for more information. The Department of Veterans Affairs has set up a special Web site (www.firstgov.gov) and a toll-free telephone number (800-FED-INFO or 800-333-4636) that feature up-to-date news and information on the data compromise.

The site offers tips on how to check credit reports, how to guard against identity theft and whom to call if an individual believes any fraudulent activity is occurring using his or her personal information.

The Navy and Department of Defense are working closely with the VA to determine how many Sailors and other service members may be affected by the compromise of records. Sailors

whose information has been compromised will be notified by a letter from the VA and the Navy so they can take the appropriate steps.

Tips on how to watch for suspicious activity include the following:

✓ Closely monitor your bank and credit card statements for fraudulent transactions. Monitoring accounts online is the best way to detect fraud early.

✓ Place a 90-day fraud alert on your credit report, which tells creditors to contact you before opening any new accounts or making any changes to your existing accounts. This action may cause some delays if you are trying to obtain new credit.

It is only necessary to contact one of the three companies below to place an alert. That company is then required to contact the other two.

The companies are Equifax (800-525-6285, www.equifax.com); Experian (888-397-3742, www.experian.com); and TransUnion (800-680-7289, www.transunion.com).

Once the fraud alert has been posted, you are entitled to free copies of your credit reports. Review these reports for inquiries from companies you haven't contacted or accounts you didn't open. The alert can be renewed after 90 days. Sailors are advised to take the following steps if they discover fraudulent accounts or transactions:

✓ Contact the financial institution to close the fraudulent account(s) that have been tampered with.

✓ File a report with the local police department.

✓ File a complaint with the Federal Trade Commission by phone at 877-438-4338, online at www.consumer.gov/idtheft or by mailing a letter to Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C., 20580.

Other Web sites with more information on how to guard against identity theft include:

www.privacy.ca.gov/sheets/cis3_english.htm
www.co.boulder.co.us/da/consumer/idtheft.htm

For more news from around the fleet, visit Navy NewsStand at www.navy.mil.

CHIPS

CHIPS Article Guidelines

CHIPS welcomes articles from our readers. Please submit articles via e-mail as Microsoft Word or text file attachments to chips@navy.mil. To discuss your article with a CHIPS editor, call (757) 444-8704 or DSN 564-8704. Go to the CHIPS Web site at <http://www.chips.navy.mil/chipsguidelines.html> for more information.

Combined Endeavor

Combined Endeavor links NATO and Partnership for Peace nations together with advanced technology

By Sharon Anderson

Combined Endeavor is the largest security cooperation and communications exercise in the world. The multinational exercise brings NATO and Partnership for Peace (PfP) nations together to plan and execute interoperability testing of command, control, communications and computer (C4) systems from participant nations to support future combined humanitarian, peacekeeping and disaster relief operations.

The U.S. European Command (USEUCOM) sponsored the twelfth annual "in-spirit-of" PfP communications exercise from May 12 through 25 on Lager Aulenbach in Baumholder, Germany, and at the forward operating site at the U.S. Eagle Base located outside of Tuzla, Bosnia-Herzegovina.

More than 1,200 different interoperability tests were conducted that will be added to the existing 12,000 technical test results currently in the Combined Endeavor interoperability guide. Approximately 1,200 military and civilian experts from 41 partner nations took part in the multinational exercise.

In total, Combined Endeavor 2006 lasted almost two months and was conducted in four phases. In Phase 1 (April 10 - May 5), the host nation, Germany, in conjunction with U.S. Army Europe (USAREUR) and U.S. Air Forces Europe (USAFE) prepared the main operating base (MOB) and the forward operating site (FOS). For Phase 2 (May 5 - May 11), coalition forces deployed to the MOB and FOS and established operating sites. Not only did Germany provide the base for the exercise, it provided 194 individuals for site build-up and tear-down.

During Phase 3 (May 12 - May 25), C4 forces established a core multinational network for common interoperability standards testing. In Phase 4 (May 26 - June 3), the massive assembly of coalition forces and equipment were returned to their respective home nations along with USAREUR and USAFE support elements.

Tests were conducted with navies from several countries including Germany, Italy and Sweden.

U.S. Marine Corps information technology specialists participated as well by chairing the newly stood-up Knowledge Management



U.S. Army Lt. Col. Joe Angyal (left) and U.S. Navy Cmdr. Stephan Abel during a virtual interview conducted May 23, 2006, with Angyal located in Baumholder, Germany at Lager Aulenbach training facility and the CHIPS staff on board Naval Station Norfolk, Va.

Panel and providing on-site expertise to the collaborative portal that was used for all information sharing throughout the exercise.

U.S. Army Lt. Col. Joe Angyal is the Combined Endeavor director. Angyal works directly for Air Force Brig. Gen. Tom Verbeck, Director of Command, Control, Communications and Warfighting Integration, Headquarters, U.S. European Command, Stuttgart-Vaihingen, Germany. According to Angyal, most of the barriers to interoperability among nations involve protocols and security policies.

"The main challenge as we move toward almost everything over IP (Internet Protocol) is sharing information. Often it is not technology; it is the policies that govern or protect that information that seem to be the next challenge that we face," Angyal said.

But interoperability is getting better among partnering nations, according to Angyal.

"There are several demonstrations and tests going on this year which are tackling that challenge head on, how to share information in a multinational environment," Angyal said. "The scenario we are using to test our common operational picture is linked to an earthquake in Armenia, which is linked directly to another U.S. exercise called Rescuer 2006. A Combined Joint Task Force Headquarters is joined together and while staff members are doing humanitarian assistance, there is a radiological device or some sort of dirty bomb set off by terrorists. The scenario goes the full spectrum from assistance to consequence management."

Cultural diversity is also figured into the interoperability piece along with identifying roles and responsibilities and testing doctrine. "If you can think of it as a pyramid and the pyramid was drawn into four layers, the bottom layer would represent human interoperability and the ability to understand each other's cultures and business practices. That is the foundation for testing the interoperability at the other three levels," Angyal said.

"As you move up that pyramid, the next level would be the technical interoperability, the means to pass the 1s and 0s. That would set the stage for becoming interoperable at the procedural level, the policies, the tactics, techniques and procedures that govern the

networks. Finally, at the top of the pyramid would be operational interoperability where we test operationally here in the exercise and then deploy it on a real-world mission."

Led by U.S. forces, no civil or humanitarian organizations participated in Combined Endeavor operations.

"This is a U.S. facilitated event with only military forces here. We exclude private corporations as well. These are the actual people that deploy and fight and use the equipment in the field," Angyal said. "There are other interoperability events, such as Strong Angel, conducted by the U.S. Defense Department that focus specifically on civil preparedness or working with non-governmental organizations."

The virtual interview conducted May 23, 2006, with Angyal located at the Lager Aulenbach training facility and the *CHIPS* staff on board Naval Station Norfolk, Va., used a Web-based desktop video conferencing application called VSee. VSee allows document sharing and the ability to see and hear conference participants via webcams and microphones. Tom Condon, an employee of the Space and Naval Warfare Systems Center Charleston, European Office (SPAWAR Europe) and a captain in the Army Reserve, assisted the public affairs office by keeping the technology up and running for the webcasts.

Emily Snell, another SPAWAR Europe employee, chaired the Knowledge Management Panel that was in charge of providing the tools and technologies for all information sharing requirements for the exercise. The collaborative portal, built on PfP Information Management System (PIMS) technology, provided the single point for all operational and administrative information and was used throughout the planning and execution stages of the exercise.

SPAWAR Europe took over PIMS program management just a little over a year ago. PIMS provides support to Pfp exercises and spearheads knowledge management and information sharing initiatives with Pfp nations, NATO and the United States. The PIMS portal solution that was utilized provided significant benefits to the operations of the exercise and will continue to be used for planning and executing future Combined Endeavors.

In addition to the KM support for both the operational and the public affairs arenas, SPAWAR supported the forward operating site in Tuzla, Bosnia, with hardware, software and network support.

Partnership for Peace is a program of practical bilateral cooperation between individual Pfp countries and NATO. Each of the participating nations has varying degrees of technology development. According to Angyal, one of the big focus areas this year was testing the disparate software tools used by the multinational coalition for displaying the common operational picture. U.S. forces tested C2PC, (Command and Control Personal Computer), an application produced by Northrop Grumman.

"You link to the Blue Force Tracker deployed across the battlespace, and it allows you to see where you are, where your buddy is, and where the enemy is. Since it is commercial software, every nation uses similar software produced by its own nation, and it is tough to get all of those to work together," Angyal said.

Testing is important because technology changes rapidly, according to Angyal. "People ask many times why we conduct Combined Endeavor every year and the very reason is because nations continue on an annual basis to field new and upgraded technology."

Besides the immediate questions of interoperability and planning in the event of a national emergency among member nations, Combined Endeavor also looks at long-range plans with nontraditional partners, according to Angyal. "The long-range plans that we work on here have a global impact. When you deploy, it is common to deploy next to nontraditional partners. We deployed a Polish multinational division and there were officers from countries such as Nicaragua, the Philippines, Mongolia and a wide variety of non-traditional and traditional partners."

"There are similar efforts happening in U.S. Pacific Command called Pacific Endeavor and within USEUCOM. We are doing Africa Endeavor with more than 20 African nations in July. All these efforts are focused on interoperability. The short answer is, we try to integrate the global aspect of this because we work with a different partner or group of partners on every mission," Angyal said.

Although Combined Endeavor is not a formal training exercise, it provides many opportunities for spontaneous learning.

"All of the nations come in at some level of capability. One of the intended consequences is that by working in such a diverse group with such professional people you cannot help but walk away from here a better soldier or a better communicator. But for all of the nations here Endeavor represents a big part of their pre-deployment workup. They practice the things that they do when they deploy, whether it is to Afghanistan, Iraq, Kosovo"

Test results are collected and analyzed by the Joint Interoperability Test Command with the assistance of subject matter experts from the participating countries. The results are published in an interoperability guide that is distributed to the participating nations and has been used as a reference for numerous coalition deployments throughout the world. The interoperability guide is actually a database with information spanning 12 years to the first Endeavor.

"We will have 12,000 after action review comments all stored in this powerful interoperability guide or database. For a multinational communicator, it is like having a copy of the test before the teacher gives it to you. The test is actually when your nation calls on you to deploy," Angyal said.

With the ongoing global war on terrorism and the possibility of a natural disaster or catastrophic event occurring anywhere, cooperation between nations is more important than ever, according to Angyal.

"In today's resource constrained environment, we cannot find a better use for the taxpayer's dollars than the security cooperation that comes from this exercise. When you get a group of 41 nations all working together, this is true phase 0 warfighting. We are working to, first of all, avert your crisis, but in the event of a crisis, to shape the battlespace. That is with 41 nations. That is why we say this is the largest and most effective interoperability effort of its kind." CHIPS



Right, ET2 Jesse Perret. Below, foreground ET2 (SW) Jared Hutchens and IT2 (SW) Dwayne Patton.

The command provides telecommunications, tactical messaging support, and wireless communications as well as Internet Protocol (IP) network traffic to shore facilities and the fleet. In addition, the command provides regional telephone service to customers throughout the Far East.

The Director Communications Security Material System - Electronic Key Management System (DCMS EKMS) Advice and Assistance team calls the command home. The NCTS FE technical control facility houses more than 500 Defense Information Systems Agency (DISA) circuits in addition to Navy and joint command circuits. NCTS FE is also home to the largest EKMS account west of the continental United States and has more than 40 local elements spread throughout its AOR.

NCTS FE has a Defense Messaging System (DMS) Local Control Center, which is the home of the Automated Message Handling System test program. NCTS FE also provides frequency spectrum management services and interference resolution for all of Japan. Its customers include seven flag commands, 13 major commands, many joint commands and multinational partners.

NCTS FE supports the warfighter in the global war on terrorism by delivering services to commands deploying and returning from expeditionary zones. The command also directly supports war efforts through many individual augmentations to Iraq, Afghanistan, the Horn of Africa and U.S. Central Command units.

NCTS FE won the CITE award in the midst of dramatic change. In 2005, NCTS Far East gained increased capability and responsibility by merging with the Information Technology Service Center Far East and the various Base Communication Offices that provide telephone services throughout the region. This merger enabled the establishment of the OCONUS Navy enterprise network known as ONE-NET.

The high morale of civil service and military personnel shows in NCTS FE's high retention rate because NCTS FE personnel perform challenging, interesting work in support of the warfighter — and it's a great place to work.



ET2 (IUSS) Michael Odom is the NCTS FE public affairs officer. CHIPS

The Communications Information Technology Excellence (CITE) award recognizes a command's ability to carry out its assigned missions and perform as an effective part of the fleet's mission essential shore support team. It has been presented to Naval Computer and Telecommunications Area Master Stations and detachments that fall under the Naval Network and Space Operations Command (NNSOC) claimancy.

The winners of this award have consistently demonstrated the highest degree of professionalism and expertise characteristic of Sailors and civilian personnel attached to winning commands. This year NNSOC recognized the hard work and dedication exhibited by the personnel of Naval Computer and Telecommunications Station Far East by naming it the "Telecommunications Station of the Year."

"It is truly an honor to receive the Naval Network and Space Operations Command '2005 CITE Station of the Year Award.' This award tells everyone that our team is indeed the best Naval Computer and Telecommunications Station in the world. It is our Battle 'E' and a testimonial to the dedication and professionalism of the Sailors and civilians that make up NCTS FE. This award recognizes the tremendous growth of our command in the last year with the assumption of base networks as well as the rollout of ONE-NET," said Cmdr. Tina Swallow, commanding officer of NCTS Far East.

NCTS Far East is a tenant of the Commander Fleet Activities Yokosuka, Japan. It has a large area of responsibility (AOR) and provides such a wide variety of services that the excellence recognized by the CITE award is a recognition of the NCTS Far East entire team of more than 800 personnel serving in outlying sites in Misawa, Sasebo, Okinawa and Kami Seya, Japan, Chinhae, Korea, and the Naval Air Facility Atsugi, Japan.

Wherever NCTS FE personnel are stationed, the CITE award reflects the combined contributions of Sailors, civil service employees, Japanese master labor contractors, and other contractors stationed throughout the region.

NCTS FE Sailors and civilian personnel deliver reliable and secure communications and information technology services to the Far East region. With detachments scattered across the Far East, the AOR for NCTS FE spans beyond Japan, reaching from Diego Garcia to Korea and Singapore to Guam.

Communicating from the field with the Australian Army

By U.S. Navy Cmdr. Danelle Barrett

U.S. Pacific Command's Standing Joint Forces Headquarters (SJFHQ) participated in Exercise Vital Prospect with the Australian Defense Force (ADF) May 2-13 at the Greenbank training area in Queensland, Australia. This yearly event, conducted by the ADF, is an exercise for the Headquarters Joint Operations Command in Sydney to evaluate Headquarters 1st Division's performance as the land Deployable Joint Forces Headquarters (DJFHQ).

In existence since 1997, the DJFHQ's charter directs the DJFHQ to command a major joint task force. Specifically, its mission states: "On order, provide ready, deployable and sustainable land forces to conduct joint operations within Australia's Area of Interest in order to support Australian national interests."

The DJFHQ's most recent full operational deployment was in response to the 1999 East Timor crisis, when a cadre of more than 1,200 were sent to Dili, East Timor, for more than six months. Elements of the DJFHQ were also deployed for tsunami relief efforts in the region. DJFHQ's annual certification exercise keeps the staff prepared to respond to a variety of emergencies.

Communications personnel and equipment enable command and control of joint forces that are instrumental to successful DJFHQ mission accomplishment. Communications for the DJFHQ are provided by the First Joint Support Unit under the leadership of Australian Army Lt. Col. Shaun Love, who is also dual-hatted as the J6 (head of command, control, communications and computer systems) to the Headquarters 1st Division. Lt. Col. Love and his team managed all communications planning and execution during Vital Prospect, and were directly supported by the 101 Signal Squadron based in Brisbane.

Vital Prospect Technical Overview

During Vital Prospect, the fictitious country of Kamaria takes aggressive action in the region threatening its neighbors. Australia, backed by a United Nations resolution, steps in to diffuse the situation and return the region to status quo. The main objectives of the exercise included:

✓ Form and operate a combined/joint task force headquarters in a deployed environment.

✓ Test communications systems processes and procedures in a joint environment.



Scientists from the Australian Defense Science and Technology Office (DSTO), left to right, Thomas Cox, Chris Cocks and Philip Stimpson.

✓ Test emerging technologies proposed by the Australian Defense Science and Technology Organization (DTSO).

Architecture Overview

To meet these objectives, the DJFHQ and the 145-member 101 Signal Squadron deployed to the Greenbank training area and established the entire communications infrastructure within four days. The architecture included a mesh topology with almost 10 megabits of bandwidth received over 11 mobile satellite terminals transferred over terrestrial networks covering 29,795 meters of cable at the exercise location. The total bandwidth managed during Vital Prospect exceeded that of any previous DJFHQ exercise. Service provided by the 101 Signal Squadron was exceptional with connectivity reliability exceeding 99.9 percent.

The backbone of the deployed communications was the Battlefield Telecommunications Network (BTN), also known as "Project Parakeet." This system encompassed a range of satellite terminals, circuit and packet switching systems, asynchronous transfer mode switches, frame relay for data interface, and line-of-site radio relay equipment. The satellite terminals interfaced into two strategic sites terminating at Melbourne and Brisbane. Services were then connected from the BTN to the Defense Communications Network, the Australian strategic communications backbone.

Satellite connectivity is essential for the ADF, and much like U.S. Pacific Command's SJFHQ, the DJFHQ is dependent on satellite services for effective command and control. The communications architecture for Vital Prospect incorporated a robust voice, video and data network with connectivity via the Australian Defense Satellite Communications Capability. ADSCC comprises a combination of commercially purchased and leased satellite transponder capability across the X, Ku, Ka, C and L bands through several service providers including Singtel, Intelsat and Inmarsat.

The Defense Payload Segment, owned by the Australian government on Singtel's Optus C1 satellite, includes an X-band payload using four transponders with Earth, regional and spot beam coverage features, an X/Ka crossband capability, and a UHF Earth coverage

beam with six channels, one 25 kHz and five 5 kHz channels. This satellite provides a majority of the connectivity to deployed units in the Australasia area.

Optus B1 satellites provide Ku-band capability. However, the Ku spot beam covers only Australia and its surrounding waters, C and X-band must be used when forces move outside that spot beam. Inmarsat (L-band) and Intelsat (C-band) assets are leased on an as needed basis to augment bandwidth beyond what is available on Optus satellites.

Iridium (L-band) service is also leased for non-secure satellite phones for tactical deployers, and the DJFHQ has four Iridium handsets. X and Ku- bands are used primarily for critical command and control communications. The Ka-band is used for non-critical command and control support functions and systems like the ADF's Theater Broadcast System, which is similar to the U.S. Global Broadcast System.

The main control of the payloads and management of satellite apportionment is done at the Defense Payload and Operations Control Center at HMAS Harman, which is actually a naval station outside Canberra. The UHF satellite communications are controlled via the Naval Communications Area Master Station Australia.

The DJFHQ field headquarters was spread over a quarter mile area and consisted of approximately 40 temporary shelters that had to be wired for voice and data. The 101 Signal Squadron laid over 13,150 meters of copper cable and 16,645 meters of fiber optic cable within four days to ensure connectivity to all key players.

The Australian classified intranet, the Defense Secret Network (DSN) ran on a 100 percent multi-mode fiber backbone for compliance with Australian network security accreditation rules. The Defense Network Support Agency (DNSA) in Canberra sets configuration standards, and network security is a priority.

The DNSA has oversight of the activities on the tactical servers, routers and switches and can provide assistance remotely. This ensures a high degree of configuration control and enables rapid technical support to field units. The main applications on the DSN are Llama/Cheetah, a Windows-based program to display the common operational picture, and the Command and Control Personal Computer (C2PC), which is the same program used on U.S. military networks, Lotus Notes for e-mail, logs and databases, and Microsoft XP.

The Australian "For Official Use Only" network, the Defense Restricted Network (DRN), is similar to the U.S.'s NIPRNET. DRN runs a copper category five-cable backbone. The main applications on the DRN are Lotus Notes for unclassified e-mail and databases, Internet access and Microsoft XP. The local DJFHQ information manager determines who has permissions for

access to e-mail and other applications/databases on the network. Communications planners for the Headquarters 1st Division are exploring options for Web-based solutions to improve data and information management.

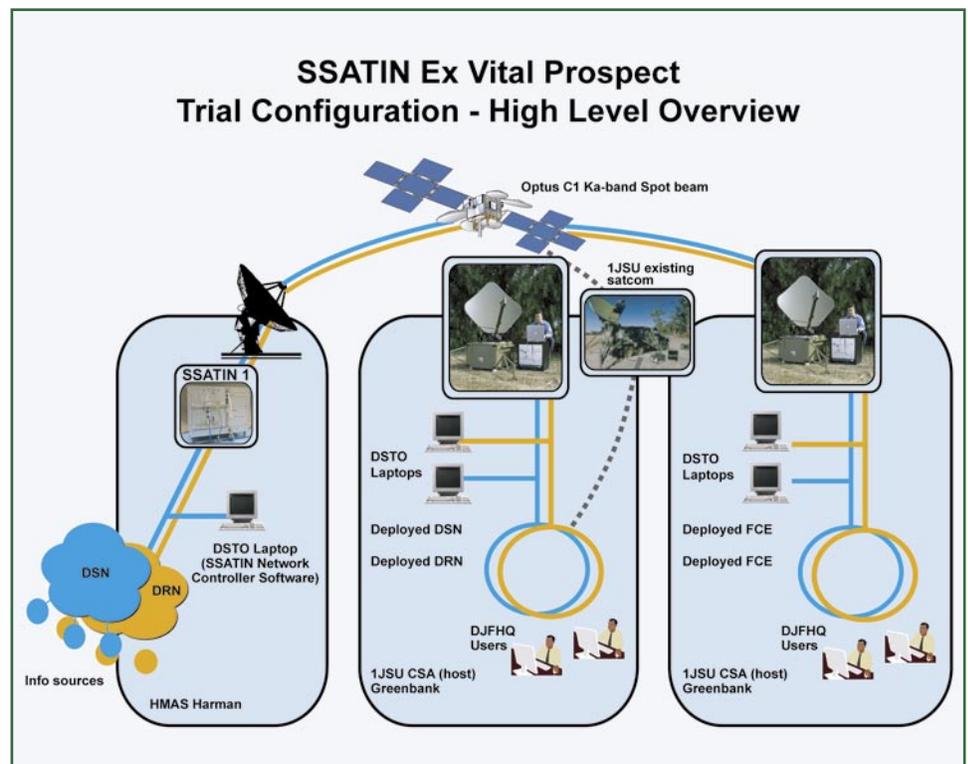
In addition to the BTN, other key services included a robust tactical voice system with 158 secure, digital voice data terminal adapter phones by British Aerospace Australia, 36 non-secure phones, and the Defense Integrated Secure Communications Network for record message traffic.

SSATIN

One of the exercise objectives was to test emerging technology for potential military application. To that end, the DSTO Information Network Division brought the Secure Satellite Internet Protocol Network (SSATIN) to test access on-demand and bandwidth-on-demand technology in a secure deployed environment. Specific goals of the SSATIN program as identified by the DSTO are:

- ✓ Access-on-demand
- ✓ Bandwidth-on-demand
- ✓ Automated user terminal
- ✓ Automated network control
- ✓ Native support for IP traffic
- ✓ Highly dynamic network control
- ✓ Fully meshed network
- ✓ Military-grade security architecture
- ✓ Efficient use of satellite bandwidth

SSATIN (shown below) has many advantages over the traditional link-based architecture currently in use by the ADF. The legacy link-based architecture uses frequency division multiple access, which is not the most efficient way for several terminals to share the ag-





Members of the Australian Army 101 Signal Squadron during Exercise Vital Prospect were joined by U.S. Pacific Command's Standing Joint Forces Headquarters (SJFHQ) May 2-13 at the Greenbank training area in Queensland, Australia.

gregate available bandwidth, nor does it allow for prioritization or quality of services on data and voice transmissions of Internet Protocol (IP) traffic. SSATIN uses a time division multiple access method to allocate bandwidth more efficiently.

The bandwidth is shared between networks of different classifications and is dynamically reassigned based on individual node demand. Less active nodes have bandwidth reduced while more active nodes have it increased automatically. Both synchronous and asynchronous transmissions are supported, including such technologies as Voice over IP (VoIP) and IP multicast.

Two radio frequency satellite terminals were used for the SSATIN test at the exercise location with an aggregate 1 Mbps over Ka-band links. These terminals, using one-meter carbon fiber dishes, connected in a spot beam of the Optus C2 satellite.

The bandwidth for the entire network was controlled by administrators at a third SSATIN terminal located at HMAS Harman, while local administrators controlled bandwidth allocated for specific services within each node. A typical reallocation from the central controller took less than a second, including satellite latency. Although the current equipment for the system is not Joint Tactical Radio System compliant, the Australian military services are interested in pursuing use of JTRS in future engineering efforts to ensure interoperability with coalition partners.

The overall results of the test were extremely positive and the DSTO engineers intend to continue refining the systems for possible future deployment.

The Communications Management Group (CMG), a team of seven DJFHQ personnel working for the J6, managed communications oversight during the exercise centrally at Greenbank. Managed in similar fashion to U.S. Joint Communications Control Centers, the CMG provided 24-hour oversight of operational and strategic communications links.

Army Maj. Adam Dunn, a 10-year veteran of the Australian Signal Corps, led the group. Dunn recently finished a 24-month exchange tour with the U.S. Army at Fort Gordon, Ga., and the 11th Signal Brigade in Sierra Vista, Ariz.

"The exercise was a success because it gave the 1st Joint Support unit the opportunity to practice deploying a network that genuinely tested the unit's wideband capability. Being static once we deployed the network, we suffered very few outages, and as a result, we were able to provide a high level of quality communications and information systems support to exercise participants," Dunn said.

Declaring Success

The ability of the Australian Army to have a deployable and fully functional DJFHQ, capable of command and control of joint forces from anywhere in the Australasian area, is essential to its regional and national security strategy. By flexing its communications capabilities and testing emerging technologies during field exercises like Vital Prospect, the Australian Army is leading the way in demonstrating excellence in deployable command and control.

"In terms of technical control, the exercise gave the DJFHQ J6 Branch the opportunity to practice as a CMG for the first time this year. The CMG was able to manage a complex network that was the key enabler to HQ's ability to practice its operational procedures in a field environment. Overall, there's room for improvement, always is, but the exercise has been a success for the DJFHQ communicators," Dunn said.



Cmdr. Danelle Barrett is an Information Professional Officer assigned to Standing Joint Forces Headquarters, U.S. Pacific Command. CHIPS

Training Navy Employees to Protect Data at Home and on the Road

By Lt. Sean W. Kelley

Background

Department of Navy (DON) employees frequently work at home. In the office, there is a staff dedicated to the protection of data. But how safe are data when employees work at home or on the road?

The Gartner Group estimated that by 2008, 41 million corporate employees globally will spend at least one day a week teleworking, and 100 million will work from home at least one day a month. The highest proportion of these will be U.S. workers. Further, Gartner specifies that these numbers do not represent the number of employees that are on the road for official business.

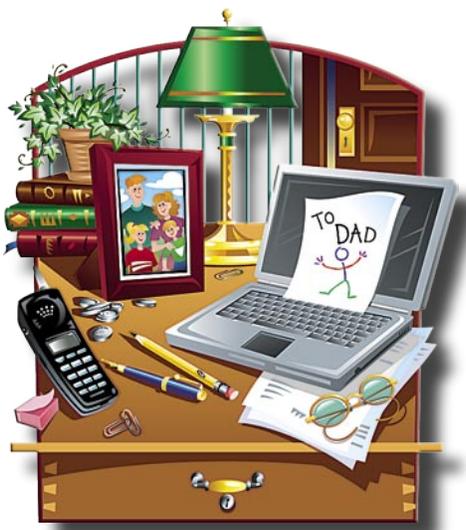
In addition, findings from the Gartner Symposium/ITxpo 2003, reported that wireless users in North America will grow from 4.2 million in 2003 to more than 31 million in 2007.

Working at home is an opportunity for personnel to spend time with their families while preparing for the next day, and many of us are often required to work in a mobile environment. But these statistics should make the need for a home security training program even more obvious.

It is crucial for all organizations to look at home network use when building their data security strategy. Every organization should have an Information Security Awareness Program. Each ISAP should cover the requirements of Navy information assurance. The goal of IA is to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation. Information assurance is essential for warfighting and homeland defense, and is required operationally throughout the Department.

Mandatory Training

All authorized users (military, civilians and contractors) of Department of De-



fense information systems were required to complete IA awareness orientation training by Sept. 1, 2005. IA awareness training is available for the DON through Navy Knowledge Online (<http://www.nko.navy.mil>) and MarineNet (<http://www.marinenet.usmc.mil>).

Depending on your organization, the command information assurance manager (IAM), information assurance officer (IAO) or information systems security manager (ISSM) is responsible for ensuring that all personnel with active user accounts complete initial or refresher training.

The course takes about 30 minutes to complete and explains the importance of classified information and how to protect it from unauthorized users both inside and outside the workplace.

For more information and step-by-step instructions for accessing IA training, please visit the IA workforce page of the DON Chief Information Officer (CIO) Web site at <http://www.doncio.navy.mil/iaworkforce/>.

The DON has deployed this centralized training module, but training should be complemented with a comprehensive training program at each command to include the protection of unclassified data and networks.

Training should include the security requirements of what to do when working at home and on the road. For guidance, refer to the Secretary of the Navy Information Assurance Manual (SECNAV M-5239.1) of November 2005 (http://neds.daps.dla.mil/Directives/5239_1.pdf/).

DON Guidance

The Bureau of Naval Personnel Instruction 12300.2 defines the requirements of the Navy's Telecommuting (Telework) Program. The instruction states: "At a minimum, all telework agreements must address the location and requirements of the alternative worksite, telework schedule, security of official information, protection of Government-furnished equipment, applicable standards of conduct, liability and injury compensation, and Government access to the alternative work site."

Per the DoD Telework Policy (Oct. 2002), the primary medium for teleworking on a regular basis (*one day or more per pay period*) should be a government-provided desktop or laptop computer or BlackBerry device. Personal computers may be used for ad hoc teleworking on limited amounts of sensitive unclassified material, as long as it is deleted once no longer required.

Ad hoc access to DON e-mail or scheduling functions through Outlook Web Access, requires command approval for access to OWA, a computer meeting the required configuration, and the use of a Public Key Infrastructure (PKI) certificate for authentication.

Users will need a Common Access Card (CAC) reader and the associated middleware on their personal computer to enable PKI authentication. The current DON policy, including computer configuration requirements, is available by searching for "remote access" on the DON CIO Web site at <http://www.doncio.navy.mil/>.

DON organizations should take steps to ensure that teleworkers and travelers are properly trained. In some cases, I have seen users connect to hotel networks and accidentally load malicious software on their personal laptop or computer resulting in the inability to complete their work. How does the DON deal with these issues?

Free Antivirus Protection

Antivirus software that provides multi-layered protection at the desktop, server, gateway and network levels is available for download at no charge to your organization. Antivirus software available for download includes McAfee, Symantec and Trend Micro products.

DoD users with a dot-mil address, including all combatant commands, military services, agencies and military academies; personnel within joint, NATO and coalition forces; contractors authorized to use government-furnished equipment; and the Coast Guard are authorized to download and use this software.

Products are available for home computers, home and office firewalls, and wireless or personal digital assistants. By expanding products to home use, the DoD is acknowledging that safeguarding computers at home is as important as safeguarding computers in the workplace. These products can be downloaded by linking to either of the following Web sites.

NIPRNET Site: http://www.cert.mil/antivirus/av_info.htm

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

Build a Defensive Program

For teaching a home security course, allow at least three hours for instructor-led training. Tailor the presentation to home and mobile users. Try to brief to the lowest knowledge level but ensure the advanced user is also challenged.

Below is a sample outline identifying material that should be covered.

✓ Explain the importance of computer security and how it should be applied to home use.

✓ Provide statistics regarding Internet threats. For example, Carnegie Mellon's CERT® Coordination Center Web site maintains incidents up to 2003. Though it discusses corporate statistics, it illustrates how Internet threats have grown: 1998 – 6 incidents; 2003 – 137,529 incidents.

✓ Explain the consequences of malicious code: viruses, worms, Trojans and spyware, and the dangers of opening e-mail attachments from unknown sources.

✓ Explain the importance of backing up data!

✓ Discuss the importance of having an antivirus, firewall and spyware removal

tool on home and laptop computers and keeping them up to date.

✓ Explain the dangers of broadband access, wireless networks and security.

✓ Explain what to do if computing devices have been hacked or there is a security violation.

✓ Discuss phishing scams and spoofed e-mails.

✓ Direct the use of good password management using strong passwords that are changed every 90 days.

For home users discuss identity theft and scams, Web browser security and protecting children from the dangers of chatrooms, blogs, pornography and "MySpace." Discuss Web protection and Web filtering mechanisms and online music downloads and software piracy.

Discuss environmental controls, such as electric power and uninterruptible power supply, temperature, humidity and the consequences of spilling food or drinks on computing equipment.

I advocate a classroom setting, but if that is not feasible, online training is the next best option, but ensure that there is a mechanism to encourage user discussion and to answer questions.

Be Vigilant!

Thanks to the Internet we can stay connected at home, on the road and in the office. But the data DON personnel handle in mobile settings are as important as data handling in the office.

Use of antivirus software with current virus definitions, a personal firewall, anti-spyware software, and PKI are all tools that can help ensure safe and secure computing from both home and mobile environments. A virus that destroys your files at home results in lost productivity and may be a source of vulnerability to Navy networks.

Telework will change the lifestyles of DON users to enable a more flexible work environment, but users must remain vigilant in protecting data. Our lives could depend on it!

Resources

In addition to DON and DoD guidance organizations like Carnegie Mellon's CERT® Coordination Center and the SANS Institute have created home network security education guidance. Microsoft has a Web site devoted to educating the home user on security matters at <http://www.microsoft.com/athome/security/default.mspx/>.

The SANS Institute offers a "Computer and Network Security Awareness" course that can be purchased for \$1,000 for a one-year subscription. Purchasers can make unlimited copies for their organizations for the subscription period. More information is available at <http://www.sans.org/staysharp/description.php?tid=311/>.

Additional resources to assist you in building your home security awareness course are available at the CERT Coordination Center's Home Network Security Web site at http://www.cert.org/tech_tips/home_networks.html.

The National Cyber Alert System was created by US-CERT and the Department of Homeland Security to help you protect your computer. One of US-CERT's overarching goals is to ensure that you have access to timely information about security topics and events. Go to http://www.us-cert.gov/referral_pg/.

Home PC Firewall Guide: <http://www.firewallguide.com/>.

ProtectKids.com: <http://www.protectkids.com/dangers/>.

"Cyberwatch" - a cyber safety site by M.E. Kabay Ph.D., associate professor of information assurance at Norwich University: <http://www2.norwich.edu/mkabay/cyberwatch/index.htm>.

Lt. Sean W. Kelley is the head for Information Technology and Communication Services at the Bureau of Medicine and Surgery. He is a Medical Service Corps officer with an IM/IT subspecialty. He has a master's degree in computer resource and information management from Webster University and a master's degree in information systems technology from the Naval Postgraduate School.

CHIPS



Interview with Lt. Cmdr. Jim McGowan
Nutrition Programs Manager
Physical Readiness Branch (PERS 676)
Navy Personnel Command

Lt. Cmdr. Jim McGowan is a Registered Dietitian (RD) and member of the Medical Service Corps with a Master of Science degree. Just before his departure to the Naval Hospital Sigonella, Italy, in June, to report as the department head of nutrition management, CHIPS asked McGowan about his experiences as the Nutrition Programs Manager for the Navy and advice for a healthy lifestyle.

CHIPS: Do you think the increase in use of electronic games and devices among young adults and children has contributed to the sedentary lifestyle in these previously active age groups?

Lt. Cmdr. McGowan: If you wanted to determine why someone has become sedentary and look at different electronic devices, you could say that video games might be a contributor. Many children and young adults would rather sit in front of the television for hours playing Xbox, PS2 (PlayStation 2), etc., instead of riding a bike, running or playing.

However, while it is easy to say that inactivity is caused by spending too much time playing electronic games, the root cause is much bigger. Often parents allow this behavior to occur instead of encouraging outside activities. Physical activities in schools have also decreased giving the children the option of computer time or play time leading to more sedentary children.

CHIPS: Technology is so much a part of our lives, could technology play in a role in encouraging people to become physically fit?

Lt. Cmdr. McGowan: Absolutely. There are many computer-based programs for children which promote healthy eating and increased activity. Also, many people use pedometers (step counters) to measure calories burned. Some pedometers can be connected to a personal computer to upload data for analysis. The bottom line to remember is that no matter how fancy the program or device, you still have to get out there and exercise.

CHIPS: What do you say to someone who tells you that my job is too important; I don't have time to exercise or eat healthy? Does stress play a role in poor eating habits?

Lt. Cmdr. McGowan: 'I don't have time to exercise' is the biggest

excuse I hear. And while your job may be important, if you are not able to perform your job due to poor health (resulting from a sedentary lifestyle and unhealthy eating), then everyone loses. Most people think that exercise is a formal routine that requires at least an hour in the gym; however, all activities count toward exercising. Planning is the key. The 2005 Dietary Guidelines for Americans recommends the following regarding activity... (See the text box on the next page.)

We all have a certain amount of stress in our lives. Excessive daily stress often leads to unhealthy eating habits and health problems. The goal is to find ways to manage it. Most bases have Health Promotion Centers which offer stress management classes. Additionally, exercise is an excellent stress reducer!

CHIPS: How would you counsel someone who has a longtime history of poor nutrition habits and a sedentary lifestyle to begin a healthier lifestyle?

Lt. Cmdr. McGowan: I start from scratch. I have service members keep a food diary for a week. In this diary, they write down everything they eat and drink, and I mean everything — breath mint, onion slice, sip of a soda — then I meet with them and discuss the diary, any medications, all activities, food likes and dislikes, medical problems, and so on.

I then calculate balanced meal and exercise plans, and discuss some basic nutrition and serving sizes. Most importantly, we work on a plan together that fits into their schedule and lifestyle. We then meet every one to two weeks to review the food diary, discuss any setbacks and make short term goals. This continues until it becomes a part of their routine. It's the behavior that must be changed.

CHIPS: What is the ShipShape program?

Lt. Cmdr. McGowan: ShipShape is the BUMED-approved weight management program. It is an eight-week program that reflects the current state of knowledge on weight loss. It is specifically designed to provide active-duty personnel with basic information on nutrition, stress management, physical activity, and behavior modification techniques to lower and maintain an acceptable body weight within Navy standards.

ShipShape is a healthy and permanent approach to weight loss. Attendance is open to all personnel, especially to active duty members who exceed, or are in danger of exceeding, body composition assessment (BCA) standards. Complete information on ShipShape may be found at <http://www-nehc.med.navy.mil/hp/shipshape/>.

CHIPS: The Naval Supply Systems Command created a healthy menu for galleys that offers baked goods and low fat food. What are some of the food choices that military members could expect to see?

Lt. Cmdr. McGowan: We all like to have a choice, especially when it comes to food. The focus is to educate Sailors to make healthier food choices. Today's galleys have more baked and low fat



Atlantic Ocean (April 29, 2006) - Airman John Lujan takes time out of his day for fitness to ensure he is ready for the upcoming semi-annual physical fitness assessment aboard the Nimitz-class aircraft carrier USS Dwight D. Eisenhower (CVN 69). U.S. Navy photo by Photographer's Mate 3rd Class Andrew Geraci.

food choices. A complete listing of recipes may be found on Navy Knowledge Online or the Naval Logistics Library (<https://nll1.ahf.nmci.navy.mil/recipe/>).

One misconception is that you can eat more food if it's lower in fat. While lower fat is healthier, the problem then becomes too many calories. Typically if you eat more calories than your body requires (and burns), it gets stored as energy (fat). The following paragraph is from the NAVSUP Web site ...

"Nutrition is a hot topic today, and the Navy's senior leadership is aware of the enlarging waistline and increase in Sailors' weight. A new requirement for the NAVSUP Registered Dietitian is to publish the metric of how many menu reviews conducted receive a passing score of 90 percent or better. The head of NAVSUP reviews this metric."

In accordance with the NAVSUP P-486, there is a requirement to have a mandatory annual menu review performed by the NAVSUP dietitian for all galleys. This evaluation includes a variety of criteria and receiving a score of 90 or greater indicates that a command is providing a menu that meets the nutritional guidelines outlined in Chapter 3 of the P-486. This publication contains all pertinent information necessary to write a menu that provides adequate nutrition and choices for Sailors.

Following a menu review, commands are mailed a package with recommendations for improvements to the menu, along with nutrition education materials. Commands scoring less than 90 percent are required to make the recommended changes and resubmit in order to achieve an acceptable menu score.

All commands have a copy of the P-486, and culinary specialists responsible for developing menus should be thoroughly aware of the contents contained in Chapter 3.

CHIPS: Why is it important to take a total approach to wellness?

Lt. Cmdr. McGowan: We must all be conscious of our total health. It's more than just eating right and exercising. Managing stress, tobacco cessation, alcohol responsibility, drug awareness and mental health are just as important. As I said, our bodies only require a certain number of calories (*taking into consideration the amount of exercise, metabolism, age, health and so on*), anything above that number gets stored as extra weight (fat).

Commands interested in starting a ShipShape program can go to the Navy Environmental Health Center (NEHC) site at www.nehc.med.navy.mil/hp/shipshape/index.htm. There are resources on this site also available to civilian personnel.

The self-study guide is available (along with other health and nutrition resources) to anyone and can be found online at www.npc.navy.mil/CommandSupport/PhysicalReadiness/Nutrition.

For related news, visit the Navy Personnel Command Navy News-Stand page at www.news.navy.mil/local/npc/.

Editor's Note: Cmdr. Alice Whitley is the new Navy Nutrition Programs Manager. CHIPS

Recommendations for a Healthy Lifestyle

Engage in regular physical activity and reduce sedentary activities to promote health, psychological well-being, and a healthy body weight.

To reduce the risk of chronic disease in adulthood: Engage in at least 30 minutes of moderate-intensity physical activity, above usual activity, at work or home on most days of the week.

For most people, greater health benefits can be obtained by engaging in physical activity of more vigorous intensity or longer duration.

To help manage body weight and prevent gradual, unhealthy body weight gain in adulthood: Engage in approximately 60 minutes of moderate to vigorous intensity activity on most days of the week while not exceeding caloric intake requirements.

To sustain weight loss in adulthood: Participate in at least 60 to 90 minutes of daily moderate-intensity physical activity while not exceeding caloric intake requirements. Some people may need to consult with a healthcare provider before participating in this level of activity.

Achieve physical fitness by including cardiovascular conditioning, stretching exercises for flexibility, and resistance exercises or calisthenics for muscle strength and endurance.

Put down that PDA and get moving!

Investing in the Navy's Future

By Jacqui L. Barker, Public Affairs Officer Combat Direction Systems Activity Dam Neck

Transforming the Department of the Navy into a "Total Force" often requires asking individuals to work harder and sacrifice more than they ever have in our Navy's history. Personal sacrifice may be required not just of military personnel, but also the civilian workforce, who also support the Chief of Naval Operations Sea Power 21 initiatives and Naval Sea Systems Command (NAVSEA) operations.

This type of commitment can be found at the Combat Direction Systems Activity Dam Neck, Va. CDSA Dam Neck is a NAVSEA Enterprise Warfare Center within the Naval Surface Warfare Center (NSWC) Dahlgren Division. Its mission is to provide acquisition support, life cycle maintenance, test and delivery for carrier, amphibious, frigate, and non-Aegis combat direction systems, advanced sensor distribution systems, and other software-intensive combat control and electronic intelligence systems.

Two civilian employees, dedicated to the CDSA Dam Neck mission answered a challenge to support NAVSEA's vision to "Put the right capability in the hands of the warfighter at the right time at the right cost."

In response to a request from the Program Executive Office for Integrated Warfare Systems to the NSWC Dahlgren Division for help on CVN 21, the 21st century aircraft carrier program, Allen Morrison and Kevin Long volunteered to assist the PEO IWS located at the Washington Navy Yard.

The CVN 21 program is the future aircraft carrier replacement program for USS Enterprise and CVN 68-class aircraft carriers. A centerpiece of the Sea Strike pillar, and integral to Sea Shield and Sea Basing, CVN 21 will be the premier forward asset for crisis response and early decisive striking power in major combat operations.

CVN 21 and the carrier strike group will provide rapid response, endurance on station, and multi-mission capability. CVN 21 balances improved warfighting capability, quality of life improvements and reduced acquisition and life cycle costs.

The first new aircraft carrier design in more than 40 years, CVN 21 will share a Nimitz-class hull form with a completely reconfigured internal space arrangement and flight deck layout. Northrop Grumman was awarded a \$108 million contract to begin design of the CVN 21-class nuclear-powered aircraft carrier in 2003. Advance construction began in 2006. Commissioning is expected to be in 2014.

Morrison, an employee from the Combat Direction Systems Branch, spent 17 months providing technical support for CVN 21 initiatives. Long, an employee from the Systems Management Engineering and Analysis Branch, replaced Morrison in the PEO IWS office in October 2005 and will serve for one year.

PEO IWS provides the Navy with fully integrated and certified warfare systems. The CVN 21 class of carriers is the first to have shipboard systems that are totally integrated. Long coordinates and manages the integration and installation of the warfare system within the new CVN 21-class hulls.

"The significance of working on CVN 21 warfare systems is that you are develop-

July 8, 2005 - Artist's concept of CVN 21 – one of a new class of aircraft carriers. The new nuclear propulsion plant will require fewer operators thereby lowering life cycle costs, and provide increased electrical power that will be available for the demands of developing technology. Smart sensors will assist in further reducing Navy watchstander requirements and in automating damage control functions such as detecting fire and flooding situations. Flight deck redesign and a transition to an advanced aircraft recovery system (AARS) will reduce crew workload, enhance safety and reduce the costs of operating and maintaining a carrier throughout its planned 50-year life cycle. U.S. Navy graphic.



ing the warfare system for aircraft carriers that will impact our fleet for the next 50 to possibly 100 years," Morrison said.

Morrison served as the senior civilian technical NSWC representative for PEO IWS 1A4B. His tasks included defining requirements, system engineering, program development, systems integration, testing and certification. His responsibilities required an understanding of contracting, budget development and management, and lifetime support engineering.

"The work environment is very dynamic, so there is never a dull moment," Morrison said. "I was able to see first hand the incredible process that makes up the Navy acquisition world and see how complex it really is. This was one of my most challenging assignments."

Long develops technical based reviews to support flag level briefs, coordinates schedules for PEO IWS and PEO Aircraft Carriers. He assists in the management of the warfare system integration contractor. He also leads various working groups to help establish interoperability of the CVN 21 class hulls within the Navy's vision of FORCENet.

"I have a new respect for the acquisition community. I was able to understand why decisions are made, ones that I could not fully understand before. Additionally, I

enjoyed the challenge of bringing together a team across three SYSCOMS (systems commands) to give CVN 21 the best warfare system possible and to provide our Sailors with warfare systems that work as advertised. I hope I made a difference in making that happen," Morrison said.

According to Capt. (Sel) James Downey, PEO IWS deputy director for Warfare Systems, Long and Morrison assisted in the program's achievement to Milestone B.

Supporting the largest acquisition program in the Defense Department, they assisted in CVN 21 certification of the C4I support plan; approval of the information support plan; processing hundreds of ship design products within an extremely aggressive schedule; establishment of a warfare system baseline control process; development and employment of sophisticated and repeatable systems engineering processes across industry and government activities, including hundreds of tasks across the NAVSEA, Naval Air Systems Command and Space and Naval Warfare Systems Command claimancies.

It is no wonder that Morrison and Long are proud to be associated with the CVN 21 program. Features of the modernized CVN 21 design include a highly automated propulsion system, electromagnetic aircraft launch and recovery systems, cruise ship automation and direct energy weapons. Each nuclear reactor will provide 25 percent more energy and three times the electrical output than the CVN 68-class carrier.

The air wing will be supported by an F-35C Joint Strike Fighter, F/A-18E/F Super Hornet, E-2C Hawkeye and EA-18G Prowler.

"We needed the best and brightest from the NSWG team and Al and Kevin certainly fit that description. They are truly dedicated, outstanding performers that have been extremely valuable team members of the CVN 21 Warfare System efforts for the CVN 21 program," Downey said.



Visit the CDSA Dam Neck Web site at <http://www.navseadn.navy.mil/>. CHIPS

Aircraft Carriers - CVN 21 Program

Starting with the lead ship, CVN 78, the new class features a multitude of improvements over existing aircraft carriers all designed to improve the combat capability of the Navy's carrier fleet while simultaneously reducing acquisition and life cycle costs.

CVN 78 warfighting capability improvements include: 25 percent increase in sortie generation rate; nearly three-fold increase in electrical generating capacity; and increased operational availability. CVN 78 quality of life improvements will result in improved work spaces, berthing and sanitary facilities; improved food service operations; increased air conditioning capacity; and increased training capabilities.

Even with all the improvements, the Navy expects to see CVN 78 cost reductions including more than \$300 million reduction in procurement costs; more than \$5 billion reduction in life cycle costs and 1,000-1,200 billet reductions in the ship's crew and air wing.

New technologies on board include:

- ✓ New propulsion plant design that includes a 50 percent reduction in the number of personnel required for plant operation and maintenance.
- ✓ Electromagnetic catapults and advanced arresting gear that support future air wing configurations including unmanned air vehicles.
- ✓ Improvements in weapons and material handling designed to more efficiently move ordnance and material around the ship in support of flight operations.
- ✓ New smaller island designed to accommodate Dual Band Radar developed by the DD(X) program.
- ✓ New Integrated Warfare System including flexible ship infrastructure design improvements to support future mission adaptability and flexibility.

Development, design and construction costs (\$5.6 billion) include the non-recurring investment in the design and development of the CVN 78-class. This is comprised of \$3.2 billion in RDT&E funds used to develop technologies to meet program requirements and \$2.4 billion of SCN funds used to develop the detail design for the class. The total cost to build the lead ship is \$8.1 billion in FY08 dollars.

Each ship in the new class will save \$5.3 billion in total ownership costs over its 50-year service life, compared to the CVN 68-class. Half of the total ownership cost for an aircraft carrier is allocated to the direct and indirect costs of manpower for operations and maintenance of the ship.

The CVN 78 is designed to operate effectively with 800 fewer crewmembers than a CVN 68-class ship. Technologies and ship design initiatives that replace maintenance intensive systems with low maintenance systems are expected to reduce watchstander and maintenance workload for the crew. The total ownership cost for a CVN 68-class ship is \$32.1 billion in FY04 constant year dollars; the total ownership cost for CVN 78 is expected to be \$26.8 billion.

General Characteristics CVN 21 Future Aircraft Carrier Program

Propulsion: Two nuclear reactors, four shafts; Length: 1092 feet; Beam: 134 feet; Flight Deck Width: 256 feet; Displacement: approximately 100,000 long tons full load; Speed: 30+ knots (34.5+ miles per hour); Crew: 4,660 (ship, air wing and staff); Armament: Evolved Sea Sparrow Missile, Rolling Airframe Missile, Close-In Weapons System (CIWS); Aircraft: 75+ (JSF, F/A-18E/F, EA-18G, E-2D, MH-60R/S, J-UCAS).

- Fact Sheet from NavyNewsStand

DON CIO Draws Diverse Audience at IM and IT Conference

An enthusiastic team from the Department of the Navy Chief Information Officer (DON CIO) led a variety of learning tracks and sessions regarding information technology issues affecting the Department at the DON Information Management and Information Technology (IM and IT) Conference in Hampton, Va.

Due to its proximity to the Norfolk fleet concentration area, the DON CIO hosted this conference at the same time and location as Transformation TechNet, sponsored by the Armed Forces Communications and Electronics Association (AFCEA).

The DON CIO-led sessions, which began May 8 and concluded May 10, drew attendees primarily from the DON, but also across the Defense, government and contractor communities. Session topics included: the DON IM/IT Workforce, Enterprise Software, Software Asset Management, System Integration Services, Enterprise Architecture, Data Management, Information Assurance, IT Performance Measurement, Knowledge Management, Wireless, Identity Management and the DON IT Umbrella Program of contracts.

The sessions provided an opportunity to share information about the latest DON IM and IT initiatives, policy, and guidance and form partnerships to further the work of the Department. The DON CIO team was joined by subject matter experts from the Naval Network Warfare Command, Naval Postgraduate School, Naval Supply Systems Command, Marine Corps Development Command, U.S. Joint Forces Command, Naval Air Systems Command, Office of Civilian Human Resources and Defense Information Systems Agency.

The series of Data Management tracks was particularly intense. The DON CIO team leader for data management, Bob Green, and Tom Brown, functional namespace coordinator for test and evaluation, facilitated a series of sessions centered on the DON's net-centric data strategy that ensures data are visible, available, understandable, trusted, interoperable and responsive to users' needs.

The DON Service-Oriented Architecture (SOA) Transformation Group presented the DON direction for a net-centric, interoperable environment, based on a SOA that ensures Web services are visible, trusted, accessible and usable to accelerate the decision-cycle process throughout the DON warfighter community via Web-centric technology.

The DON CIO enterprise licensing team leader and co-chair and DON representative for the Department of Defense Enterprise Software Initiative (ESI), Floyd Groce, led a series of tracks that discussed Defense Department acquisition models for savings on commercial software and the implementation of a software enterprise management process within the DoD. The ESI leverages the buying power of the DoD to negotiate enterprise agreements for best price products and services.

Linda Greenwade, program manager of the DON IT Umbrella Program, provided an overview of the acquisition strategy guiding the Umbrella program. Greenwade was joined by a panel of acquisition experts including Robert Smith from the Office of the Assistant Sec-

retary of Defense Networks and Information Integration, Michael Hargrove from the General Services Administration SmartBUY program, and Sylvia Johnson from the Naval Inventory Control Point.

The DON CIO knowledge management team leader, Jim Knox, explained the DON strategy to achieve knowledge dominance by creating a knowledge culture and processes to operationalize the sharing of essential information. Other tenets of KM include implementation of a comprehensive standards-based content management strategy and single authoritative data sources across the Department, and effective records management with continuation of the Department-wide implementation of electronic records management.

Knox reminded DON employees that DON membership in the American Productivity and Quality Center allows Department personnel to access the APQC's Web site (<http://www.apqc.org>) for KM information. The APQC is a research organization specializing in KM metrics, measurement, process improvement, best practices and benchmarking; it also offers access to the Knowledge Sharing Network.

Members of the DON IM/IT workforce had an opportunity to meet with their community manager, Sandra Smith, in a series of sessions. Under discussion were DON IM and IT workforce items and implementation of the National Security Personnel System within the DON.

Three short days just wasn't enough time to present the wealth of information that the DON CIO team had to offer. When you bring together people who are passionate about their work with people eager to learn, it's difficult to contain the flow of enthusiasm and discussion. But why would you want to?

The conference presentations are available on the DON CIO Web site at <http://www.doncio.navy.mil/>.

The next IM and IT Conference is scheduled for Jan. 30 to Feb. 2, 2007, in San Diego. Check the DON CIO Web site in the upcoming months for more information.

CHIPS



The acquisition panel left to right, Robert Smith from the Office of the Assistant Secretary of Defense Networks and Information Integration, Linda Greenwade, DON IT Umbrella program manager, Sylvia Johnson from the Naval Inventory Control Point and Michael Hargrove from the General Services Administration SmartBUY program.

Information Warriors Train Aboard USS Tarawa

By Photographers Mate 3rd Class Tony Spiker

Aboard USS TARAWA in port in San Diego, Calif., Information Professional (IP) Officers, in charge of Navy communications and computer systems at shore facilities and on board ships, normally depend on PowerPoint presentations to facilitate training under Job Qualification Requirements and Personnel Qualification Standards (JQR PQS).

While the information is thoroughly covered, actually being aboard a combat C4I (command, control, communications, computers and intelligence) platform with hands-on training beats classroom work any day.

The amphibious assault ship USS Tarawa (LHA 1) recently opened its doors to officers completing their qualifications training for them to experience firsthand what their futures as IP warriors will entail. This is the first time tours such as these have been organized for IP officers.

Tarawa's Combat Officer, Cmdr. Alan Kolackovsky made his department available, allowing the IP officers access to equipment they will eventually be working with in the fleet. Here, they gained valuable firsthand knowledge of the job that awaits them once they complete their JQR PQS and certification boards.

"There is a big difference from reading about something on a computer screen and actually working with it and making a visual connection to the device," said Lt. Oscar Simmons, visiting IP officer. "Actually seeing what happens on a ship this size, puts me a step ahead of where I would be without this training."

Many of the officers on the tour had been stationed at shore facilities at clear-cut jobs.

"On shore you deal with fixed communications systems like phone lines and satellite systems. But at sea, aboard a moving platform, things become much more complicated very quickly," said Information Systems Technician Second Class John Shawbell, the tour coordinator.



IT2 John Shawbell explains shipboard communications systems to Capt. Scot Miller, Director, Assessment and Experimentation, Space and Naval Warfare Systems Command, and other Information Professional Officers, aboard USS Tarawa (LHA 1) April 26th. U.S. Navy Photo by Photographers Mate Third Class Tony Spiker.

Many of the IP officers were lateral transfers from other communities such as pilots whose aircraft have been discontinued from service.

Cmdr. Patrick Owens, former S-3 Viking flight officer, said he wanted to stay in the Navy. Since his aircraft are being phased out for Navy use, he switched to the IPO community since there is an emphasis on technology and communications. "This training visit and being able to work with the nuts and bolts of the job will really help me succeed at my next command," Owens said.

Because of their visit these IP officers have a much stronger knowledge base which will definitely help both them and their community as a whole.

Capt. Scot Miller, an IPO and director of Assessment and Experimentation at Space and Naval Warfare Systems Command said, "Getting the IPO community out to sea will help the community as a whole succeed. Tours like this one keep our officers operationally aware, which

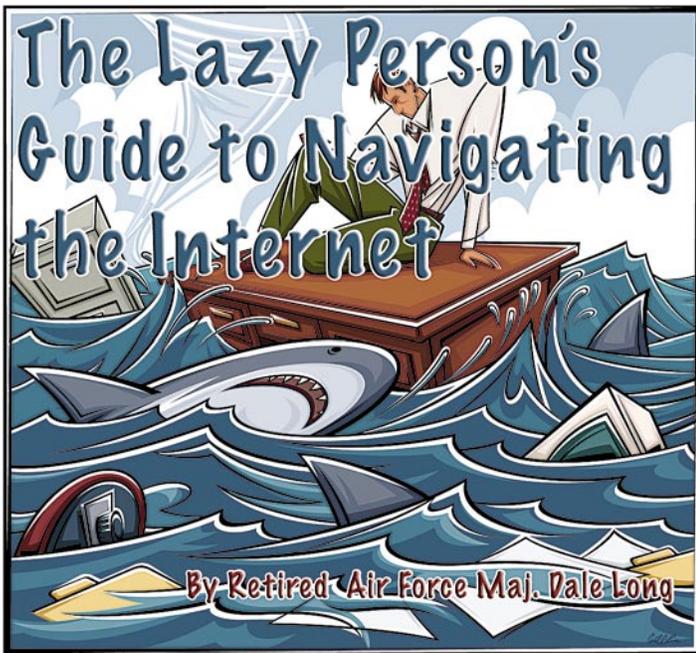


IT2 Izaak Cook and Capt. Scot Miller aboard USS Tarawa. U.S. Navy Photo by Photographers Mate Third Class Tony Spiker.

will help them advance in their careers."

The true measure of success and benefit gained by these programs will not become evident until these IP officers pass their boards and transfer their professional knowledge and C4I skills to the fleet.

For more information contact the public affairs office by e-mail at PAO@Tarawa.navy.mil. CHIPS



"No mercy, no power but its own controls it. Panting and snorting like a mad battle steed that has lost its rider; the masterless ocean overruns the globe."

– Herman Melville, from the novel "Moby Dick"

With more than 81 million host names in use as of May 2006, the Internet now resembles the vast ocean described by Herman Melville in 1851. In Melville's time, travel across an ocean was still an adventure. Now, through the near-magical quality of modern information technology, we have almost instantaneous, worldwide access to a vast ocean of information.

However, given the relative newness of this vast new cyber-ocean, many Internet surfers may find themselves far from shore without a compass. While all we have to do to return home is close our browser, it is still a bit disconcerting to find ourselves lost, adrift or even hijacked while doing something online.

So, in the interest of making the waters of the Internet less foggy and more navigable, in this issue we will look at how the Internet is organized, some of the navigation aids and other information sources available on the Net, and how to tell whether or not you can trust the site you are about to load.

Who's in Charge?

The Internet, along with the deepest ocean trenches and the outer reaches of the solar system, is one of the great modern frontiers for human exploration. As the Advanced Research Projects Agency Network (ARPANET) from 1969 until 1998, it was governed in various ways by the U.S. Department of Defense or associated contractors under the auspices of the Internet Assigned Numbers Authority (IANA) and other entities.

In 1998, perhaps in recognition of the Internet's transformation to a commercial entity, management of the Internet moved to a non-profit corporation sponsored by the Department of Commerce, the Internet Corp. for Assigned Names and Numbers.

ICANN is an internationally organized, non-profit corporation based in Marina del Rey, Calif. It is responsible for, among other things: managing Internet Protocol (IP) address space allocation; managing generic (gTLD) and country code (ccTLD) Top-Level Domain names; root server system management functions; preserving the operational stability of the Internet; and developing Internet management policy.

The most visible function of ICANN is its management of the Domain Name System (DNS). Every computer on the Internet has a unique IP address, a 32-bit number made up of four 8-bit "octets" that define every site on the Internet. For example, the IP address of the ICANN.org Web site is 192.0.34.163.

However, as most people have a hard time remembering arcane strings of digits, the DNS allows Web sites to use text as an alias for a numeric IP address, allowing us to type "www.icann.org" instead of the numeric IP address.

The principal value of the DNS is ensuring universal resolvability of Internet site addresses. This ensures that every Internet user, can access content from any site on the Internet. While there may be some governments that may not be entirely happy that their citizens can access allegedly unhealthy content via the Internet, ICANN and the Internet community have thus far successfully resisted having the Internet split up into segregated enclaves controlled by national or regional interests. The Internet remains an international resource, though with varying levels of monitoring, privacy and censorship depending on where you are.

What's in a Name?

Internet addresses are divided into groups of sites defined by domain names. "gTLD" is intended for use, at least in theory, by a particular class of organization. gTLDs were originally named for the types of organizations they represent, though some have become less restrictive over time. Let's start by looking at six gTLDs we are all probably familiar with.

.com – This domain is intended for commercial organizations, but anyone can apply for a dot-com address. There are more dot-com sites on the Internet than any other domain. The quality and reliability of these sites can vary widely, ranging from reputable sites associated with established companies to sites serving as fronts for phishing operators and online swindlers.

.edu – This domain is reserved for educational institutions. However, use of an dot-edu domain does not necessarily guarantee that the site belongs to an institution accredited by the U.S. Department of Education or equivalent foreign government agency.

.net – This domain was originally used to designate network infrastructures, but is now unrestricted. Commercial e-mail providers often use dot-net for their users' e-mail accounts (*e.g., Verizon.net, Adelphia.net, etc.*) possibly in an attempt to give the account more "net credibility" than a dot-com account.

.org – This domain was originally intended mainly for non-profit organizations that did not fit cleanly within the other gTLDs. However, like dot-net, the dot-org domain is now unrestricted.

.gov – This is a restricted domain reserved for the exclusive use of U.S. government agencies. **.mil** is similarly restricted for the exclusive use of U.S. military services and the Defense Department.

In addition to those six, the next set of sites you are likely to see are those assigned by country (ccTLDs), like ".ca" (Canada), ".ru" (Russia) or ".au" (Australia). Aside from these gTLDs and the ccTLDs, here are some lesser-known gTLDs:

.aero	for the air transport industry
.biz	for business use
.cat	for Catalan language/culture
.coop	for cooperatives
.eu	for the European community
.info	for informational sites, but unrestricted
.int	for international organizations established by treaty
.jobs	for employment-related sites
.mobi	for sites catering to mobile devices
.museum	for museums
.name	for families and individuals
.pro	for certain professions
.travel	for travel agents, airlines, hoteliers, tourism bureaus, etc.

The Internet is a big place, in a virtual sense. Netcraft.com, an Internet monitoring site, received responses from 81,565,877 sites in its May survey. According to Netcraft, the Internet grew by 909,000 sites from April to May and by 7.2 million hostnames from the beginning of the year through May. If you are keeping track that means the Internet gets a new hostname about every 3 seconds. Netcraft estimates the Internet will grow by 17 million hostnames this year.

Hostnames do not equal servers or pages. A site may have many servers and any number of pages. How many pages, you may ask? A site called the "WayBack Machine" (<http://www.archive.org/web/web.php>) has archived over 55 billion Web pages produced since 1996. To view them all you would have to view one page every second for the next 42,000 years. This begs the following question: How do we find anything in an ocean of information that mind-numbingly big?

Navigation Aids

Two types of sites help us navigate the Internet: portals and search engines. Portals are sites that collect and organize information and other functionality in your browser window based on preset conditions. The organization you work for probably has a portal of some type. Your Internet service provider (ISP) probably has a portal, and there are commercial Web sites like Yahoo.com, MSN.com and Google.com that anyone can use as a window to the Internet.

What distinguishes portals from other Internet sites is the amount of control you can exercise over what appears in your browser. My experience has been that commercial portals offer users a greater

degree of customization than portals developed by companies or government agencies for their employees. I submit, however, that the popularity of a portal has a direct relationship to how much control users have over the content.

Humans like control. If I control my portal space, I am not going to clutter it with advertisements or press releases. I'm going to include stuff I am actually interested in and use. I will accept some content from the portal owner, but if I cannot control the majority of my home page space, I will go elsewhere.

The commercial portal that is currently my home page on every computer I use allows me to create multiple pages with news feeds, links to government, financial and technology sites, Web comics, and search sites. It is a window that satisfies my personal and professional needs. The trade-off is that the portal manager can show ads in the top banner and in a side column.

Search Me

Portals organize things based on preset conditions. When we need to find something new, we use a search engine. The first generation of Internet search tools started with "Archie," (*the word "Archive" without the letter "v"*) created in 1990 by Alan Emtage, a student at McGill University in Montreal. However, Archie did not search through file content. It just downloaded the directory listings of all the files located on public anonymous File Transfer Protocol (FTP) sites and created a searchable database of filenames.

In 1991, students at the University of Minnesota developed "Gopher" (*named after the school's mascot*) which indexes plain text documents. Gopher is a distributed document search and retrieval network protocol designed for the Internet. Its purpose was similar to that of the World Wide Web. The Web has almost completely displaced Gopher. However, there are still a few active Gopher sites in existence, including one at the Smithsonian Institution.

Two other programs, apparently developed by people who missed the memo that Archie wasn't named after a comic strip character, were "Veronica" and "Jughead," which searched the files stored in Gopher index systems. Veronica (*Very Easy Rodent-Oriented Net-wide Index to Computerized Archives*) provided a keyword search of Gopher menu titles. Jughead (*Jonzy's Universal Gopher Hierarchy Excavation and Display*) obtained menu information from Gopher servers.

Then the World Wide Web tsunami swept over the Internet, changing it forever. The proof of concept for Web searching debuted in 1993 with Aliweb (*Archie Like Indexing for the Web*). The first well-known full-text search engine on the Web was WebCrawler in 1994, soon joined by Infoseek and Lycos.

AltaVista and Excite appeared in 1995, with Dogpile, Inktomi and Ask.com rounding out the second generation of Internet search engines in 1996.

These full-text search engines held their own for a while, but eventually fell victim to three things: the Web started getting

too big for their technology; the dot-com bubble burst; and someone built a better search mousetrap.

In 1998, the beta version of Google appeared on the Web. While Google also uses text indexing, it pioneered two features that gave it an edge over other browsers: link popularity and PageRank. Link popularity measures the quantity and quality of Web sites that link to pages with content that meets your search criteria. While text indexing can measure how a page meets search criteria quantitatively, link popularity is a qualitative measure of “off-the-page” criteria.

The theory is if a page is important or useful, other sites will have links to it, and pages with little or no value will have fewer citations. Link popularity analyzes how many other sites link to the target page and cross-references that with the linking site’s reputation. It is the Web equivalent of “word-of-mouth” referrals.

PageRank is the heart of Google. According to Google, *“PageRank relies on the uniquely democratic nature of the Web by using its vast link structure as an indicator of an individual page’s value. In essence, Google interprets a link from page A to page B as a vote, by page A, for page B. But, Google looks at more than the sheer volume of votes or links a page receives. It also analyzes the page that casts the vote. Votes cast by pages that are themselves ‘important’ weigh more heavily and help to make other pages ‘important.’”*

The combination of these two features allowed Google to generate more accurate search results than any other search engine on the Web at the time. Other search engines have attempted to copy its methods, but Google still has approximately 80 percent of the search engine market through user trust in their results.

However, even Google does not claim to index the entire World Wide Web — just around 20 billion pages. That leaves room for specialized search sites based on a concept known as vertical search. Google is a horizontal search engine; it attempts to index across as much of the Web as possible. Vertical search engines specialize in content areas, like travel, real estate or retail sales, and only include sites that match their special interest criteria.

As the Web grows larger, it is likely it will grow beyond the capability of any single horizontal search engine to keep up. What we may have in another 10 years are vertical search engines that work in particular content areas or domains and meta-search engines that send our queries out to multiple vertical and horizontal search engines and aggregate the results. For example, WebCrawler is now a meta-search engine.

Trust, but Verify

This brings us to a few closing thoughts on the value, authenticity, and reliability of what is displayed in our portals or search engines. How can you tell if a Web site is both legitimate and useful?

The first indicator is the domain name. If you are visiting a dot-gov or dot-mil site, it is a pretty safe bet that the content is legitimate. With any other domain, however, you take your chances. I am more inclined to trust dot-edu, dot-org or dot-net domains than dot-com or dot-ru, though I do look for independent verification.

Here’s a quick quiz. Which of the following links are what they appear to be?

1. <http://travelocity.com/>
2. <http://paypal-email.com/login.htm/>
3. <http://www2.usairways.com/>
4. <http://www.ebay.com@64.236.24.12>
5. <http://www.email.citicards.com/>

Now check your answers. How did you do?

No. 1 is a legitimate link to Travelocity.

No. 2 was once used as a phishing link to a fake PayPal site that would capture your account login and give the phishers access to your account. It is no longer active.

No. 3 is a legitimate US Airways link.

No. 4 is a phisher-style address that attempts to redirect you to a different site. In this example, the numeric IP address after the @ will attempt to redirect you to a site that doesn’t require authentication, for example, CNN.com. If the destination site is a phishing site built to require authentication and accept “www.ebay.com” as valid data, you would get no warning about the redirect, and you could be looking at something that looks like eBay — but isn’t. This site is now blocked on many networks.

No. 5 is a trick question. Yes, this is a legitimate CitiBank site address. But clicking on this link in a recent CitiBank e-mail actually took you to a different address. Disguising links with a different address label is a common phishing trick, both in e-mail and on Web sites. Most programs with the ability to activate Web links will at least briefly display the actual link address when your mouse cursor pauses over a link.

I highly recommend making sure where any link is actually going. Finally, you should report rogue links to your ISP for everyone’s protection.

Aside from phishing and other technical tomfoolery, there is another trust issue: *Is the content on any given Web site useful or truthful?* Unfortunately, there is no way to check this with technology. As with any source of information, like newspapers, television news or talk radio, we still have to use good judgment on the content.

Use this old adage as a good rule of thumb: *“Believe half of what you see and none of what you hear.”* Of course, we still have to decide which half, but at least we have a 50 percent chance.

Until next time, Happy Networking!

Long is a retired Air Force communications officer who has written regularly for CHIPS since 1993. He holds a Master of Science degree in Information Resource Management from the Air Force Institute of Technology. He is currently serving as a telecommunications manager in the U.S. Department of Homeland Security. CHIPS

Enterprise Software Agreements Listed Below



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

Additionally, the ESI was incorporated into the Defense Federal Acquisition Regulation Supplement (DFARS) Section 208.74 on Oct. 25, 2002, and DoD Instruction 500.2 in May 2003.

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

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

Software Categories for ESI:

Business and Modeling Tools

BPWin/ERWin

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

Contractor: *Computer Associates International, Inc.* (DAAB15-01-A-0001)

Ordering Expires: Upon depletion of Army Small Computer Program (ASCP) inventory

Web Link: <https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp>

Business Intelligence

Business Objects

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

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

Ordering Expires: 04 May 10

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

Mercury - NEW!

Mercury Software - Provides software licenses, training, technical support and maintenance for Mercury Performance Center, Mercury Quality Center, Mercury IT Governance Center and Mercury Availability Center.

Contractor: *Spectrum Systems, Inc.* (SP4700-05-A-0002)

Ordering Expires: 21 Feb 09

Web Link: <http://www.spectrum-systems.com/contracts-ESI.htm>

Collaborative Tools

Invoke Software (CESM-E)

Invoke Software - A collaboration integration platform that provides global awareness and secure instant messaging, integration and interoperability between disparate collaboration applications in support of the DoD's Enterprise Collaboration Initiatives.

Contractor: *Structure Wise* (DABL01-03-A-1007)

Ordering Expires: 17 Dec 06

Web Link: <https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp>

Database Management Tools

IBM Informix (DEAL-I/D)

IBM Informix - Provides IBM/Informix database software licenses and maintenance support at prices discounted 2 to 27 percent off GSA Schedule prices. The products included in the enterprise portion are: IBM Informix Dynamic Server Enterprise Edition (version 9); IBM Informix SQL Development; IBM Informix SQL Runtime; IBM Informix ES/SQL/C Development; IBM Informix ES/SQL/C Runtime; IBM Informix 4GL Interactive Debugger Development; IBM Informix 4GL Compiler Development; IBM Informix 4GL Compiler Runtime; IBM Informix 4GL RDS Development; IBM Informix 4GL RDS Runtime; IBM Informix Client SDK; IBM Informix Dynamic Server Enterprise Edition (version 7 and 9); and IBM Informix D.M. Gold Transaction Processing Bundle.

Contractor: *IBM Global Services* (DABL01-03-A-0002)

Ordering Expires: 30 Sep 06

Web Link: <https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp>

Microsoft Products

Microsoft Database Products - See information under Office Systems on page 57.

Oracle (DEAL-O)

Oracle Products - Provides Oracle database and application software licenses, support, training and consulting services. The Navy Enterprise License Agreement is for database licenses for Navy customers.

www.it-umbrella.navy.mil

Contractors:

Oracle Corp. (DAAB15-99-A-1002)

DLT Solutions – authorized reseller

Mythics, Inc. – authorized reseller

Ordering Expires: 31 Oct 06

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://ascp.monmouth.army.mil/scp/contracts/compactview.jsp>

Special Note to Navy Users: On Oct. 1, 2004, and May 6, 2005, the Navy established the Oracle Database Enterprise License, effective through Sept. 30, 2013. The enterprise license provides Navy shore-based and afloat users to include active duty, Reserve and civilian billets, as well as contractors who access Navy systems, the right to use Oracle databases for the purpose of supporting Navy internal operations. Navy users in joint commands or supporting joint functions should contact Bill Huber, NAVICP Mechanicsburg contracting officer at (717) 605-3210 or e-mail William.Huber@navy.mil, for further review of the requirements and coverage.

This license is managed by the Space and Naval Warfare Systems Center (SPAWAR-SYSCEN) San Diego DON Information Technology (IT) Umbrella Program Office.

The Navy Oracle Database Enterprise License provides significant benefits including substantial cost avoidance for the Department. It facilitates the goal of net-centric operations by allowing authorized users to access Oracle databases for Navy internal operations and permits sharing of authoritative data across the Navy enterprise.

Programs and activities covered by this license agreement shall not enter into separate Oracle database licenses outside this central agreement whenever Oracle is selected as the database. This prohibition includes software and software maintenance that is acquired:

- as part of a system or system upgrade, including Application Specific Full Use (ASFU) licenses;
- under a service contract;
- under a contract or agreement administered by another agency, such as an interagency agreement;
- under a Federal Supply Service (FSS) Schedule contract or blanket purchase agreement established in accordance with FAR 8.404(b)(4); or
- by a contractor that is authorized to order from a Government supply source pursuant to FAR 51.101.

This policy has been coordinated with the Office of the Assistant Secretary of the Navy (Financial Management and Comptroller), Office of Budget.

Web Link: <http://www.it-umbrella.navy.mil/contract/enterprise/deal/Oracle/oracle.shtml>

Sybase (DEAL-S)

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

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

Ordering Expires: 15 Jan 08

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://ascp.monmouth.army.mil/scp/contracts/compactview.jsp>

Enterprise Architecture Tools

Rational Software (AVMS-R)

Rational Software - Provides IBM Rational software licenses and maintenance support for suites and point products including: IBM Rational RequisitePro; IBM Rational Rose; IBM Rational ClearCase; IBM Rational ClearQuest; and IBM Rational Unified Process.

Contractor: **immixTechnology**, (DABL01-03-A-1006); (800) 433-5444

Ordering Expires: 26 Mar 09

Web Link: <https://ascp.monmouth.army.mil/scp/contracts/compactview.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); (800) 645-3042

Ordering Expires: Effective for term of the GSA FSS Schedule

Web Link: <https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp>

Citrix

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

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

Ordering Expires: 23 Feb 08

Web Link: <https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp>

Microsoft Premier Support Services (MPS-1)

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** (DAAB15-02-D-1002); (980) 776-8283

Ordering Expires: 30 Jun 07

Web Link: <https://ascp.monmouth.army.mil/scp/contracts/compactview.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 10 to 8 percent off GSA Schedule pricing for products and 5 percent off GSA Schedule pricing for maintenance.

Contractors:

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

Northrop Grumman - authorized reseller

Federal Technology Solutions, Inc. - authorized reseller

Ordering Expires: 5 May 09

Web Link: <https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp>

ProSight

ProSight - Provides software licenses, maintenance, training and installation services for enterprise portfolio management software. The BPA award has been determined to be the best value to the government and; therefore, competition is not required for software purchases. Discount range for software is from 8 to 39 percent off GSA pricing, which is inclusive of software accumulation discounts. For maintenance, training and installation services, discount range is 3 to 10 percent off GSA pricing. Credit card orders are accepted.

Contractor: **ProSight, Inc.** (W91QUZ-05-A-0014); (503) 889-4813

Ordering Expires: 19 Sep 06

Web Link: <https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp>

Quest Products

Quest Products - Provides a full range of Quest Software Enterprise Management products and services including training. Product groups include Application Management and Database Management (*code quality and optimization, performance and ability, and change and configuration*) and Windows Management (Active Directory, Exchange and Windows).

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

Ordering Expires: 14 Aug 10

Web Link: <https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-05-A-0023>

Telelogic Products

Telelogic Products - Offers development tools and solutions which assist the user in automation in the development life cycle. The major products include DOORS, SYNERGY and TAU Generation. Licenses, maintenance, training and services are available.

Contractors:

Bay State Computers, Inc. (N00104-04-A-ZF13); Small Business Disadvantaged; (301) 352-7878, ext. 116

Spectrum Systems, Inc. (N00104-06-A-ZF31); Small Business ; (703) 591-7400

Ordering Expires: 29 Jun 07

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

Enterprise Resource Planning

Digital Systems Group

Digital Systems Group - Provides Integrated Financial Management Information System (IFMIS) software that was designed specifically as federal financial management system software for government agencies and activities. The BPA also provides installation, maintenance, training and professional services.

Contractor: **Digital Systems Group, Inc.** (N00104-04-A-ZF19); (215) 443-5178

Ordering Expires: 23 Aug 07

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

Oracle

Oracle - See information provided under Database Management Tools on page 53.

RWD Technologies - NEW!

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) 869-1085

Ordering Expires: Effective for term of the GSA FSS Schedule

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

SAP

SAP Software - Provides software license, installation, implementation technical support, maintenance and training services.

Contractor: **SAP Public Sector & Education, Inc.** (N00104-02-A-ZE77); (202) 312-3656

Ordering Expires: Effective for term of the GSA FSS Schedule

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

ERP Systems Integration Services

ERP Systems

ERP Systems Integration Services - Provides the procurement of configuration; integration; installation; data conversion; training; testing; object development; interface development; business process reengineering; project management; risk management; quality assurance; and other professional services for COTS software implementations. Ordering under the BPAs is decentralized and is open to all DoD activities. The BPAs offer GSA discounts from 10 to 20 percent. Firm fixed prices and performance-based contracting approaches are provided to facilitate more efficient buying of systems integration services. Five BPAs were competitively established against the GSA Schedule. Task orders must be competed among the five BPA holders in accordance with DFARS 208.404-70 and Section C.1.1 of the BPA. Acquisition strategies at the task order level should consider that Section 803 of the National Defense Authorization Act for 2002 requirements were satisfied by the BPA competition.

Contractors:

Accenture LLP (N00104-04-A-ZF12); (703) 947-2059

BearingPoint (N00104-04-A-ZF15); (703) 747-5442

Computer Sciences Corp. (N00104-04-A-ZF16); (856) 252-5583

Deloitte Consulting LLP (N00104-04-A-ZF17); (202) 220-2960

IBM Corp. (N00104-04-A-ZF18); (301) 803-6625

Ordering Expires: 03 May 09

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/erp_services/erp-esi.shtml

Information Assurance Tools

Network Associates, Inc.

Network Associates, Inc. (NAI) - This protection encompasses the following NAI products: VirusScan; Virex for Macintosh; VirusScan Thin Client; NetShield; NetShield for NetApp; ePolicy Orchestrator; VirusScan for Wireless; GroupShield; WebShield (software only for Solaris and SMTP for NT); and McAfee Desktop Firewall for home use only.

Contractor: *Network Associates, Inc.* (DCA100-02-C-4046)

Ordering Expires: Nonexpiring. Download provided at no cost; go to the Antivirus Web links below for antivirus software downloads.

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

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

NIPRNET site: http://www.cert.mil/antivirus/av_info.htm

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

Securify

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

Contractor: *Patriot Technologies, Inc.*

Ordering Expires: 4 Jan 11 (if extended by option exercise)

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

Symantec

Symantec - Provides the full line of Symantec Corp. products and services consisting of over 6,000 line items including Ghost and Brightmail. Symantec products can be divided into eight 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. **Notice to DoD customers regarding Symantec Antivirus Products:** A DoD Enterprise License exists for select Antivirus products through DISA contract DCA100-02-C-4049 found below.

Contractor: *immix Technology*

Ordering Expires: 12 Sep 10

Web Link: <http://www.immixtechnology.com/esi/Symantec/> or <http://www.esi.mil>

Symantec Antivirus

Symantec - This protection encompasses the following Symantec products: 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 (AV only); and support.

Contractor: *Northrop Grumman Information Technology* (DCA100-02-C-4049)

Ordering Expires: Nonexpiring. Download provided at no cost; go to the Antivirus Web links below for antivirus software downloads.

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

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

NIPRNET site: http://www.cert.mil/antivirus/av_info.htm

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

Trend Micro

Trend Micro - This protection encompasses the following Trend Micro products: InterScan Virus Wall (NT/2000, Solaris, Linux); ScanMail for Exchange (NT, Exchange 2000); TMCM/TVCS (Management Console - TMCM W/OPP srv.); PC-Cillin for Wireless; and Gold Premium support contract/year (PSP), which includes six POCs.

Contractor: *Government Technology Solutions* (DCA100-02-C-4045)

Ordering Expires: Nonexpiring. Download provided at no cost; go to the Antivirus Web links below for antivirus software downloads.

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

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

NIPRNET site: http://www.cert.mil/antivirus/av_info.htm

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

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.* (F01620-03-A-8003); (703) 724-4555

Ordering Expires: 31 Jul 08

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

Office Systems

Adobe

Adobe Products - Provides software licenses (new and upgrade) and upgrade plans (formerly known as maintenance) for numerous Adobe and formerly branded Macromedia products, including Acrobat (Standard and Professional); Photoshop; Encore; After Effects; Frame Maker; Creative Suites; Illustrator; Flash Professional; Dreamweaver; Cold Fusion and other Adobe products.

Contractors:

ASAP (N00104-06-A-ZF33); Small Business; (800) 248-2727, ext. 5303

CDW-G (N00104-06-A-ZF34); (703) 621-8211

Softchoice (N00104-06-A-ZF35); Small Business; (703) 480-1957

Softmart (N00104-06-A-ZF36); Small Business; (610) 518-4192

Ordering Expires: 31 May 08

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

Four new Blanket Purchase Agreements (BPAs) provide both new and upgrade software licenses for Adobe products. These agreements also provide Adobe software upgrade plans, formerly known as maintenance agreements. The BPAs include software licenses formerly known under the Macromedia product brand. Products in-

clude: Acrobat (Standard and Professional); Photoshop; Encore; After Effects; Frame Maker; Creative Suites; Illustrator; Flash Professional; Dreamweaver; Cold Fusion; and other Adobe products.

The awardees are CDW-G, Softmart, ASAP and Softchoice.

A change in Adobe licensing will affect a user's ability to purchase upgrade plan coverage for legacy products. Without purchasing upgrade plan coverage, customers will not be eligible for free version upgrades.

From May 1 through Nov. 1, 2006, all Defense Department customers that own Adobe and Macromedia legacy software licenses will be able to purchase a new upgrade plan — if the customer's software licenses are at current shipping versions. The first six months of the new Adobe agreement will be the only opportunity to cover (maintain) legacy Adobe products even if customers currently have maintenance plans.

Customers that do not take advantage of this limited time offer will have to purchase an upgrade license (if available) or repurchase a new license for the Adobe product to obtain the latest Adobe versions.

After the first six-month period, upgrade plans can only be purchased for new and upgrade licenses — and only at the time of a new license purchase.

Products may be purchased through the ITEC Direct storefront (<http://www.itec-direct.navy.mil>). Customers can make direct purchases using the government credit card; contact software product managers and obtain customer service; browse our product line; review policy notices; and access small business contracts.

We will also be posting any new information and/or guidance to our DoD ESI Web site at www.esi.mil. We appreciate your patience during this transition period and will be happy to provide any assistance you may need.

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:

ASAP (N00104-02-A-ZE78); Small Business; (800) 248-2727, ext. 5303

CDW-G (N00104-02-A-ZE85); (847) 968-9429

Dell (N00104-02-A-ZE83); (800) 727-1100 ext. 37010 or (512) 723-7010

GTSI (N00104-02-A-ZE79); Small Business; (800) 999-GTSI or (703) 885-4554

Hewlett-Packard (N00104-02-A-ZE80); (800) 535-2563 pin 6246

Softchoice (N00104-02-A-ZE81); Small Business; (877) 333-7638 or (312) 655-9167

Softmart (N00104-02-A-ZE84); (610) 518-4000, ext. 6492 or (800) 628-9091 ext. 6928

Software House International (N00104-02-A-ZE86); (732) 868-5926

Software Spectrum, Inc. (N00104-02-A-ZE82); (800) 862-8758 or (509) 742-2208

Ordering Expires: 30 Mar 07

Web Link: <http://www.it-umbrella.navy.mil/contract/enterprise/microsoft/ms-ela.shtml>

Red Hat

Red Hat (Netscape software formerly owned by AOL, not Linux)

- In December 2004, America Online (AOL) sold Netscape Security Solutions software to Red Hat. This sale included the three major software products previously provided by DISA (Defense Information Systems Agency) to the DoD and Intelligence Communities through AOL. *Note: The Netscape trademark is still owned by AOL, as are versions of Netscape Communicator above version 7.2. Netscape Communicator version 8.0 is not part of this contract.*

August Schell Enterprises is providing ongoing support and maintenance for the Red Hat Security Solutions (products formerly known as Netscape Security Solutions) which are at the core of the DoD's Public Key Infrastructure (PKI). This contract provides products and services in support of the ongoing DoD-wide enterprise site license for Red Hat products. This encompasses all components of the U.S. Department of Defense and supported organizations that use the Joint

Worldwide Intelligence Communications System (JWICS), including contractors.

Licensed software products available from DISA are the commercial versions of the software, not the segmented versions 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 licensed product available for download from the DoD Download Site to support development or operation of an application associated with the GIG, GCCS or GCSS, you must contact one of the Web sites listed below to obtain the GIG segmented version of the software. You may not use the commercial version available from the DoD Download Site.

If you are not sure which version (commercial or segmented) to use, we strongly encourage you to refer to the Web sites listed below for additional information to help you to make this determination before you obtain the software from the DoD Download Site.

GIG or GCCS users: Common Operating Environment Home Page

<https://coe.mont.disa.mil>

GCSS users: Global Combat Support System

<http://www.disa.mil/main/prodsol/gcss.html>

Contractor: *Red Hat*

Ordering Expires: 06 Mar 07

Download provided at no cost.

Web Link: <http://iase.disa.mil/netlic.html>

WinZip

WinZip - This is an IDIQ contract with Eyak Technology, LLC, an "8(a)" Small Disadvantaged Business (SDB)/Alaska Native Corp. for the purchase of WinZip 9.0, a compression utility for Windows. Minimum quantity order via delivery order and via Government Purchase Card to Eyak Technology, LLC is 1,250 WinZip licenses. All customers are entitled to free upgrades and maintenance for a period of two years from original purchase. Discount is 98.4 percent off retail. Price per license is 45 cents.

Contractor: *Eyak Technology, LLC* (W91QUZ-04-D-0010)

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

Ordering Expires: 27 Sep 09

Web Link: <https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp>

Operating Systems

Novell

Novell Products - Provides master license agreement for all Novell products, including NetWare, GroupWise and ZenWorks.

Contractor: *ASAP Software* (N00039-98-A-9002); Small business; (800) 883-7413

Ordering Expires: 31 Mar 07

Web Link:

<http://www.it-umbrella.navy.mil/contract/enterprise/novell/novell.shtml>

Sun (SSTEWS)

SUN Support - Sun Support Total Enterprise Warranty (SSTEWS) offers extended warranty, maintenance, education and professional services for all Sun Microsystems products. The maintenance covered in this contract includes flexible and comprehensive hardware and software support ranging from basic to mission critical services. Maintenance covered includes Sun Spectrum Platinum, Gold, Silver, Bronze, hardware only and software only support programs.

Contractor: *Dynamic Systems* (DCA200-02-A-5011)

Ordering Expires: Dependent on GSA Schedule until 2011

Web Link: <http://www.ditco.disa.mil/hq/contracts/sstewchar.asp>

Research and Advisory BPAs Listed Below

Research and Advisory Services BPAs provide unlimited access to telephone inquiry support, access to research via Web sites and analyst support for the number of users registered. In addition, the services provide independent advice on tactical and strategic IT decisions. Advisory services provide expert advice on a broad range of technical topics and specifically focus on industry and market trends. BPA listed below.

Gartner Group (N00104-03-A-ZE77); (703) 226-4815; Awarded Nov 02; one-year base period with three one-year options.

Ordering Expires: 27 Nov 06

Authorized Users: All DoD components and their employees, including Reserve Components (Guard and Reserve); the U.S. Coast Guard; other government employees assigned to and working with DoD; nonappropriated funds instrumentalities of the DoD; DoD contractors authorized in accordance with the FAR and authorized Foreign Military Sales.

Web Link: <http://www.it-umbrella.navy.mil/contract/r&a/gartner/gartner.shtml>

Records Management

TOWER Software

TOWER Software - Provides TRIM Context software products, maintenance, training and services. TRIM Context is an integrated electronic document and records management platform for Enterprise Content Management that securely manages business information in a single repository through its complete life cycle. The TOWER TRIM solution provides: document management; records management; workflow management; Web-based records management; document content indexing; e-mail management; and imaging. The DoD Enterprise Software Initiative (ESI) Enterprise Software Agreement (ESA) provides discounts of 10 to 40 percent off GSA for TRIM Context software licenses and maintenance and 5 percent off GSA for training and services.

Contractor: **TOWER Software Corporation** (FA8771-06-A-0302)

Ordering Expires: 17 Feb 08 (5 Dec 10 if extended by option exercise)

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

Section 508 Tools

HiSoftware 508 Tools

HiSoftware Section 508 Web Developer Correction Tools

- Includes AccRepair (StandAlone Edition), AccRepair for Microsoft FrontPage, AccVerify for Microsoft FrontPage and AccVerify Server. Also includes consulting and training support services.

Contractor: **HiSoftware, DLT Solutions, Inc.** (N00104-01-A-Q570); Small Business; (888) 223-7083 or (703) 773-1194

Ordering Expires: 15 Aug 07

Web Link: <http://www.it-umbrella.navy.mil/contract/508/dlt/dlt.shtml>

Warranty: IAW GSA Schedule. Additional warranty and maintenance options available. Acquisition, Contracting and Technical fee included in all BLINS.

ViViD Contracts

N68939-97-D-0040

Contractor: **Avaya Incorporated**

N68939-97-D-0041

Contractor: **General Dynamics**

VIVID provides digital switching systems, cable plant components, communications and telecommunications equipment and services required to engineer, maintain, operate and modernize base level and ships afloat information infrastructure. This includes pier-side connectivity and afloat infrastructure with purchase, lease and lease-to-own options. Outsourcing is also available. Awarded to:

Avaya Incorporated (N68939-97-D-0040); (888) VIVID4U or (888) 848-4348. Avaya also provides local access and local usage services

General Dynamics (N68939-97-D-0041); (888) 483-8831

Modifications: Latest contract modifications are available at <http://www.it-umbrella.navy.mil>

Ordering Expires:

Contract ordering for all new equipment purchases has expired. All Labor CLINS, Support Services and Spare Parts can still be ordered through 28 Jul 07.

Authorized users: DoD and U.S. Coast Guard

Warranty: Four years after government acceptance. Exceptions are original equipment manufacturer (OEM) warranties on catalog items.

Acquisition, Contracting & Technical Fee: Included in all CLINs/SCLINs

SSC Charleston Order Processing: como@mailbuoy.norfolk.navy.mil

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

TAC Solutions BPAs

Listed Below

TAC Solutions provides PCs, notebooks, workstations, servers, networking equipment and all related equipment and services necessary to provide a completely integrated solution. BPAs have been awarded to the following:

Dell (N68939-97-A-0011); (800) 727-1100, ext. 7233795

GTSI (N68939-96-A-0006); (800) 999-4874, ext. 2104

Hewlett-Packard (N68939-96-A-0005); (800) 727-5472, ext. 15614

Ordering Expires:

Dell: 31 Mar 07 (includes one one-year option)

GTSI: 31 Mar 07 (includes one one-year option)

Hewlett-Packard: 07 May 07 (includes one one-year option)

Authorized Users: DON, U.S. Coast Guard, DoD and other federal agencies with prior approval.

Warranty: IAW GSA Schedule. Additional warranty options available.

Web Links:

Dell

<http://www.it-umbrella.navy.mil/contract/tac-solutions/dell/dell.shtml>

GTSI

<http://www.it-umbrella.navy.mil/contract/tac-solutions/gtsi/gtsi.shtml>

Hewlett-Packard

<http://www.it-umbrella.navy.mil/contract/tac-solutions/HP/HP.shtml>

Department of the Navy Enterprise Solutions BPA

Navy Contract: N68939-97-A-0008

The Department of the Navy Enterprise Solutions (DON ES) BPA provides a wide range of technical services, specially structured to meet tactical requirements, including worldwide logistical support, integration and engineering services (including rugged solutions), hardware, software and network communications solutions. DON ES has one BPA.

Computer Sciences Corp. (N68939-97-A-0008); (619) 225-2600; Awarded 7 May 97

Ordering Expires: 31 Mar 07 (Call for extension information)

Authorized Users: All DoD, federal agencies and U.S. Coast Guard.

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

Information Technology Support Services BPAs Listed Below

The Information Technology Support Services (ITSS) BPAs provide a wide range of IT support services such as networks, Web development, communications, training, systems engineering, integration, consultant services, programming, analysis and planning. ITSS has four BPAs. They have been awarded to:

Centurum Information Technology, Inc. (Small Business) (N00039-98-A-3008); (619) 224-1100; Awarded 15 Jul 98

Lockheed Martin (N68939-97-A-0017); (240) 725-5074; Awarded 1 Jul 97

Northrop Grumman Information Technology
(N68939-97-A-0018); (703) 413-1084; Awarded 1 Jul 97

SAIC (N68939-97-A-0020); (703) 676-2388; Awarded 1 Jul 97

Ordering Expires:

Centurum: 14 Jul 07 (Call for extension information)

Lockheed Martin: 30 Jun 07 (Call for extension information)

Northrop Grumman IT: 11 Feb 07 (Call for extension information)

SAIC: 30 Jun 07 (Call for extension information)

Authorized Users: All DoD, federal agencies and U.S. Coast Guard

Web Links:

Centurum

<http://www.it-umbrella.navy.mil/contract/itss/centurum/itss-centurum.shtml>

Lockheed Martin

<http://www.it-umbrella.navy.mil/contract/itss/lockheed/itss-lockheed.shtml>

Northrop Grumman IT

<http://www.it-umbrella.navy.mil/contract/itss/northrop/itss-northrop.shtml>

SAIC

<http://www.it-umbrella.navy.mil/contract/itss/saic/itss-saic.shtml>



The DON IT Umbrella Program Team
offers great customer service!

Visit us on the Web

DON IT Umbrella Program site:

www.it-umbrella.navy.mil

ITEC Direct e-commerce site:

www.itec-direct.navy.mil

DoD Enterprise Software Initiative:

www.esi.mil



Thanks for letting us serve you for 18 great years!

Since 1988, the Umbrella Program has assisted the Department of Defense and Department of the Navy in making efficient use of IT dollars. The Umbrella Program provides management, technical expertise and financial resources to support the timely and cost effective placement of acquisition vehicles for hardware, software and services. We provide full service from contract conception to the end of contract life.

The Umbrella Program supports agile business systems and net-centric operations by offering robust, integrated, standards-compliant tools. The Umbrella Program combines the systematic business strategies of the DoD and DON into a customer friendly solution that means big savings for you in both time and money.

Please call us for assistance with all your IT needs.

www.it-umbrella.navy.mil

DEPARTMENT OF THE NAVY
COMMANDING OFFICER
SPAWARSYSCEN CHARLESTON
CHIPS MAGAZINE
9456 FOURTH AVE
NORFOLK VA 23511-2130
OFFICIAL BUSINESS

PERIODICAL POSTAGE AND
FEES PAID NORFOLK, VA AND
ADDITIONAL MAILING OFFICE
SSC CHARLESTON
CHIPS MAGAZINE
USPS 757-910
ISSN 1047-9988