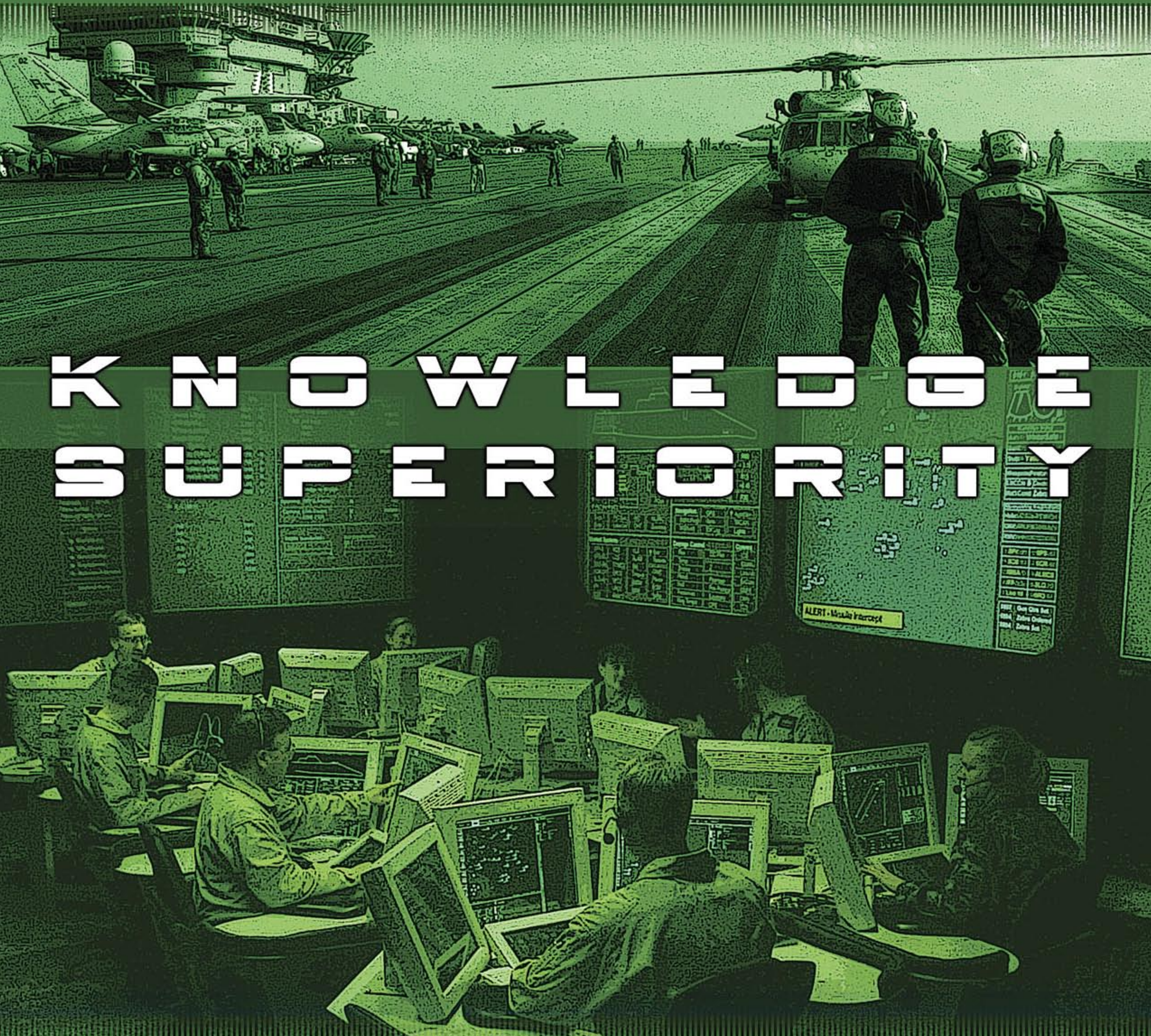
CHIPS magazine

JUL-SEP 2005



KNOWLEDGE SUPERIORITY

dedicated to sharing
information ÷ technology ÷ experience

Department of the Navy
Chief Information Officer
Mr. David Wennergren

Space & Naval Warfare Systems Command
Rear Admiral Kenneth D. Slaght

Space & Naval Warfare Systems Center Charleston
Commanding Officer
Captain Cloyes R. "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 & Naval Warfare Systems Center, San Diego, CA.

CHIPS is published quarterly by the Space & 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.

Features

Page 6

"I love telling our people what it is we need to achieve and then watch them use their talent in ways I could not imagine to make it happen."

U.K. Commodore Peter Walpole
Deputy Director
Combined Joint Operations
from the Sea Center of Excellence

Page 8

"We want to make sure we have the right Sailor, in the right place, at the right time, with the right knowledge to meet the Navy's mission requirements."

Vice Adm. J. Kevin Moran
Commander, Naval Education and
Training Command

Page 11

"FORCEnet is about transforming information and knowledge into decisive effects for anyone, anytime, anyplace – securely!"

Rear Adm. William D. Rodriguez
Space & Naval Warfare Systems Command
Chief Engineer

Page 13

Navy Information Professional officers describe how knowledge management is giving commanders and watchstanders the "knowledge edge" in a series of articles beginning with the KM successes achieved by the Multi-National Force-Iraq Knowledge Management Divsion.

CHIPS Jul - Sep 2005

Volume XXIII Issue III

On the cover. Persian Gulf (Jan. 11, 2005) - An SH-60F Seahawk helicopter, assigned to the "Dusty Dogs" of Helicopter Anti-Submarine Squadron Seven (HS-7), is refueled prior to flight operations aboard the USS Harry S. Truman (CVN 75). U.S. Navy photo by Photographer's Mate Airman Gregory A. Pierot. Bottom photo: Naval Surface Warfare Center (NSWC) Dahlgren, Va. (Aug. 19, 2004) - Navy Reservists, scientists and engineers work in the Integrated Command Environment (ICE) Human Performance Laboratory located at NSWC Dahlgren. The ICE lab focuses on the Navy's evolving human performance and human systems integration (HSI) testing. U.S. Navy photo.

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 or fax (757) 445-2103, DSN 565.

Editor's Notebook

Whether you are a Marine or Soldier on the ground in Iraq, a strike group commander or Department of Defense (DoD) business warrior, you need the knowledge superiority that the aggregate of DoD technologies can deliver.

DoD and Department of the Navy (DON) information technology users from the medical community to the financial community, from logistics to our fighting forces rely on the integrity, authenticity and non-repudiation of the data, networks and systems they use.

DoD information technology users and warfighters rely on many different systems, networks and a myriad of data sources. But they all have a common requirement: The absolute assurance that Defense networks and data are unimpeachable, impregnable to attack and real-time.

Anything less puts the DoD mission and lives in jeopardy.

Without the performance of information assurance (IA) and the practice of knowledge management (KM), knowledge superiority is only a vision.

In this issue, leaders and users of Defense IT explore the importance of information assurance and knowledge management in securing Defense and Navy networks to ensure the ultimate objective — knowledge superiority.

At one of our outreach events, the *CHIPS* staff had the pleasure of meeting U.K. Commodore Peter Walpole, deputy director Combined Joint Operations from the Sea Center of Excellence. Naturally, we asked for an interview! Thanks to 2nd Fleet public affairs team for facilitating. Go to page 6 to read about how working, training and experimenting jointly in transformational initiatives will improve interoperability for the NATO alliance.

Closer to home, the *CHIPS* staff had the pleasure of meeting our new SPAWAR Systems Center (SSC) Charleston Commanding Officer, Capt. Cloyes R. "Red" Hoover.

Welcome new subscribers!

Sharon Anderson

May 18, 2005 - U.K. Royal Navy Commodore Peter Walpole, deputy director Combined Joint Operations from the Sea Center of Excellence, visits the CHIPS exhibit at TechNet 2005 in Washington, D.C.

U.K. Royal Navy Commodore Peter Walpole (center, head of table) exercises command and control capabilities with the 2nd Fleet staff onboard the 2nd Fleet flagship, USS Iwo Jima (LHD 7). "Personally getting to know and work alongside each other is the best way to start to break down barriers, and it is the first step in delivering combined warfighting capability," said Walpole. Photo by U.S. Navy Cmdr. Dave Werner.

Members of SCC Charleston at the SCC Charleston Tidewater Node of the FORCEnet Composeable Environment (FnCE). Left to right: Will Gex, chief engineer, Tidewater C4ISR Department; Jennifer Watson, head, Tidewater C4ISR Department; Capt. Cloyes R. "Red" Hoover, commanding officer, SSC Charleston; Bobby Hensley, head, ISR and Navigation Division; and Ron Lowder, chief of operations, Tidewater C4ISR Department. Tidewater leaders gave Capt. Hoover a tour of the FnCE and other SPAWAR facilities in the Tidewater Virginia area.

DON CIO

Putting information to work for our people

As a firm believer in the power of effective knowledge management (KM), I have been thrilled to witness the KM successes of the Navy and the Marine Corps. In the early days of our implementation of KM, we focused a lot of energy on education and awareness and ways to encourage commands to embrace this important concept. Since then, KM has been woven into the fabric of the Department, with KM tenets incorporated into strategic documents, operations, education and acquisition — a powerful change from "understanding" to "doing."

Network-centric warfare is KM; FORCEnet, which makes network-centric warfare an operational reality, is KM; knowledge dominance and information superiority are KM. While support for KM is still a priority at the highest levels of the DON, KM is being recognized as everyone's business.

Knowledge officers are assigned to carrier strike group staffs. One such staff revolutionized staff planning meetings using a tool called Knowledge Web (K-Web) to store, update and display knowledge regarding situational awareness. Using K-Web, staff members can come up to speed before their planning meetings, allowing meeting discussions to focus on tactical and strategic considerations. The Commander, Naval Reserve Force has done an outstanding job of using KM tools and methods to restructure the headquarters management structure for the Naval Reserve Force. Through an initiative of the Marine Corps Center for Lessons Learned, Marines in Iraq, Afghanistan and Haiti collected, analyzed and distributed lessons learned in combat, and are sharing this knowledge with other services and joint forces. Rear Adm. Nancy Brown, as you'll read in this issue of *CHIPS*, established the Multi-National Force-Iraq (MNF-I) KM Division. MNF-I includes KM in every aspect of operations.

The Navy Personnel Development Center has set up 14 learning centers, each with a dedicated knowledge management director, to foster functional knowledge exchange, learning and the creation of knowledge-sharing communities of practice. Navy Knowledge Online (NKO) now has over 480,000 users, making education, training, collaboration and self-service transactions available via an enterprise portal. Additionally, KM courses are offered at various levels of the DON and the Department of Defense. The National Defense University and numerous other institutions teach KM courses; the Fleet Tactical Training Group, Pacific teaches an afloat KM course; the DON CIO facilitates a two-day organizational KM course; and the Naval Postgraduate School offers a two-course KM sequence via distance learning.

For Naval warfighters and those who support them, knowledge management is putting information, communities, processes and tools together to allow our people to do better work, make better decisions, and provide for the best trained, enlightened and most agile military force in the world.

Dave Wennergren

DEPARTMENT OF THE NAVY - CHIEF INFORMATION OFFICER
WWW.DONCIO.NAVY.MIL

U.K. Royal Navy Commodore Peter Walpole
Deputy Director
Combined Joint Operations from the Sea Center of Excellence

In March 2005, Commander, U.S. 2nd Fleet established the Combined Joint Operations from the Sea (CJOS) Center of Excellence (COE) to facilitate joint maritime expeditionary transformation in support of NATO Supreme Allied Commander Transformation.

The COE leverages concepts through synergistic, opportunistic, cooperative efforts. It draws benefits directly from the operational tempo of its surroundings and maintains a high state of readiness.

U.K. Commodore Peter Walpole, deputy director Combined Joint Operations from the Sea Center of Excellence, discusses how working, training and experimenting jointly in transformational initiatives will improve interoperability for allied and coalition fighting forces.

CHIPS: What is your role as the deputy director of the Combined Joint Operations from the Sea (CJOS) Center of Excellence (COE) ?

CDRE Walpole: As deputy commander, I ensure that the commander's alliance responsibilities are being met. As with many other commanders, Vice Adm. Mark Fitzgerald, 2nd Fleet commander, wears multiple hats and is responsible to different commanders for varying elements of 2nd Fleet's capability. He also has 2nd Fleet to run and train for global operations. So I work to drive forward his agenda for NATO capability.

For the NATO alliance, Striking Fleet Atlantic has provided a Combined Joint Task Force (CJTF) Headquarters in support of NATO missions for nearly a decade. The benefits of sea-basing command and control (C2) for joint operations were quickly recognized by NATO. So, when Striking Fleet answered the call — NATO was delighted.

Over the last 10 years, Striking Fleet Atlantic has been a driver in the overall development of Combined Joint Task Force concepts covering everything from deployed C2, initial entry operations, to theater liaison and reconnaissance. We have also conducted and commanded some of the largest exercises ever seen by the alliance while we have been driving toward delivering CJTF capability. The Strong Resolve series of exercises culminated in Striking Fleet operating as a CJTF headquarters, commanding over 33,000 personnel deployed throughout northern Europe in spring 2002.

The United States also has a proposal to establish a COE for Combined Joint Operations from the Sea resident within 2nd Fleet. This presents the alliance with a great opportunity to capitalize on ongoing initiatives here at 2nd Fleet in the areas of Sea Basing and Sea Strike, and it helps NATO forces develop similar capabilities. The United States is still developing the exact size and shape of the COE, but this is something nations are eager to participate in. The United Kingdom has already agreed to provide the deputy director for this exciting new center, and like other nations, will provide temporary augmentees until the posts are formally established.

CHIPS: What have you and 2nd Fleet learned in working together that can help the U.K. and U.S. navies improve coalition coordination?

CDRE Walpole: I have learned that interoperability in C4I (command, control, communications, computers and intelligence) is less about the technology and more about the procedures, permissions and human culture. I am confident that industry can provide network solutions that address security, boundary protection, bandwidth, addressing constructs and numerous other issues that we previously thought were the difficult ones to solve. In fact, I think the harder issues are the permissions, the demonstration of acceptable risk, the translation of political imperatives and getting people used to doing something different.

In addition, we have reinforced something that I suspect our forebears have known long before the Pacific campaign at the end of World War II when the Royal Navy and U.S. Navy conducted sustained, integrated, combined operations: Personally getting to know and work alongside each other is the best way to start to break down barriers, and it is the first step in delivering combined warfighting capability.

CHIPS: When we talked a few weeks ago, you mentioned how valuable simulation and virtual training exercises can be, for example, the Joint and Combined Multi-Battle Group Inport Exercise (MBGIE). With the surge in forces fighting the global war on terrorism and the need to respond to any crisis worldwide, do you think virtual exercises will replace live training?

CDRE Walpole: As technology improves both the granularity and the wider applicability of simulated training, I see these events increasingly replacing live training as a means of developing and validating capability. There is a lot more that we can do with simulation that we are not yet doing.

On the other hand, I also believe that there is no substitute on the horizon for testing the ability of a warship to completely integrate simultaneous CIC (combat information center), bridge, engine room and flight deck operations while operating in strong winds, pitching seas and poor visibility. In other words, we must let the simulated capabilities demonstrate what they can replace rather than declaring too hastily that we only need to go to sea when we actually deploy. It may be that certain phases of training can be more effectively completed in a simulated environment, and I am convinced that we can demonstrate resource efficiencies in this area. The simulated training future is a very exciting one.

CHIPS: Are there any technological, cultural or human systems barriers to interoperability between the U.S. and U.K. navies?

CDRE Walpole: I do not believe that there are any insurmountable technological barriers to interoperability, although available resources can sometimes act as speed bumps on the road to progress. Use of language, however, is a key enabler. When referring to the United Kingdom and the United States someone once said, "We are two people divided by a common language." As a Brit, I need to remember that Americans use words differently and have very different meanings for words in common U.K. parlance.

I also have to constantly remind myself that when operating in broader coalitions many other people are working in their second and third languages when using English. It would do us all well, Brits, Americans, Canadians and Australians to remember to slow down the speed of delivery and avoid the use of endless acronyms and esoteric military expressions. It shows courtesy and consideration to all coalition members and improves common understanding.

CHIPS: U.S. military services are working to improve interoperability within the services. Is interoperability an issue for U.K. forces?

CDRE Walpole: Each of the U.S. services are often bigger institutions than the armed forces of many NATO countries. It is not surprising; therefore, that issues of interoperability between the U.S. services can sometimes be as big an issue as between, say, the Royal Navy and the U.S. Navy.

Within the United Kingdom, the biggest single initiative to deliver truly joint interoperable forces has been the use of joint funding. There is no single service acquisition funding in the United Kingdom. All acquisition is done jointly. This has forced improved interoperability because the project office buying ultra high frequency (UHF) radios or logistics software tools does so across the whole business area of defense. That means that economies of scale in acquisition and support can be achieved while still taking account of unique environments.

That said, the United Kingdom continues to work with legacy systems acquired before our most recent acquisition reforms, and it will be a while; therefore, before all of the benefits can be realized. I have no doubt; however, that joint acquisition is the way to go to improve interoperability and deliver value for money.

CHIPS: Your background as a principal warfare officer (PWO) specializing in communications and electronic warfare, sea tours and responsibilities for all aspects of officers' communications training brings unique talent to your role as the CJOS COE deputy director. How do you apply your experience in making sure that British warfighters get the training and equipment they need?

CDRE Walpole: Matching valid requirements to realistic opportunities is key to the effective delivery of both training and future capabilities. It sounds a bit like an online dating service, but I have found it to be true.

CHIPS: The U.S. Army's G6 and chief information officer, Lt. Gen. Steven Boutelle, recently stated that if warfighters aren't given the right technology to work with in the battlespace, they will buy it themselves. Have you found this to be the case in the Royal Navy?

CDRE Walpole: It may be that our purse strings are a little more tightly controlled and that devolved responsibilities for purchasing do not always extend all the way to the warfighter in the United Kingdom. That said, I do recognize the ingenuity and adaptability of our current generation of sailors, and I am a firm believer that an empowered, informed sailor makes a formidable foe for our enemies.

I always want to allow the good sense and innovation of our people to bring forward the best ideas of how to confront today's challenges. I love telling our people what it is we need to achieve and then watch them use their talent in ways I could not imagine to make it happen.

In 1994, U.K. Royal Navy Commodore Peter Walpole undertook a two-year tour within the Communications and Information Systems Plans and Policy Branch at the headquarters of the Supreme Allied Commander, Atlantic in Norfolk, Va. On return to the United Kingdom, Walpole commanded the Type 23 frigate HMS Westminster for nearly two years. In 1998, he took command of HMS Lancaster, his second Type 23 frigate, assigned to NATO Standing Naval Force Atlantic.

Promoted to captain in December 1998, Walpole led the Royal Navy study into qualifications and examination structure for commanding, executive and watchkeeping officers on behalf of the Commander in Chief Fleet. Before joining the staff of Second Fleet/Striking Fleet Atlantic, Capt. Walpole served for two years as the Director of Maritime Intelligence within the U.K. Defense Intelligence Staff. He served as deputy chief of staff from June 2001 to July 2003, was promoted to the rank of commodore and took his present position as deputy director Combined Joint Operations from the Sea (CJOS) Center of Excellence (COE).

Editor's Note: NATO Striking Fleet Atlantic was deactivated June 24, 2005. The CJOS COE was established as a new beginning for NATO transformation efforts. CHIPS

Vice Admiral J. Kevin Moran

Commander, Naval Education and Training Command

Talks about how Navy Knowledge Online serves the education and training needs of today's Navy Sea Warriors

When CHIPS asked the Naval Education and Training Command to explain the significance of the redesigned Navy Knowledge Online, Vice Adm. Moran stepped up to the plate to answer some questions and explain the importance of NKO to today's warfighters.

The right quality and number of trained, professional, joint warfighters are necessary to have the "right" force to take on the challenges of the 21st century. We must invest in our people and their warfighting excellence. By meeting the personal and professional needs of our diverse population of Sailors, Reservists, civilians and their families, we ensure the highest level of personnel readiness. We are developing a Human Capital Strategy to create a workforce that provides the right skills, at the right time, to accomplish the right work.

To realize the opportunities and navigate the challenges ahead, we must have a clear vision of how our Navy will organize, integrate and transform. Sea Power 21 is that vision. It will align our efforts, accelerate our progress and realize the potential of our people. The foundation of Sea Power 21 is our people. Sea Warrior implements our Navy's commitment to the growth and development of our people. It will serve as the foundation of warfighting effectiveness by ensuring the right skills are in the right place at the right time.

Traditionally, our ships have relied on large crews to accomplish their missions. Today, our all-volunteer service is developing new combat capabilities and platforms that feature dramatic advancements in technology and reductions in crew size. The crews of modern warships are streamlined teams of operational, engineering and information technology experts who collectively operate some of the most complex systems in the world.

As optimal manning policies and new platforms further reduce crew size, we will increasingly need Sailors who are highly educated and expertly trained. The goal of Sea Warrior is to integrate the Navy's manpower, personnel and training organizations — active and Reserve — into a single, efficient, information-rich human resources management system.

Its focus is on growing individuals from the moment they walk into a recruiting office through their assignments as master chiefs or flag officers, using a career continuum of training and education that gives them the tools they need to operate in an increasingly demanding and dynamic environment. Through Sea Warrior, we will identify Sailors' precise capabilities and match them to well-articulated job requirements.

Behind the process improvements fostered by Sea Warrior is advanced technology. Navy Knowledge Online, the Navy's knowledge portal, is the key element in ensuring Sea Warrior succeeds in providing the fleet with the right Sailor, who has the right training at the right time. Career path development for enlisted Sailors is well under way through capturing a Sailor's progress along five vectors: professional development; personal development; professional military education and leadership; certificates and qualifications; and professional performance.

The same intelligent agents that analyze a Sailor's job preferences and skills and compare them to available jobs will also interrogate this career model and evaluate the Sailor's progression along each vector and factor this information into assignment recommendations.

This will help Sailors and their supervisors to better understand individual growth and development and highlight strengths and skills that are in need of improvement. Linked directly to the job requirements, the 5 Vector Model (5VM) will help develop the right knowledge, skills and abilities in our Sailors and complete a critical association between personnel and training.

CHIPS: What are some of the new or improved capabilities of NKO?

Vice Adm. Moran: The right information at the right time will enable our Sailors to make the right career choices. Providing this information effectively through NKO is essential.

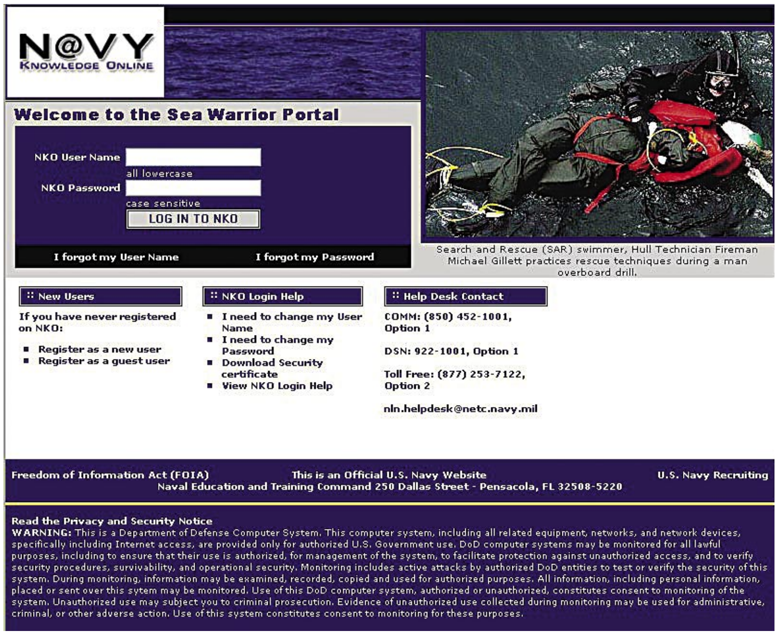
The goal of NKO Redesign was to improve overall usability of the site by making content easier for users to find. Users will experience a more intuitive display with detailed login and help instructions, an improved user-friendly navigation model and labeling of content. The new layout focuses on content relevant to the individual based upon the user's status: active duty, Reserve, civilian, rank, rate, etc. Changes include a new global navigation structure that supports all users, improved site nomenclature, content and layout improvements for information and community specific user home pages.

Top-level categories are available at all times and local toolbars drill down into those categories to direct users to content

"The goal of Sea Warrior is to integrate the Navy's manpower, personnel and training organizations – active and Reserve – into a single, efficient, information-rich human resources management system."

– Vice Adm. J. Kevin Moran

Sea Warrior implements the Navy's commitment to the growth and development of its people.


N@VY KNOWLEDGE ONLINE

Welcome to the Sea Warrior Portal

NKO User Name
all lowercase
NKO Password
case sensitive
LOG IN TO NKO

I forgot my User Name   I forgot my Password

Search and Rescue (SAR) swimmer, Hull Technician Fireman Michael Gillett practices rescue techniques during a man overboard drill.

:: New Users

If you have never registered on NKO:

- Register as a new user
- Register as a guest user

:: NKO Login Help

- I need to change my User Name
- I need to change my Password
- Download Security certificate
- View NKO Login Help

:: Help Desk Contact

COMM: (850) 452-1001, Option 1

DSN: 922-1001, Option 1

Toll Free: (877) 253-7122, Option 2

nln.helpdesk@netc.navy.mil

Freedom of Information Act (FOIA)   This is an Official U.S. Navy Website   U.S. Navy Recruiting
Naval Education and Training Command 250 Dallas Street - Pensacola, FL 32508-5220

Read the Privacy and Security Notice

WARNING: This is a Department of Defense Computer System. This computer system, including all related equipment, networks, and network devices, specifically including Internet access, are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed or sent over this sytem may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of the system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

NKO, now designated as the Sea Warrior Portal.

quickly and seamlessly. Category areas, (formerly called tabs), are: Career Management, Leadership, Personal Development, Learning, Reference and Organizations & Communities. The 5 Vector Model, the Navy Personnel Command (NPC) legacy Job Advertising Selection System, now referred to as JASS Career Management System (JCMS), and National Security Personnel System will be found under Career Management. General Military Training (GMT), health and finance will be found under Personal Development.

Navy E-Learning and the electronic training jacket (ETJ) will be found under Learning. Navy library programs, such as the Navy Warfare Library, and Naval Telecommunication Procedures (NTP) will be found under Reference. Learning Centers, Navy Reserve and educational institutions will be found under Organizations & Communities.

NKO will provide access to specific content on the home page through administrator, personalization and user customization. For example, users can manage communities, teams and the group pages they desire to access directly from their home page. A top banner on the home page will now provide immediate access to common tools such as search, advanced search, white pages, instant messaging, the NKO library and user profile. NKO content managers will have the ability to add keywords to allow more precise search tool results for portal pages.

CHIPS: What kind of technologies does the redesigned NKO use?

Vice Adm. Moran: The effective use of technology in support of Sea Warrior is taking training and support capabilities to Sailors wherever they are around the globe. Since June 2004, under a competitively awarded contract, we have employed Computer Sciences Corp. (CSC) to transition to Phase II of NKO development. CSC implemented the Art Technology Group (ATG) Portal Suite with Document Management and Content Administration, Bantu Instant Messaging and ATG Advanced Search. These leverage Autonomy products, such as the Intelligent Data Operating Layer (IDOL) Server and Dynamic Reasoning Engine (DRE). Autonomy DRE uses natural language and concept matching techniques to provide higher quality search results. Avenue A | Razorfish, a CSC partner, has done much of the user and portal analysis for the navigation and redesign transition.

CHIPS: What are some of the functionalities that Sailors use most?

Vice Adm. Moran: Two of the most popular functionalities Sailors use are viewing their electronic training jacket and accessing Navy E-Learning courses. Navy E-Learning hosts over 4,000 courses from information technology to soft skills, to Navy-developed courses. As more courses come online, Sailors in both resident schoolhouses and around the globe are able to take distance-learning courses, whenever it's convenient.

A Sailor's ETJ shows all the training they've taken since coming into the Navy, awards and more. Quickly gaining in popularity on NKO is accessing the Sailor's 5VM, which displays a Sailor's current skill sets along vectors such as professional development, personal development and leadership. The 5VM identifies any skill gaps Sailors might have in a particular area and the skills and courses needed to close those gaps.

CHIPS: Since NKO is a portal, can Sailors log on and use it all day in the performance of their naval duties? In a typical day, how would a Sailor use the diverse features that NKO offers?

Vice Adm. Moran: Many Sailors log on in the morning and remain on the portal all day. Some Sailors log on and look at current events, everything from their specific community, to what is happening around the fleet. Sailors are able to access a myriad of manpower, personnel, training and education applications through NKO. They can search their individual community to see what's current in their specific field, conduct threaded discussions, chat or instant message with subject matter experts or their peers on a variety of topics. They access their individual 5 Vector Model and ascertain skills required for a specific Navy job or access the JCMS site to see specific jobs and map them against their current skill sets.

They browse the Navy E-Learning catalog and enroll in online courses that range from information technology courses, to leadership and management courses, to specific Navy-developed courses they once could only take in a resident classroom. Sailors may also use the portal to take mandatory courses, such as annual security training. Many Sailors access their electronic training jacket on a routine basis to verify documentation of schooling, coursework or other completed training.

CHIPS: What functionalities of NKO afloat are available to fleet users? Is connectivity a problem for afloat users because of bandwidth constraints?

Vice Adm. Moran: NKO, now designated as the Sea Warrior Portal, is partnering with the Naval Sea Systems Command (NAVSEA) Distance Support (DS) Program, which is rolling out DS to all ships by early fiscal year 2007. The first spiral phase of NKO with the redesigned look and feel, a subset of content, courses and shipboard specific communities, will be deployed to ships with DS installed early July 2005.

A broader Sea Warrior portal, with NKO as the front door, is being integrated with the JCMS, 5VM, ETJ and more in a spiral development phased approach through October 2005. We're focused on ensuring Sailors afloat are afforded the same access to manpower, personnel, training and educational content and information their ashore counterparts have. This may entail a disconnected (from the Internet) suite of applications, integrated in a way that allows for a much smaller footprint than ashore, so that afloat servers can handle the applications.

Due to the nature of each ship's platform and inherent "at sea" constraints, bandwidth certainly plays a role everywhere; however, we're progressing toward a solution that will work afloat regardless of bandwidth.

CHIPS: What is your process for gathering, analyzing and deploying user requirements?

Vice Adm. Moran: Since June 2004, CSC partnered with Avenue A | Razorfish to take a scientific methodology approach to usability of the NKO portal for the redesign effort. We conducted user research interviewing fleet Sailors, civilians and Reservists stationed in San Diego, Calif., Great Lakes, Ill., Kings Bay, Ga., Norfolk, Va., Reserve stations and onboard the submarine USS Albany (SSN 753), the aircraft carrier USS George Washington (CVN 73), the amphibious assault ship USS Tarawa (LHA 1) and the destroyers USS John Paul Jones (DDG 53) and USS Mason (DDG 87), among others.

The research provided insight into attitudes and behaviors to ensure the redesign would be intuitive and provide value to each user. Additionally, we solicited and continue to solicit user feedback and requirements via a submission form and user surveys that are reviewed by a governance board. If a submission is validated, requirements are prioritized and migrated into the overall program management process for subsequent deployment.

CHIPS: What improvements are planned for NKO in the future?

Vice Adm. Moran: Sea Warrior's rich language of Sailor knowledge, skills and abilities makes possible profound improvements in human systems integration. System engineers can identify the exact capabilities of Sailors in a particular job, take these capabilities to the lab, and design a system that "fits" the Sailor.

As with any program, the advent of technology and systems continue to grow. We need to remain flexible to incorporate those that work to the Sailor's advantage. As we look at the Navy's requirements for Sailors to be trained for specific jobs and skill sets, it's vital we incorporate those tools that will empower Sailors in everyday use, allowing content and information to be updated immediately for their benefit and to meet fleet requirements.

NKO will fit into the workday to enable Sailors to make career decisions while they're in the Navy and whenever they transition to civilian life. We are continuing to analyze how Sailors use the portal, and we are looking at tools that will allow true metrics to be gathered to help us determine the best way to affect that growth.

Sea Warrior, supported through NKO, is a key element in the Navy's transformation. It is all about fleet readiness. We want to make sure we have the right Sailor, in the right place, at the right time, with the right knowledge to meet the Navy's mission requirements.

CHIPS

NKO Redesign

The redesigned NKO required transitioning the original Navy Knowledge Online site with the same functionality and capabilities to new servers, using new and current portal technology and migrating more than 20 gigabytes of data, content and courses.

There are now more than 480,000 worldwide users of Navy Knowledge Online. Sailors can learn more about Navy Knowledge Online's redesign functionalities and capabilities by exploring the links on the NKO home page.

Detailed instructions, user guides and tutorials can be found under the "Inside NKO" tab. These links and learning tools will be updated and can be found on the NKO home page under "About NKO." For more information about Navy Knowledge Online or to jump-start your career educational planning, visit the NKO Web site at http://www.nko.navy.mil/.

Rear Admiral William D. Rodriguez Chief Engineer (SPAWAR 05) Space and Naval Warfare Systems Command Talks about FORCEnet Development

The Space and Naval Warfare Systems Command is the chief engineer for delivering FORCEnet capabilities. To accomplish this goal the FORCEnet Innovation and Experimentation Framework was established to institutionalize and streamline technology discovery, establish a transition process and identify a funding structure to accelerate fielding and sustainment.

FORCEnet is the Naval net-centric warfare operational construct and architectural framework for integrating warriors, sensors, networks, command and control, platforms and weapons into a networked, distributed force, scalable across the spectrum of conflict from seabed to space, from sea to land. The technical vision for FORCEnet is to provide a networked architecture that will allow integrated system-like capabilities to be quickly composed in response to requirements, challenges and demands of the dynamic current and future operational situation.

CHIPS asked Rear Adm. Rodriguez for an update on FORCEnet development just days before the FORCEnet Engineering Conference, which is planned for June 28-30, 2005, in Norfolk, Va. The purpose of the conference is to promote a collaborative environment for key engineering communities to identify and address challenges and issues that impact the successful transformation of the Naval enterprise to FORCEnet.

CHIPS: Where does the Navy stand in developing FORCEnet architecture?

Rear Adm. Rodriguez: FORCEnet is not just an architecture per se, it's actually an architectural framework coupled with an operational construct. So, while we have many of the elements needed for traditional architectures, things like defined "mission threads" detailing a particular set of system interactions required to acquire and engage a contact, FORCEnet will continue to evolve over time and these products will change as technology changes.

That said, there are particular documents now available for guidance to systems developers. The FORCEnet Architecture Volumes 1 and 2 have been published as have the initial operational views, and supplemental guidance has been published by various program executive officers for the programs under their control.

We continue to work with the cross-service architecture groups and other related forums as we further refine these evolving products.

CHIPS: What are some of the challenges you have in implementing FORCEnet?

Rear Adm. Rodriguez: I really see two challenges, one is organizational and the other is technical. The major organizational challenges are cultural and funding which go hand in hand, such as, how do you change your way of doing business to fund future improvements? For instance, do you decommission aircraft carriers to fund network improvements? Do you maintain legacy business applications while building new ones?

The major technical challenge is maintaining legacy architectures while defining future architectures and migrating to them. Synchronizing the integration of our existing systems into joint architectures while ensuring we remain connected with our allies and coalition partners continues to be one of our biggest priorities. Additionally, we are in a process of developing an integrated road map for both tactical and non-tactical networks.

CHIPS: What direction will FORCEnet take to ensure that Navy information technology (IT) keeps up with rapidly changing requirements?

Rear Adm. Rodriguez: In the IT business, one of the roads to getting capability out there faster is to rely on the commercial marketplace to drive the solutions. Senior leadership in the Navy has directed that the government should not be in the integration business; it is best left to industry.

Having a consistent architecture and defined process on which to build programs will facilitate speed to implementation. Therefore, FORCEnet, at its core, is a prime enabler to shorten the cycle time from need identification to solution implementation.

CHIPS: How does FORCEnet interface with the Global Information Grid (GIG)?

Rear Adm. Rodriguez: FORCEnet is the Navy's instantiation of the Department of Defense (DoD) GIG. A simple analogy that illustrates the way the Navy sees this and its role in the GIG architecture development is GIG initiatives like GIG Bandwidth Expansion, which could be compared to the national interstate highway system.

The federal government builds the interstate highway system in coordination with the states, while the states build roads that connect to the interstate highway system. All users of this highway system

"FORCEnet is about transforming information and knowledge into decisive effects for anyone, anytime, anyplace – securely!"

– Rear Adm. William D. Rodriguez

employ the same traffic signals and signs for interoperability.

FORCEnet builds the Navy's roads to the GIG interstate using common standards and interoperability, such as the Joint Technical Architecture. Instead of developing our own architectures and standards from the ground up, the Navy is participating fully in DoD's architecture and standards development process to ensure interoperability.

CHIPS: What is meant by the term "composeability?"

Rear Adm. Rodriguez: Composeability enables Navy IT to deliver tailored information to the warfighter supporting Sea Power 21 and the need for a flexible and agile "FORCE." It allows for the composition of tactics, doctrine, techniques and procedures at all warfighting levels.

FORCEnet composeability provides a means to allow system-like capabilities to be constructed in response to requirements, challenges and demands during dynamic operational situations. FORCEnet brings together modern information technologies, business logic, architectures, standards and protocols to achieve this new level of required responsiveness. This approach provides flexible and dynamic functionality and allows interoperability across naval, joint, allied and coalition components.

CHIPS: What tools will be supporting the FORCEnet Engineering Process to implement the Naval transformation to a net-centric operation? How are these tools managed from a Naval enterprise level?

Rear Adm. Rodriguez: The FORCEnet Implementation Toolset (FIT) will exploit the Naval Collaborative Engineering Environment (NCEE) to implement FORCEnet system engineering practices. As part of the system engineering effort, FIT provides the mechanism for enterprise tools: requirements management and governance. This supports the FORCEnet Implementation Process and related processes to better utilize the existing infrastructure of data resources.

FIT provides the capability to collect and manage enterprise requirements for tools from all stakeholders in the Naval enterprise. FIT will match requirements to the existing tools for portfolio management for reuse, build and buy decisions.

CHIPS: Is FIT a set of guidelines or engineering techniques; can you provide an example? Is FIT a tool just available to SPAWAR or will all commands working on FORCEnet have this capability?

Rear Adm. Rodriguez: We're fairly early in the development of this toolset. We put together a beta version for initial testing and further refinement from those populating the data fields, and we've been working to make the tool more user-friendly while providing greater availability.

Of course, sensitive data must be protected, so we are working protection and permission issues as well. As FORCEnet matures, we anticipate a matching maturity of the NCEE and associated data structures.

CHIPS: How are you ensuring that FORCEnet delivers improved warfighting effectiveness?

Rear Adm. Rodriguez: FORCEnet provides much needed capability to our ultimate customer — the warfighter. We have included human systems integration in every FORCEnet product and process: assessment, experimentation, architecture and concepts. A major portion of our Trident Warrior experiment includes the impact on warfighting effectiveness (such as shared situational awareness) measured across a mission area.

CHIPS: Business systems are now included in FORCEnet. When did FORCEnet start including business processes under its umbrella?

Rear Adm. Rodriguez: FORCEnet has included business systems from the start. Initial emphasis was on the systems and infrastructure that support the warfighter directly. A large part of the Navy's IT costs is associated with business systems, and business IT supports the warfighter as critically as tactical systems.

The Navy Marine Corps Intranet (NMCI) is the naval infrastructure to support ashore requirements. Once NMCI was implemented, it became apparent that to manage IT infrastructure, return on investment had to be a priority. Applying an engineering discipline across IT is critical to obtain return on investment.

Business IT makes up one of the pillars of FORCEnet. Business IT is part of our net-centric organization on par with other tactical systems. The FORCEnet Engineering Conference is one of the venues where the FORCEnet business IT team can collaborate to determine how to accomplish this work.

CHIPS: What are your next planned activities to execute the vision for FORCEnet?

Rear Adm. Rodriguez: The FORCEnet Engineering Conference allows us to continue building a collaborative environment for key Naval engineering communities where challenges, issues and information can be exchanged impacting the direction for FORCEnet.

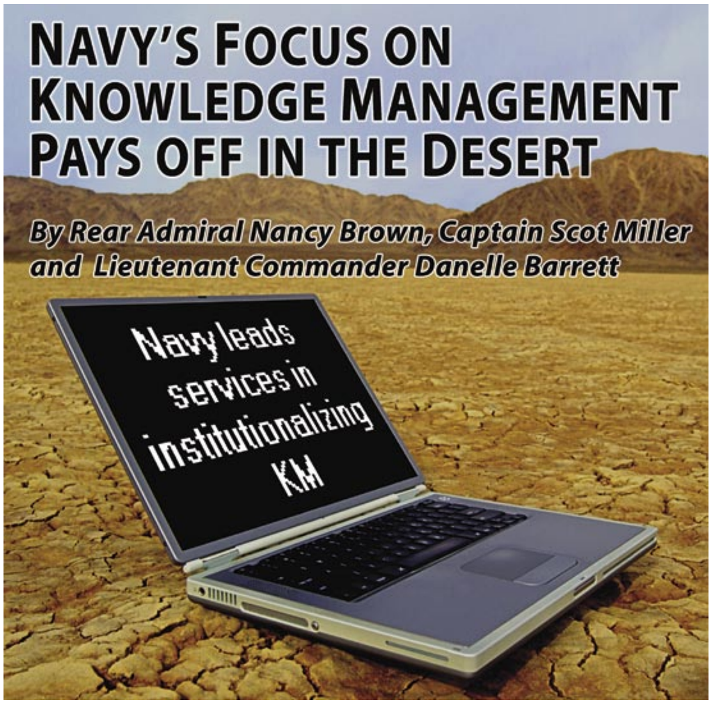
I am excited about future conferences, like this one, for communities, such as command and control (C2); communications; networks; business IT; intelligence surveillance and reconnaissance (ISR); information operations (IO); assessment and experimentation; human systems; and architecture and certifications systems, to exchange information and provide us the opportunity to adjust our focus as these communities grow and learn.

We're allowing working-level engineers and operators to join together in a structured forum with program offices, resource sponsors and users to freely exchange needs, desires and ideas.

As with any such event, we will learn from what we've done this time and make future conferences better and better over the next few years. CHIPS

Navy's Focus on Knowledge Management Pays off in the Desert

By Rear Admiral Nancy Brown, Captain Scot Miller and Lieutenant Commander Danelle Barrett



The Navy is creating knowledge-enabled organizations afloat and ashore. Since the late 1990s, proponents for knowledge management (KM) have emerged within the Navy. Commander, Pacific Fleet and Commander, Second Fleet assigned a knowledge manager to their staffs as early as 1998. Several key projects were implemented to address information management (IM), a subset of KM, and necessary precursor to success. This included Collaboration at Sea (CAS) to share information in the afloat environment and the Knowledge Wall and K-Web to improve situational awareness afloat.

In parallel, Navy and coalition networks afloat and ashore have advanced to better support these and other KM applications. The coalition wide-area networks afloat are now the primary warfighting networks used in Operations Iraqi Freedom and Enduring Freedom in Afghanistan. The Navy's early successes in KM have built a service culture of understanding and appreciation for KM which was transferred by Navy Information Professional (IP) officers to the ground war and nation-building efforts at Multi-National Force-Iraq.

While the Navy began KM early, the iterative progression of acceptance and concepts put into practice did not happen overnight or without growing pains. Recent events have codified and institutionalized KM across the Navy. In October 2001, the Navy established the IP Officer Community, an operationally oriented "Signal Corps" for the Navy. Career success as an IP derives from operational excellence in what was traditionally known as command, control, communications and computers (C4). Today, it encompasses many elements of information operations and management.

From its inception, KM was embraced as a core competency by the IP community. IPs now fill knowledge manager billets at sea, and based on demand from strike group commanders, increased their presence on strike group staffs from two in 2001 to 12 in 2005.

Fish Out of Water …

Navy officers in a ground war in Iraq? Some would compare them to "fish out of water." The exact opposite proved to be the case with their work of putting KM concepts into action in the desert. Rear Adm. Nancy Brown, the Navy's senior IP officer and one of its most experienced joint leaders, was assigned as the Deputy Chief of Staff for Communications and Information Systems for the Multi-National Force-Iraq (MNF-I) in August 2004. One of her first acts was to bring Navy IPs with KM experience to theater, and establish the MNF-I Knowledge Management Division. The strategic mission of MNF-I is:

"In partnership with the Iraqi Government, MNF-I conducts full spectrum counter-insurgency operations to isolate and neutralize former regime extremists and foreign terrorists, and organizes, trains and equips Iraqi security forces in order to create a security environment that permits the completion of the U. N. Security Council Resolution 1546 process on schedule."

MNF-I supports the maturation of Iraqi self-governance and assists with Iraqi economic redevelopment and many other aspects of nation building in support of democracy. As the senior military organization in Iraq, MNF-I also works closely with key stakeholders such as the United Nations, the U.S. Department of State and, most importantly, the Iraqi Transitional Government.

Significant improvements in communications and information systems infrastructure were ongoing to provide more robust and reliable connectivity to warfighters and decision makers, which meant information was flowing. However, it became immediately clear that information flow did not ensure shared situational awareness and operational excellence. Standardized processes and systems were needed to make sense of all the information and provide a meaningful context for enhanced decision-making. Personnel were needed to provide structure for information capture, assessment and to exchange requirements and implement process changes to leverage new technology.

The MNF-I KM Division faced daunting challenges because a freewheeling information environment had resulted with little implementation of best practices for managing the authoritativeness, trustworthiness and value attributes of information. The temptation to leap into action implementing quick wins which could lead to long-term interoperability problems was palpable. But the KM team resisted and instead adopted the approach depicted in Figure 1.

The key to success was centered in evaluating the needs of internal and external personnel for information exchange. A questionnaire was developed to quiz staff on their frustrations, ideas, documents, data, information sources and how they collaborated with other staff members. Three distinct components influenced the assessment process based on the following assumptions.

- *The purpose of KM is to enable the creation, capture, organization and sharing of knowledge within an organization and external stakeholders. This principle was a KM team focus because at MNF-I there were many pressing operational tasks in support of the campaign plan competing for people's time.*

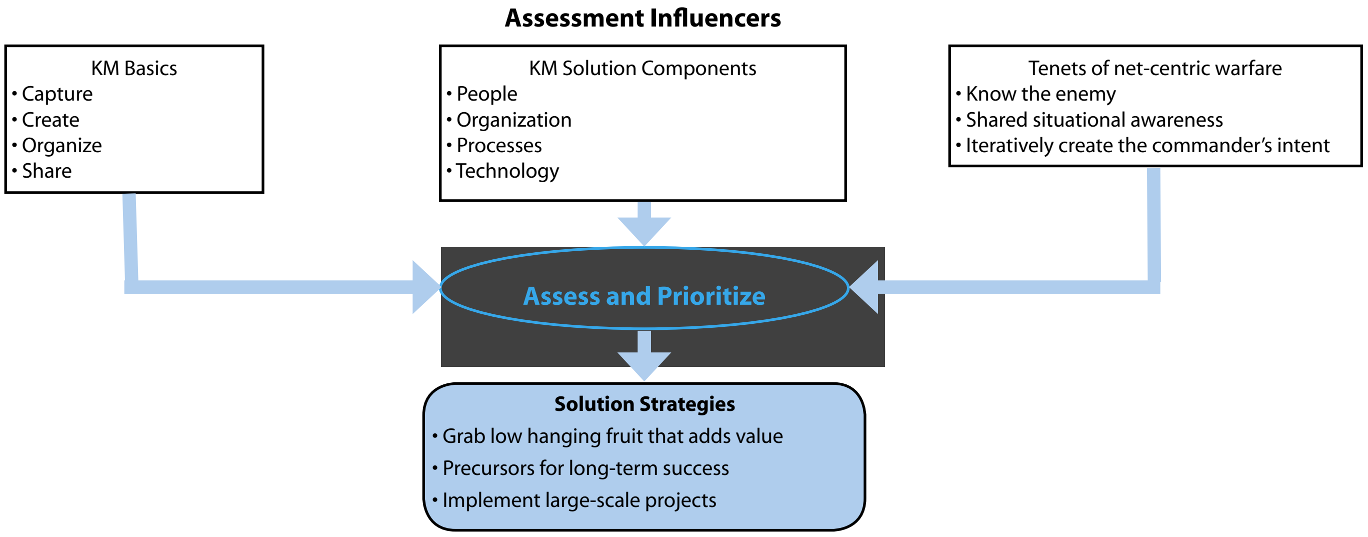

Assessment Influencers
KM Basics
• Capture
• Create
• Organize
• Share
KM Solution Components
• People
• Organization
• Processes
• Technology
Tenets of net-centric warfare
• Know the enemy
• Shared situational awareness
• Iteratively create the commander's intent
Assess and Prioritize
Solution Strategies
• Grab low hanging fruit that adds value
• Precursors for long-term success
• Implement large-scale projects

Figure1. MNF-I KM Team Initial Approach

- *All KM solutions or initiatives consist of four components: people, organization, processes and technology.*

- *Network-centric warfare conducted in a connected environment suggests that knowing the enemy is an overarching principle to success. This includes culture, religions, politics, economic landscape, etc.*

- *Shared situational awareness means more than tactical plots; it includes how MNF-I captures and shares events, such as assessing progress in economic development and measuring progress in building governance.*

- *Iteratively create the commander's intent by collectively understanding the commander's objectives, and help as a group to assist the commander create operational objectives in a spiral manner.*

The assessment paid rapid dividends. Besides providing input to the KM strategy, the team learned that continuous reassessment would have to be a part of the overall approach because of the 130 percent annual turnover rate of MNF-I personnel. The good news was that many members of the MNF-I staff were acquainted at least with process reengineering and already had good ideas that just needed the kind of help the KM team could provide to move them from concept to action. At the conclusion of the assessment, the KM team developed a three-step action plan.

The first step was to develop a KM strategy that included addressing long-term systemic knowledge sharing problems with parallel efforts to grab low hanging fruit. The team aligned strategy with the campaign plan and its four operations: security, governance, economic development and communications. It quickly became apparent that knowledge sharing was instrumental in synchronizing political, military and economic effects.

Once the overall KM strategy was created, short- and long-term enterprise solutions were formulated and executed. Plans were devised that used process and organizational changes, training, IM standards and technology to improve mission accomplishment. While long-term enterprise solutions were the priority to provide a framework for long-term success, quick organizational or process changes were targeted for immediate improvement. These parallel efforts, in compliance with the enterprise vision, would bring immediate benefits, required little or no funding and were achievable in a short time.

Grab low hanging fruit …

The KM Division understood the importance of good IM practices as a precursor to successful KM. The team began by looking at what could be done to improve IM at headquarters and with external organizations. Information management was a critical first step to efficiently and effectively provide the right information, to the right decision-makers, at the right time.

Some initiatives were simple, yet improved processes for a wide audience, such as revamping command indoctrination and developing a Web-based white pages directory tied to an electronic organizational chart, which made it easy to find personnel. A Web-enabled yellow pages directory made it easy to find people with subject matter expertise in more than 50 categories.

Mechanisms were devised to ensure consistent messages were distributed. For example, previously, there was no standard way to inform people of uniform upgrades because of a heightened security posture. It was so confusing that sometimes an e-mail about a change conflicted with information posted at guard stations. To eliminate confusion, the KM division purchased an electronic marquee system for Camp Victory South, the portion of Camp Victory that houses MNF-I headquarters and is home to several thousand personnel. Marquees were installed in areas where people congregated: chow halls, the gymnasium and Al Faw Palace. Messages were synchronized making information reliable and timely.

Some of the biggest challenges were IM deficiencies in data, the information architecture and the KM elements or organizations and processes that relied on them. The MNF-I staff is dispersed between two locations with much of the command in Al Faw Palace on Camp Victory (CV) and the Strategic Operations

Ground convoys on Route Irish are routinely attacked by insurgents using vehicle-borne or ground-planted improvised explosive devices (IEDs). Convoys typically require a protective detail of 8 to 10 people.

Portal equipment being delivered to Camp Victory. The Convoy Tracker Web service, chat and virtual meetings reduced the number of administrative ground convoys and risk to personnel.

Center (C3) in downtown Baghdad at the U.S. Embassy in the International Zone (IZ) four miles away. So ensuring command and control over the force can be facilitated by Web-enabling more information with a focus on process reengineering.

KM reduces the number of personnel at risk …

Prior to November 2004, most business was conducted in face-to-face meetings, which required travel on Route Irish, one of the most dangerous roads in Iraq. Ground convoys on this route are routinely attacked by insurgents using vehicle-borne or ground-planted improvised explosive devices (IEDs). The average convoy between Camp Victory and the IZ required a protective detail of 8 to 10 people and several hours to coordinate and conduct. In addition to the security risks and direct costs in terms of time and fuel, there were secondary costs, such as maintenance on vehicles and weapons, lost productivity during travel, etc.

Convoys were also uncoordinated centrally. Individual groups arranged convoys for administrative travel in a vacuum, unaware if others were doing the same. This created situational awareness deficiencies from a force protection standpoint and increased the possibility that more convoys than necessary were conducted. The KM team recognized that efficiencies could be realized by publicizing available seats and consolidating trips, thus conserving resources and significantly decreasing the likelihood of putting personnel at risk.

The KM team took a two-pronged approach to solve this problem. First, the KM team installed a collaborative tool server in the IZ with the help of the U.S. Joint Forces Command (USJFCOM) Standing Joint Force Headquarters (SJFHQ), which supplied the equipment, technicians and trainers. The server was federated with the server at Camp Victory to provide technology for virtual meetings with chat, Voice over Internet Protocol (VoIP), document sharing and whiteboard capabilities. Then the team conducted a training and awareness program marketing the tool as a way to reduce trips on Route Irish. The response was immediate and positive. Hundreds of people were trained to use collaborative tools for virtual meetings.

Secondly, a Convoy Tracker Web was established for personnel to sign-up online for available convoy seats for those that still needed to travel. This service further decreased the number of administrative ground convoys and risk to personnel.

Web services to the rescue …

One of the most comprehensive efforts was the realization of a Web services architecture and identification of authoritative data sources to improve the reliability of information for decision-makers and to share with the Iraqis.

Initial KM assessments revealed that there was no method to easily access or share information. While the KM team focused on immediate concerns, they also looked to the future to anticipate emerging information sharing needs. They realized that as the United States begins to turn over governance and security functions to the Iraqis over the next few years, there will be a need to securely transfer a large amount of releasable information to the Iraqis in a logical fashion. No information architecture, system or process had yet been planned to fulfill this requirement.

The existing MNF-I Web site was basically acting as a file server without any way to put the information in useful context. New data sources were cropping up like mushrooms without thought of what already existed. Many of the new databases were found to be wholly or partially duplicative of an existing source, which clouded the ability of operators to definitively trust information. The challenge was how to rein in all of these new initiatives to ensure that reliable information is easy to obtain.

The team drafted a data management strategy, an open standards portal requirements document and concept of operations to provide the means to overcome knowledge roadblocks. The portal was to be the user interface to Web services comprised of information from authoritative databases in a standard format using Extensible Markup Language (XML) with a standards-based messaging protocol, Simple Object Access Protocol (SOAP), for moving data.

These Web services would empower users to quickly and easily share information and enable security metadata tagging of information. The portal would also provide users with the ability to customize information and be notified of changes to data to improve collaboration. The portal architecture was designed with redundancy to replicate data properly tagged as releasable to the Iraqis' identically configured portal. Replication would be done iteratively, first with an air gap, and later with the capability for automatic transfer via an electronic data guard to be implemented once it received security accreditation.

The detailed portal and document management requirements generated by the MNF-I KM team were sent to about 10 organizations to see what solutions might fulfill command requirements. The USJFCOM Joint Experimentation (J9) Joint Prototype Pathway Branch was developing an open standards, open source portal as part of its Command Cross-Domain Collaborative Information Environment suite. It was selected by MNF-I to get the capability in theater in a compressed time frame. USJFCOM staff not only provided portal equipment, engineering and installation, they also provided several full-time developers to provide the initial Web services requested by MNF-I.

Additionally, USJFCOM SJFHQ prepared documentation for system users and trainers to ensure that successful system integration into the MNF-I environment was properly addressed.

Concurrently, the KM team inventoried and analyzed all databases at MNF-I, including all spreadsheets with more than 1,000 lines, to determine what data existed and who was using it. Best of breed data sources were selected and duplicative sources were eliminated. A comprehensive Information and Data Management Policy and Strategy were implemented laying out requirements for standards-based data formats and Web services to improve data reliability and interoperability throughout Iraq. Then functional data owners and managers were assigned to manage the authoritative data sources for the portal Web services that could be written.

Web services requirements were drafted including services to improve fragment orders writing, notification and search, strategic operations center briefing and administrative convoy tracking. These services were developed by USJFCOM J9. Four of these Web services have been fielded with others still in beta testing. The MNF-I Web services architecture and data management strategy were unprecedented and had immediate and positive impacts on strategic military operations in Iraq.

In all of these efforts technology was important, but the corresponding focus on awareness, process change and training was far more challenging and fundamental to making success achievable. Innovation was a basic tenet of the MNF-I knowledge management strategy. All assumptions were questioned as to why things were done a certain way. If a decision was made based on the circumstances of six months ago, the process was re-examined to determine if it was still germane. Because everything from the political situation, to warfare and personnel change every six to 12 months, it was imperative to constantly re-evaluate basic assumptions and propose new ways to conduct operations and warfare support processes.

Bringing everyone into the KM fold …

Since KM was a new concept for MNF-I, it was important to demonstrate how its concepts could be employed to directly benefit the warfighter. Understanding by key stakeholders and the command at large was critical to ensure changes of lasting value. The KM division devised a multifaceted approach for building awareness of the various KM initiatives, the importance of knowledge-enabled organizations and how sharing increases operational effectiveness.

To this end, team members fanned out among the staff popularizing the use of collaborative tools and assisting users in articulating their requirements for Web services. The requirements were then passed to engineers for development. Awareness training included such simple ideas as placing KM concepts on slides in conspicuous areas and key general officer workspaces.

The messages were hard to ignore and momentum for many of the KM initiatives soon built. Kindred spirits were discovered and leveraged across the staff. Briefings to senior leaders and key stakeholders were instrumental for securing "buy-in" for KM concepts and projects.

An organizational change for MNF-I that was essential to communicating information sharing requirements and solutions was creation of the directorate knowledge management officer (KMO). The KMO is similar in function to the information management officer (IMO) each directorate employed, so it was a construct that was easy to understand. The IMO is usually a collateral duty for an information technology savvy enlisted member or officer. The IMO assists the staff with basic computer and applications issues.

KMOs work across functional area boundaries to optimize applications and data structures, eliminate redundancies, facilitate collaboration and generally serve as information referees to ensure the integration of relevant and meaningful content into the portal. They also help users articulate trouble reports. The KM Division designed a rigorous training course and established a requirement for each directorate to assign a KMO. The KMOs provided feedback for issues to the core KM team and offered knowledge sharing opportunities generated in the various directorates.

The lessons learned and solutions fielded in Iraq were instrumental in building a military culture that includes knowledge management in every aspect of operations, not just as a separate KM function, but as an integral element of campaign success.

Rear Adm. Nancy Brown is currently vice director, Command, Control, Communications and Computer (C4) Systems, J6, Joint Staff, Washington, D.C. Brown returned in April from a seven-month deployment as the Deputy Chief of Staff for Communications and Information Systems at Multi-National Force-Iraq. Her assignment, as director for Command Control Systems, J6, North American Aerospace Defense Command and Director, Architectures and Integration, J6, U.S. Northern Command, Colorado Springs, Colo., is expected for Aug. 1, 2005.

Capt. Scot Miller is the commanding officer of the Navy Center for Tactical Systems Interoperability (NCTSI) in San Diego. He recently served six months as the first chief of the Knowledge Management Division under Rear Adm. Brown at Multi-National Force-Iraq.

Lt. Cmdr. Danelle Barrett is the communications officer on the staff of Carrier Strike Group Twelve. She recently served as the deputy knowledge manager at Multi-National Force-Iraq. CHIPS

Finding the Knowledge Edge

Using Knowledge Management Afloat to Give the Warfighter a Knowledge Edge

By Cmdr. John Hearne and Lt. Cmdr. James H. Mills

The Knowledge Edge

Knowledge is power. The old adage is true in the business world as well as in the military. Intelligence about our adversaries, our battlespace and ourselves is critical to succeeding in any military operation. To continue to dominate the maritime battlespace, the U.S. Navy must find a competitive edge — a *knowledge edge* — that will allow our forces to exploit our asymmetric advantages over our adversaries.

Carrier strike groups (CSG) and expeditionary strike groups (ESG) are expected to accomplish a wide range of tasks including: conducting inland time-sensitive strikes, maritime interdiction operations, defense of national borders, ensuring the free flow of commerce on the high seas, regional engagement and information operations.

These missions are being accomplished with fewer platforms in all corners of the globe. The new Fleet Response Plan (FRP) dictates longer periods of readiness and greater flexibility in deployments to meet national needs. For today's naval leaders, operating in these conditions requires leveraging all available resources at the right time and in the right place.

To this end, a "toolkit" available to the naval warfighter is knowledge management (KM) afloat. When properly employed, KM gives the warfighter a decisive advantage or knowledge edge, an ability to sharpen processes, maximize the use of information technology and exploit the knowledge, skills and experience of our people.

KM is no longer just a concept. Employing KM afloat presents challenges different than many other areas of the Navy enterprise. The Navy's Information Professional (IP) Officer Community is currently delivering officers to the fleet who are trained with critical knowledge sharing skills.

During a recent deployment in support of the global war on terrorism, the Harry S. Truman (CVN 75) Strike Group successfully employed these concepts and techniques to improve planning and situational awareness of the environment as the expeditionary strike force commander in the Arabian Gulf.

The Harry S. Truman (HST) Strike Group was responsible for a CSG and two ESGs. By coupling an operational focus with KM techniques, strike group processes, such as planning, information flow, watchstander turnover and mission transfer between units, were enhanced to be more agile and streamlined.

Enter the KMO

The knowledge management officer (KMO), an IP, provides a unique perspective and skill set to the strike group commander. To succeed, KMOs must be self-motivated and proactive. They must be well-versed in command, control, communications, computers and intelligence (C4I) systems, skilled in information management (IM) techniques, have operational experience in naval warfare, and be able to think strategically.

KMOs must have a working knowledge about change management theories and techniques and have the ability to understand process change implications that cross functional lines. Because each strike group is unique, each tour will be unique with new challenges. At all times, the KMO must keep the perspective of how each process or knowledge flow enables improved command and control or better decision-making. Initiatives they champion must provide obvious value to the watchstander, planner and deckplate Sailor.

Today's naval warfighter is faced with an onslaught of information. The perception is that more information equates directly to more knowledge. This is a fallacy. Tactical watchstanders are faced with information and task overload. Tactical action officers are monitoring a dozen or more chat rooms on U.S. and coalition networks, four or more voice nets, a half-dozen tactical displays, a handful of phones, message traffic and e-mail!

The rate of information exchange exceeds the ability of tactical watchstanders to recognize, process and integrate information to formulate actionable knowledge in the context of the tactical situation.

> *"Fourth generation warfare demands cooperative engagement and tactical agility. You cannot go it alone, and you must be highly responsive. To succeed, you must share knowledge and provide situational awareness in a concise and effective manner to be agile enough to respond to 21st century threats. Knowledge management is the core capability that enables the warfighting effectiveness and responsiveness of the flexible joint multi-national task forces."*
>
> *Rear Adm. Michael Tracy*
> *Commander, Expeditionary Strike Force Five*

This flood of information with current IM methods does not enhance the watchstander's knowledge inventory.

KM systematically brings together people, processes and technology to facilitate the exchange of operationally relevant information. We can improve this knowledge inventory through employment of KM techniques to refine processes, establish more effective business (watchstanding) rules, and innovate our use of existing technology to better frame and alert the watchstander to timely and relevant information.

New technologies to filter out "noise" and deliver operationally pertinent information are required to further enhance the situational awareness and understanding of the warfighter. FORCEnet initiatives, such as the Trident Warrior experimentation series must continue to focus on the dimension of enhancing situational awareness and understanding. In the near term, executing a robust KM afloat strategy will set us on the right course to manage information overload, spark innovation and grow the warfighter's knowledge inventory.

Step 1: Get Leadership "Buy-In"

To have successful KM and achieve the knowledge edge, the KMO's relationship with the commander, the chief of staff and the operations officer must be well-defined. Leadership buy-in for KMO-led initiatives is a prerequisite for success and leaders are the key to keeping the strike group staff operating at peak efficiency.

As these relationships mature, the KMO must also build relationships with warfare commanders, commanding officers and operations officers because afloat KM must serve all of their needs. The outcome and benefit of KM must be aligned with the commander's objectives and understood as providing value-added for all players.

The focus here is for the KMO to develop initiatives with tangible products useful in the tactical domain. *The bottom line is: The KMO must coach and deliver operationally relevant products to strike group leadership.*

Step 2: IM before KM

Let's face it, information management does not sound as fascinating as knowledge management. A lot of what today's KMOs must do is really IM and not KM. The tendency for the inexperienced KMO and eager-for-results commander is to move directly to a KM initiative and discount the need to address information management issues.

Vision

The Navy will employ Knowledge Management to achieve Knowledge Dominance, resulting in:

– A warfighting force empowered with accurate, timely and relevant information
– A culture of innovation, knowledge sharing and organizational learning
– Projection of decisive warfighting capability across naval, joint and coalition domains

Fleet Knowledge Management 2003 Working Group Tactical Challenges

IM involves working in the trenches and spending time identifying seemingly minor solutions to real problems faced by staff and operators alike. The Navy and Department of Defense (DoD) have fielded a collection of information technology (IT) with the goal of improving efficiency, speeding information transfer and saving manpower. KMOs must partner with the ship's IT department and be champions for more effective and innovative use of the IT tools employed by the strike group to find ways to promote proper IM.

By establishing policy through IM operation tasks (OPTASKs) and by identifying timesaving techniques, the KMO can make a near-term and positive impact on strike group operations. A simple thing, such as disciplined management of file sizes or alternate file formats for information posted to strike group Collaboration at Sea (CAS) systems can make a major difference to the officers and crew of a bandwidth-limited destroyer or frigate.

This may not be a big deal to shore staffs, but afloat it can be the difference between sharing information and possibly having no information at all.

Finding new ways to share information is another IM technique that enhances operations. The commander's ability to share information with staff so they can better understand the commander's intentions and improve situational awareness is the articulation of KM afloat.

This shared situational awareness allows better synergy in making time-critical decisions and assists in eliminating the knowledge seams between decision makers who are not collocated.

The Harry S. Truman Strike Group KMO was empowered to be the "IM cop" and was able to enforce the information management plan. The IM plan emphasized policies on the approved techniques and procedures for the information technologies common within the strike group.

The IM plan must be more than mere words on paper. The KMO must market the advantages to the staff, key stakeholders and other information brokers, so they understand the benefits of proper IM. With hard work early in the process, the KMO can build self-sustaining IM processes and procedures, which will later become a matter of efficient routine.

Step 3: Maximize Knowledge Flow

Once the IM house is in order, the KMO should focus on evaluating strike group processes and confirming they are well aligned. An early quick-win to improve the effectiveness of operational planning is to examine the strike group battle rhythm. Often there are overlaps or gaps in battle rhythm events.

By focusing on the strategic perspective, the KMO can recommend battle rhythm refinements that increase the effectiveness of the planning cycle and mission execution. This proved to be quite effective for the HST Strike Group for reducing redundant meetings and reports, which were not in sync with the operational tempo.

Organizational alignment is another area where the KMO can improve knowledge flow within the strike group. Identifying proper roles for liaison officers or alignment of staff personnel can be critical.

> ***"Second patrol under the auspices of CTF 50/152 was characterized by more clear and smoothly directed tasking … lines of communications on CENTRIXS are revealed and more clear," said the commanding officer of the Royal Netherlands Navy frigate, HNLMS Tjerk Hiddes.***

North Atlantic Ocean (July 12, 2004) - The USS La Salle (AGF 3), the Dutch frigate HNLMS Jacob Van Heemskerck (F812) and submarine tender USS Emory S. Land (AS 39) steamed together in the Atlantic Ocean while participating in Majestic Eagle 2004. The Majestic Eagle, a multinational exercise, was conducted off the coast of Morocco. The exercise demonstrated the combined force capabilities and quick response times of the participating naval, air, undersea and surface warfare groups. The NATO-led exercise included the United Kingdom, Morocco, France, Italy, Portugal, Spain and Turkey. U.S. Navy photo by Photographer's Mate Airman Josh Kinter.

The KMO can often suggest a plan for improvement by interviewing those involved in a process and identifying the corporate knowledge in an organization.

In some cases, a formal organizational change might not be the right answer. A community of practice (COP), a collaborative group with a common purpose or goal, can be established and with routine activity can improve knowledge sharing by honing processes which would not have been possible without combined networking.

An example of a COP used during our deployment was bringing together a group of coalition operators and technicians to solve the issue of regional nation communications between the United States and Gulf Cooperative Council nations. The end results were secure communications and standard operating procedures between navies and supporting shore facilities.

The KMO observes many best practices throughout the strike group. A key element of success is for the KMO to identify, collect, measure and market these best practices. Best practices should then be shared and employed within the strike group to improve overall knowledge flow and process efficiency. They should also be passed along to relieving strike groups and training strike groups. Sharing innovation and KM initiatives maximizes the return for warfare commanders and strike group leadership.

Step 4: The Coalition Domain

KM is equally important in coalition operations. Our allies and coalition partners are a critical piece in fighting the global war on terrorism and providing for our mutual defense. By applying the same IM and KM principles developed during the Fleet Readiness Training Plan workup cycle to the coalition arena, the HST Strike Group was able to effectively and efficiently relay the commander's intentions and scheme of maneuver to our coalition partners.

Until recently the U.S. Naval Forces Central Command (NAVCENT) maritime infrastructure did not support a cohesive information sharing environment. There were multiple systems in place, but nothing that reached all the maritime partners. The Combined Enterprise Regional Information Exchange System (CENTRIXS) is now that medium. It is an essential command and control system for maritime operations in the 5th Fleet area of operations. It was fielded as the primary method of planning, collaborating and controlling all coalition and U.S. forces.

Ensuring that our coalition partners have visibility of the commander's intentions, maritime tasking, scheme of maneuver and conditions within the operational environment is crucial to the success of our coalition. The new CENTRIXS enclave, the Combined Naval Forces U.S. Central Command (CNFC), contains similar collaborative tools employed with SIPRNET.

By using best practices from the SIPRNET environment, the HST Strike Group was able to quickly improve the processes and procedures in the coalition domain. A new coalition IM plan was drafted, which proved instrumental in setting responsibilities for content management, content input and established a level of expectation management. Redundant CAS databases were consolidated and routinely refreshed.

The results were improved information sharing and situational awareness among the operating forces. Many operations would not have been as successful without the use of the new tools because they greatly improved command and control.

Several success stories in this enclave include the use of CNFC chat to collaborate with Australian assets during a tense boarding operation. Pakistani and Italian liaison officers acknowledged they easily found needed information in a central repository on the CTF 50/152 CNFC Web site upon arrival in theater. With this type of cooperation between the coalition partners, true information sharing is enabled.

Step 5: Put Corporate Memory to Work

After meeting the IM and baseline KM challenges head on, systematic processes must be put in place for corporate memory to be kept alive and prosper.

Corporate memory is the collective knowledge base of the organization. It is inherent not only in the instructions, briefs and other documents of the organization, the explicit knowledge, but also in the unstructured or tacit knowledge resident

The KMO's Task List

√ Construct relationships and develop initiatives with tangible products useful to the tactical domain

√ Establish information management policy through IM OPTASKs and other timesaving techniques

√ Build a routine and reliable conduit for collaboration; exploit the strengths of coalition partners

√ Make a best practices repository based on explicit knowledge derived from past and present activities

√ Fill knowledge gaps in the organization

Atlantic Ocean (July 18, 2004) - USS Harry S. Truman (CVN 75) Carrier Strike Group (HSTCSG) deployed Oct. 13, 2004, in support of the global war on terrorism. Commanded by Rear Adm. Michael Tracy, commander, Carrier Strike Group 10, HSTCSG included the Norfolk-based aircraft carrier Harry S. Truman with its embarked air wing, Carrier Air Wing (CVW) 3, the Norfolk-based guided-missile cruiser USS Monterey (CG 61), the Norfolk-based guided-missile destroyers USS Barry (DDG 52) and USS Mason (DDG 87), the Groton, Conn.-based fast-attack submarine USS Albuquerque (SSN 706) and the combat logistics ship USNS Arctic (T-AOE 8) from Naval Weapons Station Earle, N.J. U.S. Navy photo by Photographer's Mate Airman Ryan O'Connor.

within the individuals who make up the organization.

Strike group corporate memory today is cyclical and tied to the influx and outflow of personnel in leadership and other key warfare billets. In many cases, individuals within the strike group must relearn lessons their predecessors learned in the previous deployment cycle. What is missing is the bridge between the corporate knowledge of the previous deployment cycle and the next.

The ability to keep the knowledge level high is a requirement during the FRP sustainment period. The KMO has a critical role in designing and building that sustainment plan. Simple things such as creating a knowledge repository for turnover or interviewing individuals with recent strike group operational experience are some methods to maintain corporate knowledge.

When knowledge is captured, it must be relayed to those who need it. It should also be stored for easy recovery and knowledge mining. Organizing the collection of information for easy retrieval by watchstanders or staff is necessary for maintaining and sharing corporate knowledge.

Building a best practices repository focused on strike group exercises and operations is also beneficial. Along with the tactical training community, KMOs afloat must work to build a sustainable network between strike groups to share, enhance and improve best practices across the fleet.

There is much work to do in this area and with the increased FRP readiness plateau, it will be increasingly important for strike groups to share, maintain and enhance corporate memory.

Recommendations

A recommendation is for the Naval Network Warfare Command (NETWARCOM) to serve as the fleet KM lead and consolidate a KM best practices repository, tailored toward the afloat environment. This repository should be managed by someone in the tactical training cycle to be shared with all strike groups as they work up for deployments.

Another recommendation is to designate the commanders of the Strike Force Training Atlantic and Pacific commands as the keepers of afloat tactical best practices given their role in the FRP and tactical development of the strike groups.

Next Steps: Knowledge Fusion

As the Navy proceeds along the transformation path toward the Sea Power 21 vision, KM afloat competencies become even more critical. Realizing the knowledge edge will be the differentiator between our Navy and any adversary.

With increasing competition for resources to meet all the missions for ships at sea, leadership must have the right knowledge to determine where and when to place platforms and sensors to destabilize an adversary's center of gravity.

> **"KM is the responsibility of all levels of management, and managers must be courageous enough to look for the knowledge edge."**

KM facilitates manpower efficiencies, and it is needed if the Navy is to succeed in transformation and to achieve future capabilities, such as FORCEnet. The assignment of Information Professionals as staff knowledge managers is an excellent start and must be fully exploited. However, it is important to note that KM is the responsibility of all levels of management, and managers must be courageous enough to look for the knowledge edge.

Cmdr. Hearne is the commander, Carrier Strike Group Ten (CSG-10) knowledge manager and a former member of Task Force Web.

Lt. Cmdr. Mills is the CSG-10 Flag communications officer and former NETWARCOM knowledge manager and director of FORCEnet Innovation & Experimentation. Hearne and Mills are Information Professional officers. CHIPS

Navy Wireless Networks – FIPS 140-2 or Bust!

... a vulnerabllity assumed by one is shared by all ...

By Commander John MacMichael

Background

Home and corporate users in ever-increasing numbers are using wireless networks based on the 802.11b, 802.11a, 802.11g and the emerging 802.11x/i/n standards. In March 2003, the Gartner Group reported that there were 4.2 million frequent users of wireless local area networks (LAN) and predicted that number to grow to 31.7 million users by 2007. This same group further indicated that approximately 30 percent of all companies with a computer network have some kind of wireless network, either official or rogue.

Popular small office, home office (SOHO) equipment, such as the Linksys WRT54G Netgear WGR614 and D-Link DI-24 have begun to appear on Navy networks as rogue access points (AP). As consumers of SOHO equipment have become more familiar with wireless networking, the demand for these products has increased while the price for entry-level equipment has dropped. However, this equipment does not meet the Department of Defense (DoD) or Naval Network Warfare Command (NETWARCOM) requirements for wireless usage because it does not provide adequate access control or encryption at link layer 2.

Navy and Defense Network Security Policy

In July 2004, the NETWARCOM Network Security Division (NNWC NSD) released two messages that imposed a "wireless moratorium" for both afloat and ashore network infrastructure: ALCOM 038-04 (DTG 021619Z Jul 04) and ALCOM 046-04 (DTG 191834Z Jul 04). This moratorium included but was not limited to "commercial wireless technologies and their derivatives, as standardized in IEEE standards 802.11, 802.15 and 802.16 commercial wireless devices, services and technologies and voice and data capabilities that operate either as part of the Navy enterprise network or stand-alone systems."

While these messages imposed a moratorium, they also delineated a waiver process for identifying and mitigating the risks associated with wireless networks that were deployed under an Interim Authority to Operate (IATO) or ATO or operated without official approval by NNWC NSD. To be considered for a waiver, the information assurance manager for each network was directed to register the network and provide specific technical details to NNWC NSD no later than Aug. 30, 2004.

Upon receiving registration information, NNWC NSD reviewed each wireless network's specifications and System Security Authorization Agreement (SSAA) to determine whether the system met the requirements of DoD Directive 8100.2, Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GIG). Each wireless network considered for a waiver had to comply with DoDD 8100.2 and implement access control methods to be considered for a waiver. The registration and waiver process remain in effect at this time.

Federal Information Processing Standards

The information assurance triad is composed of authentication, integrity and confidentiality. DoDD 8100.2 addresses the confidentiality requirement of the IA triad by mandating encryption. The requirements of DoDD 8100.2 are straightforward and stringent, "Encryption of unclassified data for transmission to and from wireless devices is required …. At a minimum, data encryption must be implemented end-to-end over an assured channel and shall be validated under the Cryptographic Module Validation Program (CMVP) as meeting requirements per Federal Information Processing Standards (FIPS) Publication (PUB) 140-2." Complete information about FIPS 140-2 is available at http://csrc.nist.gov/wireless/S05_NIST-tk2.pdf.

While not specifically delineated in DoDD 8100.2 or the NNWC moratorium, NNWC directed that FIPS 140-2 compliance will be at layer 2. Layer 2, or the data link layer, defines physical addressing and network topology and directs the functional and procedural means to transfer data between network entities of the Open Systems Interconnection (OSI) model. This is an important distinction because some wireless mechanisms may be FIPS 140-2 compliant at network layer 3, which provides the routing, flow control, segmentation/desegmentation and error control functions required to transmit information between networks.

Encryption at layer 2 ensures that all of the packet contents, except the data link header, are encrypted. This ensures that data and routing information are encrypted and protects access points and the computer's Internet Protocol (IP) address, as well as the media access control (MAC) address. Encryption at layer 2 can be used to ensure access control, prevent attacks on data privacy ("sniffing" of layer 2 header information) and thwart spoofing attacks.

FIPS 140-2

The National Institute of Standards and Technology (NIST) published FIPS 140-2, Security Requirements for Cryptographic Modules, May 25, 2001. This standard describes the requirements that hardware and software products should meet for sensitive but unclassified (SBU) use. FIPS 140-2 compliance is mandatory for federal agencies and has become the de facto standard for industry.

FIPS 140-2 addresses the confidentiality and integrity pieces of the information assurance triad, but it does not address access control. There is no single standard for wireless authentication and access control; however, NNWC has deemed products such as TACACS+, RADIUS and Kerberos acceptable for controlling authentication, authorization and accounting (AAA).

It is the responsibility of the vendor to achieve certification of its cryptographic product. Certification of a product to this standard is a strong selling point within both the federal government and industry. On average, the certification process takes 15 months and costs approximately $200,000 for laboratory testing, mandatory certification documentation and follow-on changes required to meet the FIPS 140-2 standard.

The CMVP is jointly managed by U.S. federal agency, NIST, and Canada's national cryptology agency, the Communications Security Establishment (CSE). Vendors contract with one of nine independent laboratory-testing facilities. Laboratory personnel review and test products and submit validated FIPS 140-2 candidates to NIST and the CSE for certification. A graphic representation of this process is shown in Figure 1.

Once certified, the certification applies only to the version of the process that was originally submitted, all product updates must be revalidated. It is important to note that a vendor may submit an entire product or a cryptologic module for testing. A vendor may implement a FIPS 140-2 module into a product that operates in both FIPS 140-2 compliant and non-compliant modes. Information assurance managers must ensure that they understand the method of implementation.

Similarly, vendors may purchase the rights to incorporate a FIPS 140-2 certified module into their products. These products may then be labeled "FIPS inside" to indicate that a FIPS validated component has been incorporated. NIST maintains a list of approved cryptologic modules at http://csrc.nist.gov/cryptval/140-1/1401val.htm/. Products that are currently undergoing evaluation are listed on a prevalidation list at http://csrc.nist.gov/cryptval/preval.htm/.

Compliance

Navywide, relatively few wireless systems were reported to NNWC, so it is likely that not all wireless networks were reported. In March 2005, the NNWC C4I and Network Security Division jointly directed the Fleet Information Warfare Center (FIWC) Navy Red Team *(see the Red Team text box on the next page)* to complete a search for 802.11 wireless networks onboard selected Navy installations. In April 2005, the Naval Computer Incident Response Team (NAVCIRT) directed a similar action. NAVCIRT went one step further and directed the localization and identification of unapproved wireless networks operating onboard Navy installations.

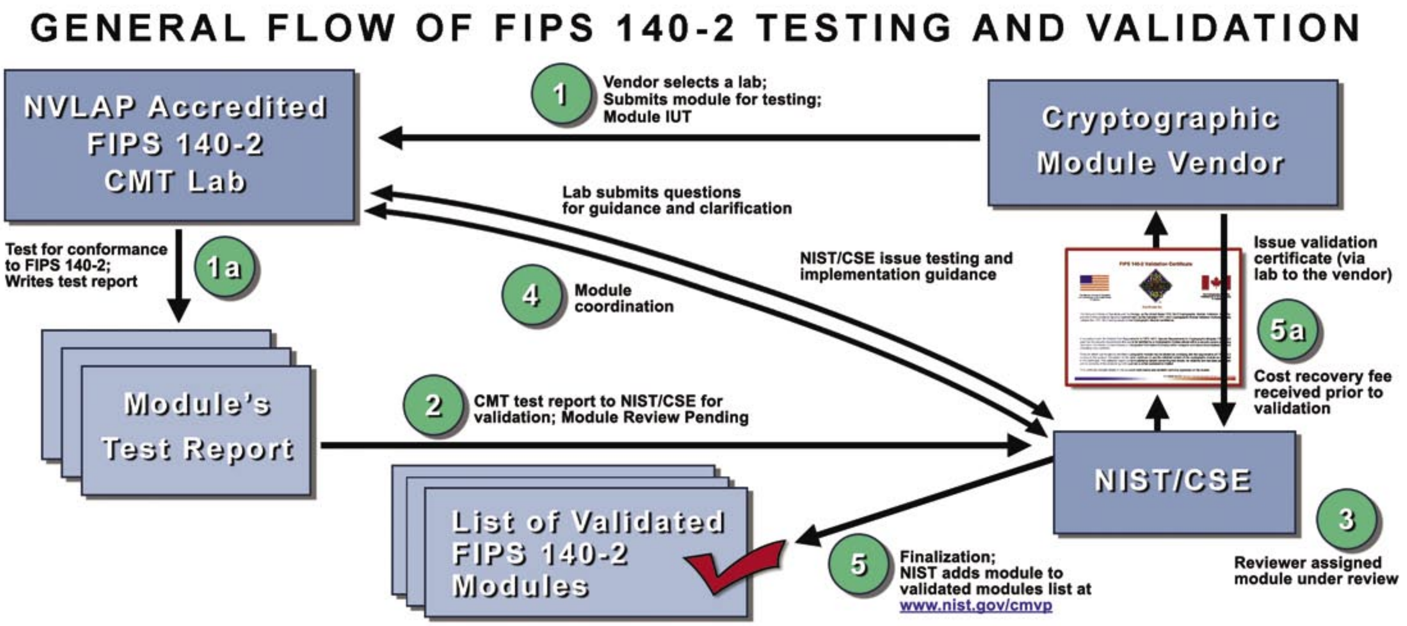
To comply with personal privacy and Title 10 concerns, and in keeping with the detection and localization effort, the Navy Red Team configured wireless equipment to capture and retain only the header information from wireless IEEE 802.11 data packets. These actions ensured that data of an attributable nature were not collected. The results of these actions are classified; however, the Navy Red Team specifically investigated any network operating with an encryption scheme that was not FIPS 140-2 certified.

Examples of unapproved encryption schemes are Wired Equivalent Privacy (WEP) and wireless fidelity (Wi-Fi) Protected Access Pre-Shared Key (WPA-PSK) encryption. This is the encryption method generally used with SOHO equipment. Neither of these encryption schemes are FIPS 140-2 certified; consequently, both may be attacked though various methods.

WEP and WPA

WEP was the original encryption scheme designed for wireless networks. WPA-PSK is an improved standard that addresses known WEP vulnerabilities. Temporal Key Integrity Protocol (TKIP) is the wireless security encryption mechanism within WPA-

Figure 1. A graphic representation of the FIPS certification process.


GENERAL FLOW OF FIPS 140-2 TESTING AND VALIDATION
NVLAP Accredited FIPS 140-2 CMT Lab
1
Vendor selects a lab; Submits module for testing; Module IUT
Cryptographic Module Vendor
Lab submits questions for guidance and clarification
Test for conformance to FIPS 140-2; Writes test report
1a
4
Module coordination
NIST/CSE issue testing and implementation guidance
Issue validation certificate (via lab to the vendor)
5a
Cost recovery fee received prior to validation
Module's Test Report
2
CMT test report to NIST/CSE for validation; Module Review Pending
NIST/CSE
3
Reviewer assigned module under review
List of Validated FIPS 140-2 Modules
5
Finalization; NIST adds module to validated modules list at www.nist.gov/cmvp

PSK that removes the predictability of WEP initialization vectors (IVs) in the encryption scheme. Collectively, this is known as WPA-PSK (TKIP).

An information assurance manager might wonder how serious a security risk is posed by using WEP or WPA-PSK on a Navy network. In 2001, when Scott Fluher, Itsik Mantin and Adi Shamir published "Weaknesses in the Key Scheduling Algorithm of RC4," and the Shmoo Group released the beta version of Airsnort, compromising a WEP key was a daunting task. A would-be attacker required in-depth Linux knowledge to patch and install unsupported wireless drivers, compile programs, capture a substantial amount of wireless network data, and use the poorly documented tools available.

Under the WEP 128-bit encryption scheme, 16 million keys can be generated; roughly 9,000 of these are weak (also known as interesting) due to the implementation of the IV. By capturing approximately 5 million data packets, Airsnort could "guess" most WEP keys. This number would statistically ensure collection of approximately 4,000 interesting IVs. The process of breaking WEP was time consuming because collection of these packets was dependent on network utilization. Collection time varied with wireless data network usage. However, a network with few users and moderate network usage might take two weeks of packet capture before the WEP key could be obtained.

These statistically weak or interesting IVs received wide recognition within the industry and, as a result, most vendors made changes to their WEP firmware and software implementations which filtered or removed interesting IVs. Older versions of Airsnort and other tools that attacked WEP by examining interesting IVs became unusable against most wireless equipment produced after 2002.

But even with vendor implementation changes, WEP and WPA continue to be serious security risks. Advances in the art of cracking WEP and WPA networks have made arguments for using these encryption schemes in Navy networks indefensible. The greatest advancement has been the proliferation of well-documented tools accompanied by Internet tutorials that explain the process of compiling and using the unsupported drivers required to operate wireless equipment in "promiscuous" or "monitor" mode. This mode allows an attacker to passively capture network wireless traffic and then reinject traffic into a WEP or WPA protected network.

An average Linux user can follow instructions that will guide him or her in the compilation and installation of the drivers, libraries and tools. As an alternative, an attacker may download and install precompiled components using a Linux distribution compatible with the Red Hat Package Manager (RPM) or Debian Advanced Package Tool (apt-get). Additionally, many tools that formerly ran on Linux operating systems have been ported to the Microsoft Windows operating system.

WPA-PSK is Unsuitable for Navy Networks

In 2004, a new WEP statistical cryptanalysis attack (the exploitation of weak keys) was released by Korek. While still based on the Weaknesses in the Key Scheduling Algorithm of RC4, the Korek Attack removed the requirement for the collection of interesting IVs. This attack has been coded into several tools, most notably Aircrack, WepLab and the newest version of Airsnort. Each has tool functions that slightly differ, but each tool requires far fewer packets to break WEP.

Computer Network Defense Red Team

Red Team refers to a group of subject-matter experts tasked with playing the role of the enemy in training exercises. The purpose of Red teaming is twofold: (1) It identifies weaknesses in the defender's perimeter that would otherwise be overlooked; and (2) It gives the defenders valuable training in detecting and reacting to attacks. Properly conducted Red Team operations can identify planning shortfalls, deviations from doctrine and missed opportunities. These operations provide independent data for use in risk-management decision making. This concept has been used by the military for decades primarily in wargaming. In industry, it is often called a "peer review."

The Computer Network Defense (CND) Red Team located at the Fleet Information Warfare Center (FIWC) was created in 1996 and provides operational and exercise support to commands to improve their ability to fend off malicious computer activity. The Red Team offers many services to all levels of the Navy, from the component commander to individual commands. The FIWC Red Team is a key participant in Navy Integrated Vulnerability Assessments (NIVA). Although the Red Team is only concerned with network security testing, a typical NIVA visit includes assessments performed by a variety of teams on a host of topics such as disaster preparedness and terrorism prevention.

Navy Marine Corps Intranet (NMCI) Security Service Level Agreement (SLA) tests are performed by the Red Team under the direction of the NMCI director to ensure that the NMCI meets the security standards set forth in the contract with EDS. SLA tests are highly standardized to ensure that the results from different installations can be meaningfully compared.

The FIWC Red Team performs test and evaluation under the direction of the Navy's Operational Test and Evaluation Force (COMOPTEVFOR) and the Space and Naval Warfare Systems Command (SPAWAR) on fleet systems prior to their inception. The remainder of Red Team activities can be collectively described as special projects. Any Navy command may request FIWC assistance in testing the security of its network. This training is tailored to the needs of the individual command. Special projects can include any or all of the following elements: open source research, port scanning, remote attacks, social engineering, physical intrusion, insider attacks, and malware use and detection.

The requirement for the statistical attack is generally in the range of 500,000 to 1 million unique, as opposed to weak, IVs. While this represents a significantly smaller number of packets than in the past, network usage might dictate that a substantial amount of time before collection of the requisite number of packets had been completed. An uninformed information assurance manager might believe that security on a network with a relatively low volume of traffic may be ensured by regularly changing the WEP key before a large number of unique IVs are generated.

Aireplay negates time as a factor by allowing an attacker to inject captured encrypted packets into a wireless network. By injecting captured Address Resolution Protocol (ARP) packets, the attacker may force a reply with an unique IV. Aireplay can force the AP to generate thousands of packets per minute and provide the attacker with the requisite number of IV packets to crack WEP in a relatively short period of time.

Kismet may be the best tool for promiscuously capturing wireless network traffic. Developed by Mike "Dragorn" Kershaw, this free tool began as a wireless discovery tool and has evolved into an 802.11, layer 2, wireless network detector, sniffer and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring mode (rfmon) and can sniff 802.11b, 802.11a and 802.11g traffic. Kismet can specifically log the Transmission Control Protocol (TCP) and IV packet data required to break WEP or WPA, and it can allow data packets to be reinjected into WEP and WPA networks.

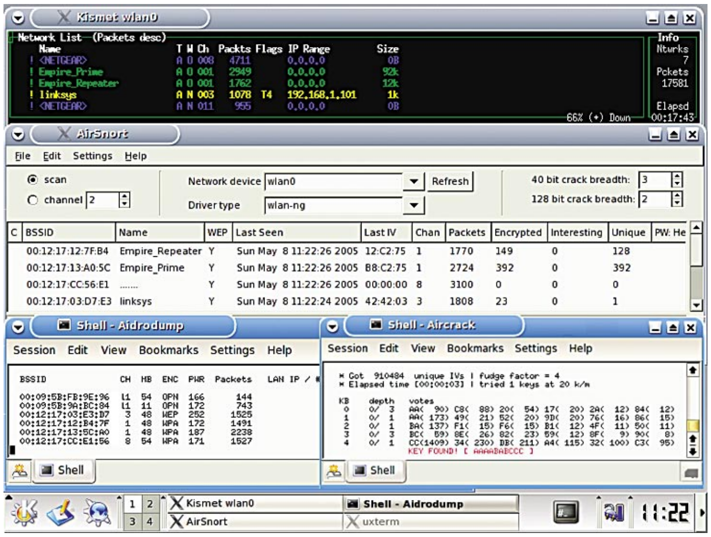
Just as filtering interesting IVs in WEP did not deliver a more secure system, WPA-PSK is also not the answer to WEP. Both WEP and WPA-PSK use a key (passphrase) that is susceptible to offline brute-force dictionary attacks. The WPA-PSK key can be between eight and 63 bytes, and SOHO implementations allow only a single PSK to be used on each wireless network. The tools WEPCrack and "dwepcrack" are capable of offline brute forcing weak WEP passwords.

Robert Moskowitz's article, "Weakness in Passphrase Choice in WPA Interface," describes a theoretical attack on WPA passwords. The tools WPA-psk-bf, CoWPAtty and WEP Crack are implementations of this attack and have demonstrated the ability to break WPA-PSK keys that are 20 characters or fewer. The Aircrack tool suite operates in an active or passive mode to gather the data required to launch these attacks. In passive mode, the Aircrack tools capture the four-packet authentication handshake between an AP and client. The handshake is then processed through a WPA breaking tool for an offline brute-force attack. If the attacker has not captured the handshake, the Aircrack tools active mode will force a disassociation and reassociation.

Threat Tools Simplified

To use the aforementioned tools, average knowledge of Linux is required to patch and install unsupported wireless drivers, compile Unix-based tools, capture network traffic and execute WEP and WPA-PSK exploits. Even with the increase in documentation and ease of compiling drivers and tools, these tasks were hurdles that had to be overcome by a novice attacker. But these barriers have all but been removed with the advent of the live Linux distribution based on the Knoppix Linux distribution. These distributions are free and distributed as an ISO. An ISO is a file that contains the complete image of a disc. These files are often used when transferring CD-ROM images over the Internet. The user simply inserts a disc into a system and powers the system on. The system will boot from the disc into a full-fledged Linux operating system.

Knoppix variants such as Auditor, Knoppix-STD (Security Tools Distribution) and Whoppix have precompiled drivers, software and cryptologic libraries that allow even a novice Linux user to launch sophisticated attacks against wired or wireless networks. Figure 2 is a screen capture from an Auditor Linux distribution.



```
Network List (Packets desc)                                  Info
   Name                   T W Ch  Packts Flags IP Range       Size   Nturks
 ! <NETGEAR>              A O 008  4711        0.0.0.0         0B        7
 ! Empire_Prime           A O 001  2949        0.0.0.0        92k    Pckets
 ! Empire_Repeater        A O 001  1762        0.0.0.0        12k     17581
 ! linksys                A N 003  1078  T4    192.168.1.101   1k
 ! <NETGEAR>              A N 011   955        0.0.0.0         0B    Elapsd
                                                   66% (+) Down   00:17:43
```

● scan
○ channel 2

Network device: wlan0
Driver type: wlan-ng

40 bit crack breadth: 3
128 bit crack breadth: 2

C	BSSID	Name	WEP	Last Seen	Last IV	Chan	Packets	Encrypted	Interesting	Unique	PW: He
	00:12:17:12:7F:B4	Empire_Repeater	Y	Sun May 8 11:22:26 2005	12:C2:75	1	1770	149	0	128	
	00:12:17:13:A0:5C	Empire_Prime	Y	Sun May 8 11:22:26 2005	B8:C2:75	1	2724	392	0	392	
	00:12:17:CC:56:E1	....	Y	Sun May 8 11:22:26 2005	00:00:00	8	3100	0	0	0	
	00:12:17:03:D7:E3	linksys	Y	Sun May 8 11:22:24 2005	42:42:03	3	1808	23	0	1	

```
 BSSID              CH  MB  ENC  PWR  Packets   LAN IP / #

 00:09:5B:FB:9E:96  11  54  OPN  166      144
 00:09:5B:9A:BC:84  11  11  OPN  172      743
 00:12:17:03:E3:D7   3  48  WEP  252     1525
 00:12:17:12:B4:7F   1  48  WPA  172     1491
 00:12:17:13:5C:A0   1  48  WPA  187     2238
 00:12:17:CC:E1:56   8  54  WPA  171     1527
```

```
 * Got  910484  unique IVs | fudge factor = 4
 * Elapsed time [00:00:03] | tried 1 keys at 20 k/m

 KB    depth   votes
  0    0/  3   AA(  90) C8(  88) 20(  54) 17(  20) 2A(  12) 84(  12)
  1    0/  1   AA( 173) 49(  21) 52(  20) 9D(  20) 76(  16) 86(  15)
  2    0/  1   BA( 137) F1(  15) F6(  15) B1(  12) 4F(  11) 50(  11)
  3    0/  3   BC(  59) 8E(  26) 82(  23) 59(  12) 8F(   9) 90(   8)
  4    0/  1   CC(1409) 34( 230) DB( 211) A4( 115) 32( 100) C3(  95)
               KEY FOUND! [ AAAABABCCC ]
```

Figure 2. A screen capture from an Auditor Linux distribution. The tools Kismet, Airsnort, Airodump and Aircrack are shown running in a test environment.

The tools, Kismet, Airsnort, Airodump and Aircrack, are shown running in a test environment. An experienced Linux user could spend an hour or more reading the documentation, compiling and configuring network drivers, libraries and tools and have the ability to exploit a wireless network. I was able to download the Auditor ISO image, boot to the Auditor Linux distribution and run each of these tools within 20 minutes.

It should be apparent that powerful network attack tools to compromise WEP or WPA-PSK are freely available to anyone with an Internet connection and the ability to follow well-defined instructions. It should also be apparent that the use of wireless equipment that does not meet the requirements of FIPS 140-2, does not implement access control and has not been approved by NNWC NSD, places the entirety of Navy networks and the GIG at risk. Unapproved equipment may also become a vector for an attacker to compromise the network of a command.

The mantra, *a vulnerability assumed by one is shared by all*, definitely applies to wireless networks. An attacker could use insecure and unapproved equipment as a vector into other Navy networks or as a jumping off point into public or commercial networks, creating the false appearance that Navy personnel had launched the attack. Both NNWC and NAVCIRT are actively using the FIWC Navy Red Team to detect, localize and remove unapproved wireless networks.

Don't compromise your command or the Navy with unauthorized wireless equipment.

Cmdr. MacMichael is the Fleet Information Warfare Center (FIWC) deputy operations officer and an Information Professional (IP) officer with a master's degree in information systems technology from the Naval Postgraduate School. He has the following certifications: Certified Information System Security Professional (CISSP), GIAC Security Essentials Certification (GSEC) and Certified Wireless Network Administrator (CWNA). CHIPS

NAVCIRT Receives SAS Award for Network Defense

By Journalist 2nd Class (SW/AW) Jennifer Zingalie, Naval Network Warfare Command Public Affairs

Information technology gives the warfighter options beyond fighting the enemy on the seas, above the seas or under the seas …

The Navy Computer Incident Response Team (NAVCIRT) received the SAS Enterprise Intelligence Award May 11 in Washington, D.C. The award recognizes achievements in solutions to computer network defense through software application, and illustrates the dedication of NAVCIRT's watch team in preventing virus attacks, intrusions and disruptions to the network that could affect and degrade Navy operations.

SAS, a company that creates business software for analyzing large amounts of data, recognized the strategic vision and collaborative efforts of the NAVCIRT in applying business intelligence to enhance organizational performance.

According to Capt. Steven Carder, NAVCIRT commanding officer, the application of information technology gives the warfighter options beyond fighting the enemy on the seas, above the seas or under the seas.

"We are taking the fight to the enemy in the cyber domain. The tools we use allow us to see where a problem is geographically and, in turn, allow us the capability to provide defense-in-depth and support mission fulfillment at the right time."

"The Department of Defense runs the largest computer network in the world, and our job is to defend the Navy portion of the network. Information is a critical commodity, and it is essential for all the network components to work together to make us an effective warfighting force because any compromise of those components degrades our warfighting capability," said Carder.

"The potential for cyber warfare is very real, and we deal with thousands of probes against DoD perimeter defenses every day," said Carder. "We know that we have enemies with capabilities to wage war in an information domain."

By using the MOBIUS application, watchstanders can provide situational metrics on the status of the network. The software stores cyber security data for historical analysis, trending, data visualization, reporting and event-correlation capabilities that deliver real intelligence on potential threats. The system is based on SAS Intelligence Platform components that include SAS Enterprise BI Server, SAS ETL Server and SAS Intelligence Storage.

MOBIUS is named after the mathematician August Ferdinand Mobius, who devised a two-dimensional surface with only one side.

"The MOBIUS application helps us look for anomalies or indications of warnings of a computer network attack," said Jim Granger, NAVCIRT technical director.

"We look for probing activities, precursors of someone doing reconnaissance for a possible later attack. We can use this information to stop attacks in progress or predict future attacks, and ideally stop them before they start," Granger said.

"In this net-centric era it is important that those in network security are proactive instead of reactive. That is just what we are," said Granger. "We are proud to have tools that can enable us to better do our job monitoring computer networks. We are able to make more informed decisions that drive us forward."

As Granger puts it, NAVCIRT watchstanders are a lot like firefighters. In the old days, a fire in a building would cause one main alarm to sound, but once the fire was put out the entire building would have to be searched to find the source. Eventually, it was decided there needed to be dozens of detectors or sensors everywhere. With these in place, fires were easier to pinpoint, and potential fires could be averted.

Cryptologic Technician (networks) 1st Class Dan Ricci, an assistant watch officer at NAVCIRT, said that "fire prevention" happens every day. "Network security has been happening for awhile; however, there were only a certain amount of sensors placed around the world. Now we have sensors everywhere, and we are able to look at a lot of information at one time," said Ricci.

"We have people who analyze this data. Before, they would have to eyeball long lists of data looking for trends and identifying probes of possible computer threats," said Ricci.

"Now we have software known as MOBIUS that allows us to do our job more efficiently because it gathers similar information and patterns or trends for us; it does the leg work. This allows the analyst more time to look at the data in-depth and respond more rapidly to any threats."

NAVCIRT's cyber warriors are always at general quarters keeping the lines of communication open. "One of the greatest benefits of MOBIUS is that it makes information readily available to the warfighter," said Granger. CHIPS

Preventing the Compromise of Classified Data on DON IT Systems and Networks

By Jennifer Korenblatt

Introduction

This article discusses the responsibilities of Department of the Navy (DON) information technology (IT) users for protecting classified information on DON IT systems and networks. Classified data exist in both a physical and electronic state. While physical protection of classified information is critical regardless of media, this article primarily focuses on protecting classified data residing on IT systems.

Classified information is so designated by the U.S. government based on the amount of harm to national security that would occur if unauthorized individuals obtain it. There are three levels of classified information:

CONFIDENTIAL – *some damage to national security would occur*
SECRET – *serious damage to national security would occur*
TOP SECRET – *exceptionally grave damage to national security would occur as defined by the Department of Defense (DoD) 5220.22-M, National Industrial Security Program Operating Manual.*

To understand the importance of information security, it is important to understand several key security definitions. Information security refers to the protection of information and information systems from "unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide" integrity, confidentiality and availability of the information as defined by the Federal Information Security Management Act (FISMA) of 2002.

A security compromise refers to the unauthorized disclosure of classified information to a person(s) who does not have a valid clearance, authorized access or a need-to-know. A compromise can occur when classified information is not properly controlled as defined in FISMA. Other terms often used for compromise are: classified information spillage, unauthorized disclosure and system contamination. A compromise can also occur if data of a higher classification is disclosed to a system or network only approved to process information at a lower classification level (i.e., top secret information disclosed onto a secret system, secret information disclosed onto a confidential system, etc.).

Information technology includes, but is not limited to, telephones (including cell phones), computers and workstations, information and communication systems, software, networks, pagers, fax machines, personal digital assistants (PDAs), Internet access and e-mail.

The Problem

The DON increasingly depends on IT to conduct mission functions. This dependence increases the DON's vulnerability to the mishandling of classified information on its systems and networks. The compromise of classified secret information onto unclassified systems and networks is a growing problem in the DON. A new Navy Marine Corps Intranet (NMCI) Contract Line Item Number (CLIN), NMCI CLIN 0046, "File Removal Service," issued Jan. 19, 2005, allows the NMCI vendor to charge commands for file removal service of each compromise of classified information on the NMCI.

Costs can be as high as $11,800 for just one compromise incident. The DON must prevent compromises to avoid significant costs and lost productivity. It can take up to three weeks to resolve a compromise incident, so each compromise affects the security of DoD and DON mission functions. DON users are the first line of defense for protecting information on DON networks and systems. However, one of the greatest threats to the information security posture of any system is the insider threat. So it is imperative for all DON IT system users to increase awareness of individual responsibility to safeguard classified information.

Compromise Incident Examples

How does a compromise of classified information occur? Consider the following scenarios.

Scenario: It is 1600 on Friday afternoon; your boss sends you a classified secret document via SIPRNET asking you to review it as soon as possible. With your mind on your dinner reservation you decide to save the document to a disc so you can work at home. You save the secret document on a disc in a classified secret computer, insert the disc into an unclassified computer, upload the document to your unclassified system and e-mail the document to your personal e-mail account.

Result: You have just compromised classified information, and the consequences will ruin more than your dinner plans. What happened? You processed secret information on an unclassified system and did not apply proper security controls to classified data. You e-mailed secret information over the NIPRNET, which is not an authorized network to process secret information. Sending secret information to an unclassified, personal e-mail account is the unauthorized dissemination of classified information via an unclassified e-mail (either within the body of the e-mail or as an attachment).

Clear text sent over the Internet is available for anyone to read. Sending DoD classified information over the Internet exposes the information to unofficial release to the public. A public media compromise is the unofficial release of DoD classified information to the public resulting in its unauthorized disclosure.

Prevent compromise by: (1) Marking and protecting media according to the security classification level of the data residing on the media per Secretary of the Navy Instruction (SECNAVINST)

5510.36, DON Information Security Program (ISP) Regulation and the Defense Information Systems Agency (DISA) Information Assurance Security Awareness Briefing; (2) Remembering that classified information should be afforded a level of control commensurate with its assigned security classification level; and (3) Never sending DoD classified information over the NIPRNET or Internet.

Scenario: You pick up a disc with messages from the data center. You are sure the disc contains only unclassified messages despite its being labeled as secret. You place the disc with a secret label into the disc drive of an unclassified system. Lo and behold, the disc contains a secret classified message, and you just uploaded it to an unclassified system.

Result: Uploading classified secret information onto an unclassified system causes a compromise of classified data. This incident occurred through improper handling of marked classified material. Prevent this compromise by observing security classification markings on media and protecting media accordingly.

Everyone's Responsibility

Every DON military, civilian and contractor employee has a responsibility to protect the availability, integrity and confidentiality of DON IT assets. While most security breaches are not deliberate, intentional misuse of classified information is a crime. The Computer Fraud and Abuse Act (CFAA) lists the crimes associated with actions such as gathering, transmitting or losing defense information and disclosure of classified information.

Computer crimes are serious, and the punishment for offenses ranges from fines to imprisonment for up to 20 years. While the majority of compromises of classified information are unintentional, the consequences remain serious. Authorized users can do the most damage to a system or network through mistakes and mishandling information. We must remain vigilant and use sound information assurance (IA) practices when using DON systems, and pay special attention to actions that involve use of the Internet and moving data between different security classification levels.

Training

In addition to federal law, DoD and DON policies require users of DoD information systems to receive IA training commensurate with their duties as a condition of system access. DON annual IA training is not only mandatory, but it is an opportunity to reinforce knowledge of sound security practices for safeguarding all classifications of information. The goal of the training is to make sure all DON personnel who use DON information systems know the risks associated with their day-to-day activities, their individual responsibilities to meet the requirements of laws, policies and procedures, and the best security practices to use to reduce risks.

Each command is responsible for providing IA awareness training and ensuring all personnel understand their responsibilities for safeguarding classified information. If you have not received this training, speak to your security manager immediately. Standardized IA awareness training is available to Navy users through Navy Knowledge Online at http://www.nko.navy.mil and Marine users through MarineNet at http://www.marinenet.usmc.mil. Training must be completed by Sept. 1, 2005, for all authorized DoD users.

Resources

- *Free information assurance training products are available upon request from the DoD IA Portal at http://iase.disa.mil/. The DoD IA Portal also has a link to the DISA Information Awareness Security Briefing.*

- *Computer Fraud and Abuse Act (CFAA) Title 18 PT1, Chap. 47 § 1030 (a)*

- *Defense Security Service (DSS), http://www.dss.mil*

- *Federal Information Security Management Act of 2002, available at http://www.csrc.nist.gov/policies/FISMA-final.pdf*

The following can be accessed from the Policy and Guidance tab of the DON CIO Web site at http://www.doncio.navy.mil

- *DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), January 1995*

- *DoDD 8500.1, Information Assurance (IA), Oct. 24,2002*

- *DoD Instruction (DoDI) 8500.2, Information Assurance (IA) Implementation, Feb. 6, 2003*

- *DoDD 8570.1, Information Assurance Training, Certification and Workforce Management, Aug. 15, 2004*

- *SECNAVINST 5510.36, Department of the Navy (DON) Information Security Program Regulation, March 17, 1999*

- *SECNAVINST 5239.3A, DON IA Policy, December 2004*

What To Do If Classified Data Is Compromised

Individuals who become aware of the loss or compromise of classified information must immediately notify their commanding officer or security manager of the incident. DON users who discover a compromise on an NMCI system or network shall immediately cease operation on the affected system and contact the NMCI Help Desk (Toll Free: 1-866-843-6624) and their command information assurance manager or designated personnel. SECNAVINST 5510.36, Chapter 12, details reporting responsibilities for both individuals and commanding officers upon loss or compromise of classified information.

DoD and DON information technology users are responsible for protecting classified information and knowing which security controls are required to protect classified data. By applying controls continuously and complying with applicable regulations, we can protect classified data and help ensure the integrity, protection and security of DON IT systems and equipment.

Jennifer Korenblatt is a member of the Department of the Navy Chief Information Officer (DON CIO) Information Assurance Team. CHIPS

Creating an IA Empowered Workforce – Standardizing Skill Development

By Sandra J. Smith

The Department of Defense Directive (DoDD) 8570.1, Information Assurance (IA) Training, Certification, and Workforce Management, calls for further professionalization of the IA workforce. This instruction forever changes the way we identify, train, certify and assign personnel, who perform IA functions associated with managing and supporting DoD enclaves, networks and computing environments.

The IA Imperative

Trusted information is the key to modern warfighting, and a secured Global Information Grid (GIG) is the cornerstone of this process. FORCEnet is the naval component of the GIG that will provide seamless and secure interoperability to Sailors, Marines and civilians. Since threats to information security can be catastrophic, our information must be protected from enemies, criminals, insiders or self-inflicted accidental events. Strong IA provides user confidence in information because the five crucial conditions — confidentiality, integrity, availability, authentication and non-repudiation — have been met. Creating a highly skilled and certified IA workforce becomes an imperative.

A Trained, Certified and Managed IA Workforce

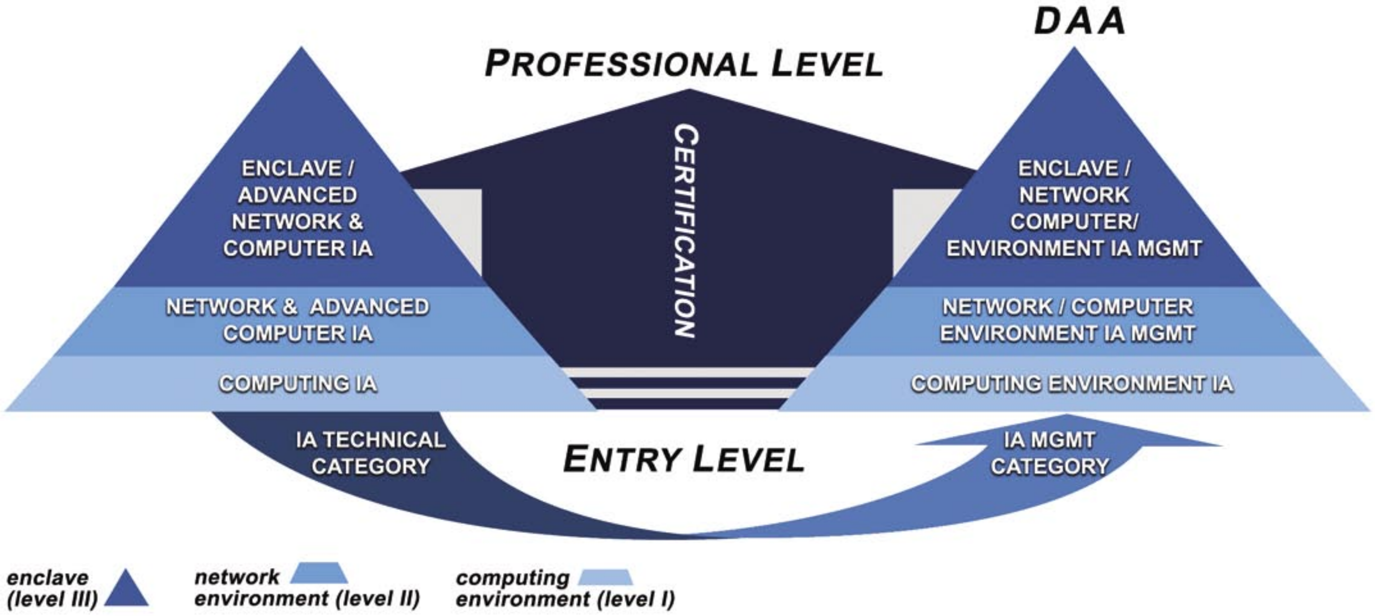
Several DoD directives and instructions have been published over the last few years that provide high-level IA policies and responsibilities. By law, the DoD is required to ensure its workforce is sufficiently educated and trained to assure the security of government networks. Additionally, the Federal Information Security Management Act of 2002, Title III of the E-Government Act of 2002 (PL 107-347), requires the Department of the Navy (DON) to report to DoD on IA training statistics and the status of personnel performing IA functions.

> *The protection of the GIG is everyone's business – this cannot be overstated. We take specific actions to train, license, qualify, and certify pilots and weapon systems users – we must consider no less of a standard for the operation, security, and integrity of the GIG. Our information base and our ability to leverage the technology to support warfighting, intelligence, and business functions must have the highest level of trust and confidence or we lose the advantage that information provides us.*
>
> *– Excerpts from Mission Possible - Security to the Edge*

DoDD 8570.1 specifically establishes IA training, certification and a workforce management policy for the Department of Defense, and authorizes publication of a manual that defines job role functions, minimum certification requirements and reporting, aligned to a four-year implementation plan. The focus of DoDD 8570.1 is on personnel (military, civilian, contractors and foreign nationals) with privileged access and IA managers.

The policy identifies IA personnel by the functions they perform — regardless of job series, occupational specialty or whether an

Figure 1. Proposed Overview of the IA Workforce Structure.


DAA
PROFESSIONAL LEVEL
CERTIFICATION
ENCLAVE / ADVANCED NETWORK & COMPUTER IA
NETWORK & ADVANCED COMPUTER IA
COMPUTING IA
ENCLAVE / NETWORK COMPUTER/ ENVIRONMENT IA MGMT
NETWORK / COMPUTER ENVIRONMENT IA MGMT
COMPUTING ENVIRONMENT IA
IA TECHNICAL CATEGORY
ENTRY LEVEL
IA MGMT CATEGORY
enclave (level III)
network environment (level II)
computing environment (level I)

individual is full-time or assigned to an IA function as an additional duty. IA professionals working in policy or training areas that are not performing DoD-defined IA functions are not included as part of the IA workforce that requires certifications. The draft DoD 8570.1-M, currently being finalized by DoD, describes IA management and technical functions and IA workforce levels, as depicted in Figure 1. Key policy requirements include:

- All authorized users of DoD information systems (IS) shall receive initial IA awareness orientation as a condition of access and, thereafter, must complete annual IA refresher awareness.

- Personnel performing IA privileged user or management functions, regardless of job series or military specialty, shall be properly identified in appropriate personnel databases.

- All positions involved in the performance of IA functions shall be identified in appropriate manpower databases by category and level.

- All IA personnel shall be identified, tracked and managed so that IA positions are staffed with personnel trained and certified by category, level and function.

- Privileged users and IA managers shall be fully qualified, trained and certified to DoD baseline requirements to perform their IA duties.

- The status of IA certification and training shall be monitored and reported as an element of mission readiness and as a management review item.

A DON Collaborative Approach

In response to these policy requirements, the DON IA Workforce Working Group (IAWWG) was established to help determine an Enterprise way ahead for implementation, and to develop strategies, recommendations and plans to achieve near- and long-term objectives. These objectives include standardizing skill development, ensuring blended and streamlined training, identifying associated efficiencies and identifying Naval Enterprise solutions to ensure compliance with workforce management mandates.

The DON CIO Strategy for Achieving Consistent IA Training, Certification, and Workforce Management, issued March 18, 2005, emphasizes key focus areas and an ongoing collaborative effort, which are crucial for not only achieving compliance, but also for strengthening the DON's IA posture, to grow and sustain a certified and trained IA workforce.

Under the auspices of the DON IAWWG, three tiger teams are focusing on (1) manpower and personnel; (2) training and certification; and (3) technological aspects of monitoring, tracking and reporting on the workforce. Initial efforts are focused on identifying personnel performing IA functions and improving records management of IA training. Identification of the workforce will also serve to establish a valid requirements baseline for human capital planning, and to formulate resource and implementation plans for IA training and certification programs.

The DoD's common naming schema will provide a universal language for delineating job roles of the IA workforce across the DON. Additional guidance will be provided as the IAWWG continues with Enterprise collaboration.

This is a major DON initiative that has engaged a dynamic group of representatives across the Department, which includes manpower, personnel and training organizations. As the DON further professionalizes the IA workforce with the knowledge, skills and tools to effectively prevent, deter and respond to threats, it not only shapes the workforce now and in the future, it ultimately supports network-centric operations and FORCEnet.

For additional information, visit the IA Workforce page of the DON CIO Web site at http://www.doncio.navy.mil/iaworkforce/.

Sandra J. Smith is the DON IM/IT Workforce Management team leader.

Annual IA Mandatory Training Deadline is Sept. 1, 2005 Do it: It's the Law!

All authorized users (military, civilians and contractors) of Department of Defense (DoD) information systems are required to complete information assurance (IA) awareness orientation training by Sept. 1, 2005.

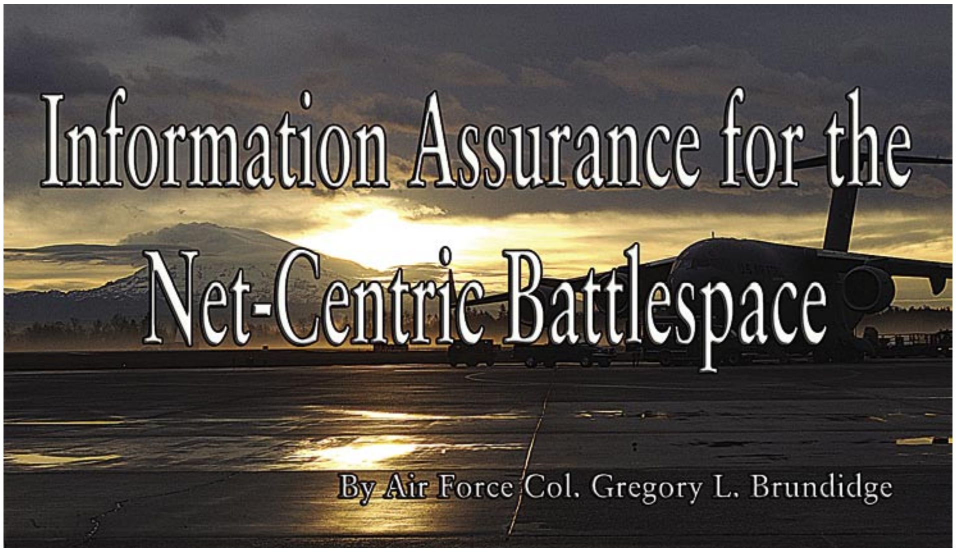
IA awareness training is available for the Department of the Navy (DON) through Navy Knowledge Online (http://www.nko.navy.mil) and MarineNet (http://www.marinenet.usmc.mil). Depending on your organization's structure, the command information assurance manager (IAM), information assurance officer (IAO) 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 of the workplace. For more information and step-by-step instructions for accessing the IA training, please visit the IA workforce page of the DON CIO Web site at http://www.doncio.navy.mil/iaworkforce/. If you need additional assistance, please contact the following POCs:

Navy – (757) 417-6757/DSN 537-6757

Marine Corps – (703) 693-3490/DSN 223-3490

DON – (703) 601-0605/DSN 329-0605



Information Assurance for the Net-Centric Battlespace

By Air Force Col. Gregory L. Brundidge

To meet the demands of today's net-centric-operations environment or battlespace, we must adapt a much broader construct for information assurance …

Today's aerospace operations environment is highly complex, lethal, and one that we must continue to dominate to achieve military operational objectives. Central to achieving these operational ends are the concepts of vertical and horizontal integration. These two operational tenets form the basis for how processes, operational capabilities and decision-quality information flow are knitted together to minimize or eliminate seams in the find-fix-target-track-engage-assess-kill chain.

Our recent successes in air campaigns in the Balkans and Southwest Asia demonstrate how well we have mastered the art and science of aerospace operations. Aerospace dominance, time-sensitive targeting, predictive battlespace awareness and effects-based operations are now today's essential operational realities.

Looking forward, we must further evolve these realities to achieve total battlespace awareness supporting real-time decision-making. Total battlespace awareness depends on dominant and agile operational support from a capabilities-focused enterprise that meets warfighter needs and eliminates seams.

At the center of all of these major operational movements is "the net" — the aggregate of all network connectivity (terrestrial, airborne and space), capabilities and processes from the physical layer connections and protocols, to net-enabled operational processes and applications. It is the essential fabric that serves to integrate vertically and horizontally, facilitates battlespace awareness and effects-based operations, enables operations support from a capability-focused enterprise and provides the means for accurate real-time decisions.

In this net-centric environment, information assurance is not simply ensuring that information is protected, accurate and delivered on time, it also means ensuring that all the components involved in making that happen are postured, prepared and ready to do so.

To define IA requirements for the net-centric environment, we must consider three pillars:

•**Technology:** Relevant technical capabilities and mission-driven innovation.

•**Processes:** Concept of Operations (CONOPS) and tactics, techniques and procedures (TTPs).

•**People:** Indoctrination, Training and Development.

Technology

When we consider the unstoppable advance of increasing capabilities in information processing, transfer and networking, the essential first component for IA is capable technology. As industry continues to improve information technology capabilities to process, exchange, transfer and store more information, faster and better, we must demand the parallel development of information protection capabilities. The ability to achieve authentication, integrity, confidentiality, non-repudiation and availability, the traditional elements of information assurance, or what we call "small ia," relies heavily on technologies that are on par with advancing information capabilities.

Therefore, it is not only important for us to be competent with today's ia technologies, but we must always have an eye on the ia technologies for tomorrow. Encryption, intrusion detection, firewall and authentication tools for our networks must evolve and grow with other network capabilities. This is especially important as more and more of these technologies are designed into network components vice stand-alone, add-on boxes.

By staying in touch with those who perform network operations (NETOPS) and deliver the full spectrum of network services, those who acquire these capabilities for the Air Force and Department of Defense (DoD) can ensure they deliver timely, usable and relevant technologies for tomorrow's ia demands.

Equally as important, is the need to standardize on vendor solutions or, at a minimum, provide specifications for vendors to meet when providing hardware or software components for the net-centric environment. This is an essential step to eliminating hard-to-manage, service disruptions on our networks and corresponding training and operations and management challenges in our NETOPS centers.

We do not acquire other weapon systems this way, so we should not expect our air crews and air, space and missile operators to train for unmanaged variability in the systems they operate.

Processes

We must consider the other two essential components: *processes and people*. To effectively command and control net-centric operations there must be well-defined

CONOPS, policies and procedures for governance, operation and sustainment.

Because NETOPS in the net-centric environment is a young operational discipline, we are in the process of developing many of the governing and guiding documents. Several CONOPS, such as the Air Force Network Operations (AFNETOPS), Air Force Network Operations Security Center (AFNOSC or Global NETOPS) and Integrated-Network Operations and Security Center (I-NOSC) have been finalized or are in draft review.

Likewise, we continue to evolve policy and strategy documents for guiding the development, implementation and operation of the net.

The process component of what we call "big IA" is critical because it enables optimized use of available technological capabilities. It does no good to have superior information technology — if we don't have the processes in place that enable us to leverage its power and transform it into relevant operational capability for the warfighter.

How often have we raced to field the latest hardware or software network tool or application only to complete fielding and find that we did not evolve our operations, concepts and procedures, so that our net technicians and users could leverage full capability?

Instead, we must use a capability-driven model that brings new network capabilities as operational requirements dictate and adjust CONOPS and associated processes and procedures prior to fielding. Ideally, we should train our technicians in advance, so we can implement new capabilities without disrupting current NETOPS.

The Air Force transitioned from SCOPE Network teams that focused on optimizing and securing base networks to SCOPE EDGE (enterprise, design, guidance and evaluation) teams. The advent of a centralized standardization and evaluation program, such as SCOPE EDGE for NETOPS, is a critical first step to form the foundation of a broader standardization and evaluation construct that will assess all critical processes delivering the net-centric environment. This will include network management, network administration, network defense and associated NOSC and Network Control Center (NCC) operations.

We will know we have achieved success when the TTPs, checklists, bold print and technical orders (TO) that govern these processes are in place and guiding the actions on the operations floors of our NETOPS centers. To keep these items current, the process for evolving network capability must accommodate the steps necessary to update them as we add new tools, applications and capabilities.

People

The most important component of the big IA triad is our people. It is our people who deliver the net-centric environment today in a less than ideal environment. We made a significant step in improvement with the advent of the Operationalizing and Professionalizing the Network (OPTN) initiative in 1998 to treat the network as a weapons system as one base, one network and one enclave.

However, with the exception of a recurring funded training line for essential network skills and standard NCC structures, we stopped short of realizing the OPTN objectives of an operationalized NOSC, NCC, and a professionally-certified and mission-qualified force of network technicians.

In the net-centric environment, the essential mindset is one that understands the interdependencies of the net and fully appreciates the importance of standards in our technologies and processes. The transformed net professional realizes that a network risk or vulnerability assumed by one is assumed by all. To complete a necessary mindset transformation, we start with training processes that span the development cycle for the technician.

From technical school to 7-level training, the program must be focused on building cross-trained net technicians. If we have standard system hardware and applications, and we employ standard processes and procedures in our NOSCs, NCCs and other NETOPS centers, then we should be able to mission-qualify and certify crew members who can perform proficiently in a like crew position at any Air Force NCC or NOSC.

We should "push the envelope" wherever possible to take net warrior training to the next level …

In addition to standardized training, we should "push the envelope" wherever possible to take net warrior training to the next level.

In industry, credibility comes from not only being able to deliver capabilities upon demand, but also from the level of certification one brings to the table. Thus, along with baseline training that allows net warriors to seamlessly flow from one organization to another, we should work toward getting our people mission-driven certifications recognized by industry, and focus on higher degrees of mission qualifications.

Certifications, such as Certified Information Systems Security Professional, Project Management Professional and Security A+, could equate to specialist, senior specialist and master specialist ratings for NCC and NOSC crew positions. Ratings would be determined by training and education completed, hours in the position and scores on check rides.

These ratings would mark the difference between those who dabble in our field and those whom we would consider to be experts. This produces a win-win situation for our organizations and the individual. Additionally, it raises the bar for improving net-centric operations across all dimensions of the mission area.

We can and must take steps to achieving a standard environment and training. As we standardize hardware and software and the TTPs we use to employ them, we pave the way for completing a transformation. To succeed, we must have the flexibility and leeway to acquire standard infrastructure hardware and core service applications for the Air Force.

Air Force Col. Gregory L. Brundidge is the former director of Communications and Information Pacific Air Forces. CHIPS

Introduction

The Naval Oceanographic Office (NAVOCEANO) Systems Integration Division (N64) has provided on-scene environmental prediction systems for the surface fleet for more than 20 years. From documentation to databases and data processing, NAVOCEANO N64 has served the mission of the warfighter. A key to this success is the development of Web-based applications.

Since its inception, the Geophysics Fleet Mission Program Library (GFMPL) has been the principal software suite used for fleet on-scene environmental predictions. Originally hosted on minicomputers and later personal computers, GFMPL consisted of meteorological, electromagnetic, electro-optical, oceanographic, acoustic and hazard-avoidance software applications. The software applications in the library continue to be used to increase safety for the warfighter and ensure combat effectiveness.

GFMPL

GFMPL was built from algorithms, models and databases from the Oceanographic and Atmospheric Master Library (OAML) established by the Naval Meteorology and Oceanography Command (NMOC). This master repository, of environmental data gathered by NAVOCEANO and computer code developed by research institutions, is the core of Navy environmental predictions. GFMPL has been integrated into other computer hardware and software systems, such as the Navy Integrated Tactical Environmental System (NITES) to maximize utility and meet broader fleet requirements.

Environmental databases and environmental prediction systems must be easily accessible to fleet users through state-of-the-art systems. To meet this challenge, NAVOCEANO has become fully integrated in FORCEnet planning and a full participant in net-centric warfare. Crucial to effectiveness, is the efficient transfer of tactical data and functionality using Web services.

Web services at geographically dispersed locations can be combined to provide users with services from a centralized location. The result is faster, more accurate, more consistent tactical information. GFMPL Web derives much of its data and functionality through a Web service infrastructure. The NAVOCEANO Web Services Working Group (NWSWG) was established in 2003 as the project manager for the creation of Web services for NAVOCEANO environmental databases and environmental prediction systems. When fully implemented, Web-based databases and Web-based applications, such as GFMPL Web will be accessed through the Navy Marine Corps Portal (NMCP).

In the future all Navy and Marine Corps applications will be accessed through the NMCP, and GFMPL Web will be an integral part of the NMCP. The NMCP will allow users to organize applications into customized "workplaces" and will provide a common "look and feel" for various tactical decision aids. Content will be organized into basic functional areas. Applications may be selected individually from hyperlink menus or by dragging and dropping to a workplace.

GFMPL Advantages

The advantages of Web services are many. Access to GFMPL Web is done through the user's Internet browser. The user may take advantage of the greater computing power of the server, which hosts GFMPL Web, and where the actual updates to software, databases and documentation are made. Larger, more dynamic environmental data can be made available to applications via online connectivity. The network employed by Web services can provide the user a much broader perspective of the tactical arena. The most important feature of GFMPL Web will be a reach-back capability for fleet users.

Upon connecting with the GFMPL Web on a secure SIPRNET workstation, the user is presented with a Web-based user interface. Individual applications are accessed through a menu structure of titled tabs and hierarchal hyperlinks. GFMPL Web applications use radio buttons, checkboxes and pull-down menus to quickly enter data, make configurations and generate desired outputs. An important feature is the use of scalable vector graphics (SVG), which provide interactive click-and-drag and zoom in or out capability. Nine software modules currently comprise the GFMPL Web, which are described below.

Map Utility (MAP) – seamlessly integrates with GFMPL Web applications by providing latitude and longitude coordinates and a reference to which output data may be plotted or displayed. The user may pan across the globe using an array of eight direction keys or choose to interactively zoom in or out of the map display. Entering latitude/longitude coordinates centers the geographic display accordingly. MAP is the geographic background and option that first appears to the GFMPL Web user when the connection is made.

Solar/Lunar Almanac Predictions (SLAP) – generates daily/monthly solar/lunar illumination, daily rise/set/transit times and hourly ephemeris data, as well as a Light-Level Planning Calendar (LLPC). GFMPL Web provides output graphs for Solar Daily Illumination (SDI), Lunar Daily Illumination (LDI), Solar Elevation Azimuth Angles (SEAA) and Lunar Elevation Azimuth Angles (LEAA). It also provides a location library in which to save inputs and predictions. A login is required to access the configuration controls.

Tidal Predictions (TIDES) – calculates a time series of daily/hourly tidal heights for specific tidal stations across the world. Latitude and longitude data are accepted with a mouse click in Map display. TIDES output may be selected from stations positioned on the map display with reference and secondary stations shown as display options seen in MAP. TIDES and SLAP applications interact to generate the Astronomical Planning Data, a presentation of sun/moon rise/set times and lunar percent illuminations with a graphical depiction of hourly tide levels superimposed on a day/night/twilight chronological display.

Surf Predictions (SURF) – computes wave height, percent breaking waves and the modified surf index (MSI) for sea and swell waves that move ashore. A graphic display is computed from the entered nearshore depth profiles. SURF provides a table of MSI limits for various landing craft used in amphibious warfare. MSI limits are color-coded with the familiar Go/No-Go (Green/Yellow/Red) criteria. Colors are determined by the computed MSI.

Wind Conversion – provides three-way conversion of true wind, measured (relative or apparent) wind and desired ship's heading/speed. When two of the three aforementioned data sets are entered, the remaining data set is computed. Computation may be done by direct data entry or by clicking and dragging the vertices of the wind triangle in the electronic maneuvering board. Depending on the magnitude of winds and speeds, the maneuvering board can be set to five different scales for size accommodation of the vector graphic. The user may also toggle the maneuvering board grid on and off.

Temperature Utility (Temp Util) – computes the wind chill temperature (WCT), heat stress index (HSI) and wet-bulb global temperature (WBGT) given the following inputs: ambient temperature (T), wind speed (for WCT), pressure for HSI and a moisture parameter for wet bulb temperature (WBT), dew point temperature (DPT) or relative humidity (RH). When one parameter is entered, the other two are computed. A black globe temperature (BGT) is required for WBGT calculation. Temp Util also allows the user to change the system of units employed by the calculation.

Pilot Balloon (PIBAL) – computes a vertical profile of wind direction and speed given the radio telemetry observations of a pilot balloon. PIBAL input includes the angles of elevation and azimuth of the balloon at whole-minute time intervals for three different weights of balloons. Output consists of a tabular listing of the inputs and the wind direction and speed at 300-meter intervals. PIBAL output may be saved for use in other tactical decision aids that require wind directions and speeds for input.

Pressure Altitude/Density Altitude (PADA) – computes the following parameters: sea level pressure (SLP), altimeter setting (ALSTG), pressure altitude (PA), density altitude (DA) and the standard atmosphere based on the upper/lower station pressure and the following optional data fields: station elevation (for ALSTG, PA, DA), 12-hour mean temperature (for SLP), temperature (for DA) and dew point for DA. PADA replaces the calculator wheel once used by fleet aerographers.

Unit Conversion Utility – consists of 47 electronic conversions in seven categories useful for forecasting, acoustics and nautical science. Categories are angle, density, distance, pressure, speed, temperature and time.

GFMPL Web has extensive online user documentation in the form of HTML Help. Web connectivity opens up many possibilities in the area of guidance and instruction. GFMPL Web text and images are easily captured for briefing support, using the inherent features of the Internet browser. Hardcopy printouts from GFMPL Web are obtained through the browser or with Windows functionality.

Future Enhancements

A number of enhancements are planned for GFMPL Web. SLAP will eventually be executed for saved plan of intended movement (PIM) tracks identified in MAP. SURF will access sea and swell inputs from the simulated waves nearshore (SWAN) wave model, surface wind data from the Navy Operational Global Atmospheric Prediction System (NOGAPS) database and depth profiles from a Web-based Hydrographic Reconnaissance Charts (HRC) library. The TIDES application will have additional tide stations from which to perform calculations.

PIBAL will include PILOT, PILOT SHIP and PILOT MOBIL messages as output options. Upgrades to the Briefing Support module are being investigated that will allow users to broadcast GFMPL output on the Web itself. With this webcasting feature, GFMPL Web will not only reach back but will also reach out to all users who require environmental predictions. Current development is underway for the future NMOC Enterprise portal.

In the future Sailors and Marines will access all meteorology and oceanography (METOC) support products, including GFMPL Web, at a single location on the Web. Currently, GFMPL Web may be accessed on the Navy Enterprise Portal or directly on the NAVOCEANO server at https://www.navo.navy.smil.mil/. Search for "GFMPL" in the Quick Search and then select the "GFMPL Web" radio button. GFMPL Web may also be used in a stand-alone mode for users, such as the Mobile Environmental Team offices, who must operate independently of the Internet. Plans are for the GFMPL Web Stand-alone to be downloaded from the GFMPL Web site or delivered on a CD-ROM by request.

GFMPL Web applications were successfully used in Trident Warrior 2004 (TW04), when net-centric warfare operations were put into practice. NAVOCEANO N64 supported the software training efforts of Space and Naval Warfare Systems Command (SPAWAR) personnel during TW04. It is from such exercises as Trident Warrior and the recommendations of forward-deployed units that vital software requirements are elicited. With fleet support, GFMPL Web will become indispensable in serving today's surface warfighter.

Peter Washburn works in the Naval Oceanographic Office Systems Integration Division (N64).

CHIPS

Trident Warrior 2005 - the premier FORCEnet Sea Trial event

By Brad Poeltler and Dr. Shelley Gallup

TW05 – the Navy's road to speed to capability

This fall, Nov. 28 - Dec. 10, the Naval Network Warfare Command (NETWARCOM) takes FORCEnet to sea for the third in a series of Trident Warrior events, when U.S. Second Fleet units of the USS Iwo Jima Expeditionary Strike Group and coalition partners will participate off the coast of Virginia in Trident Warrior 2005 (TW05).

Participants will include 2nd Fleet's Commander, Amphibious Squadron (COMPHIBRON) 4, 24th Marine Expeditionary Unit (MEU), USS Wasp (LHD 1), USS Iwo Jima (LHD 7), USS Nashville (LPD 13), USS Whidbey Island (LSD 41), USS Philippine Sea (CG 58), USS Bulkeley (DDG 84) and USS Cole (DDG 67). Coalition units participating from Australia, the United Kingdom, Canada and New Zealand will include the HMCS Montreal (FFH 336), HMCS Fredericton (FFH 337), HMNZS (virtual), HMNZS Te Mana (F111) and HMS Liverpool (D92).

Other commands supporting NETWARCOM and TW are:

- Space and Naval Warfare Systems Command (SPAWAR) – the TW engineer
- Naval Postgraduate School (NPS) – the TW lead in data collection, analysis and TW05 findings
- Naval War College (NWC) – conducts the TW wargame
- Marine Corps Concept Development Command (MCCDC) – provides the Marine Corps lead for TW
- Naval Personnel Development Command (NPDC) – provides the naval doctrine lead for TW.

While FORCEnet provides the command and control (C2) component of Sea Power 21, TW05 will create an operating environment to explore the functional concept for FORCEnet. The Chief of Naval Operations, Admiral Vern Clark, and the Commandant of the Marine Corps, General Michael W. Hagee, signed and formally issued a joint FORCEnet document titled "FORCEnet: A Functional Concept for the 21st Century."

The overarching hypothesis of the FORCEnet Functional Concept states "… that if all forces and organizations down to the level of individual entities are interconnected in a networked, collaborative command and control environment, then all operations and activities can enjoy the benefits of decentralization, including initiative, adaptability and increased tempo, without sacrificing the coordination or unity of effort typically associated with centralization."

The operational impact should be "… *command and control characterized by shorter decision cycles that allow commanders to make and implement better decisions faster than any enemy can tolerate….*" The results will be units and platforms able to adapt more quickly and effectively to changing circumstances and the ability to self-synchronize in furtherance of the mission.

To understand the operational impact of FORCEnet command and control concepts, C2 must be executed in a realistic environment to assess, in quantitative and qualitative terms, FORCEnet enabling technology and ways it is used through tactics, techniques and procedures (TTPs).

Analysis of collected data provides insights resulting in dedicated procurement and development decision information required to produce "speed to capability" (S2C). Speed to capability is the rapid fielding of improved FORCEnet C2 warfighting capabilities to the fleet with full supportability and maintainability. It also includes continuous development of supporting TTPs.

In today's global war on terrorism with responses ranging from large or small scale regional conflicts to relief operations, there is a potential for the configuration of an expeditionary strike group (ESG) or carrier strike group (CSG) to include coalition partners pulled from their national regional assets. So FORCEnet concepts must also provide continuity across the coalition with a Combined Forces Maritime Component Commander (CFMCC). NETWARCOM is partnering with 2nd Fleet to focus on FORCEnet support of a CFMCC from the operational to tactical level.

TW05 will focus on key enablers of FORCEnet capability to make the CFMCC fully capable of creating coalitions able to meet all challenges. Specific FORCEnet capabilities will be advanced in the following areas.

• **Naval Networks**. Optimizing communications bandwidth on naval networks for the fleet and providing communications interoperability capability for coalition forces are critical. Increasing bandwidth is a serious challenge across a strike group and especially with coalition partners. However, improving the efficient use of bandwidth can be accomplished through technical and administrative means.

TW05 will explore a range of these options, document them, and make them part of ESG and Combined Forces Maritime Component Commander TTPs. There will also be specific focus on the integration of enhanced coalition interoperable doctrine and technology into the Combined Enterprise Regional Information Exchange System (CENTRIXS).

FORCEnet will enable command and control characterized by shorter decision cycles that allow commanders to make and implement better decisions faster than any enemy can tolerate …

- **Cross Domain Solutions (CDS).** Cross Domain Solutions create a network-centric capable strike group across U.S. and coalition forces. The technical means to include and increase the capabilities of the assigned staffs and ships from the coalition nations will be included in TW05. Specifically, CDS will address multinational, multilevel, multidomain and interoperability issues that involve dynamic networks consisting of guards that support cross domain transfer of information.

- **Information Management/Collaboration.** This is essential to create and manage a CFMCC information management plan that addresses information management and processing between coalition units brought together in an ESG. TW05 will also be used as an opportunity to define Navy FORCEnet requirements for chat and collaboration tools.

- **Knowledge Management (KM).** Basic KM research begun in TW04 will continue in TW05. While information management focuses on the connectivity and flow of information, the KM focus of TW05 will be the definition of the "actionable information" moving across the networks. These knowledge flows may be documented, measured and used to improve the content of information and information systems.

- **Command and Control.** C2 decision tools are essential to synchronize planning and resource management for assets across the strike group. CFMCC operational planning tools and a common operating environment (COE) that integrates access to data used in automatic generation and dissemination of maritime task plan information will be developed in TW05.

- **Human System Integration (HSI).** HSI focuses on the integration of warfighters engaged in automated information processing and decision-making tasks. In TW05, HSI experts will document the information and knowledge requirements a CFMCC needs in a global war on terrorism. HSI focus will find the best methods to populate a CFMCC decision-support system by filling in knowledge gaps with the required information.

- **Intelligence, Surveillance and Reconnaissance (ISR)**. Future synchronization of ISR capabilities will be worked through distributed ISR nodes, which, in turn, will support effects-based operations in joint-coalition environments. TW05 will identify and document interoperability and information exchange requirements between Network-Centric Collaborative Targeting (NCCT) and Cooperative Engagement Capability (CEC) which are used to provide improved battlespace awareness. In addition, TW05 will be the Navy's first opportunity to work the Global Hawk Maritime Concept of Operations (CONOPS) and TTPs to support intelligence dissemination. Data from Global Hawk Maritime events in TW05 will be used to determine a baseline for time, accuracy and quality of intelligence dissemination.

Atlantic Ocean (April 23, 2005) - Aviation Boatswain's Mate 2nd Class Courtney F. Godfrey runs behind the foul line as a Marine Corps AV-8B Harrier II+, assigned to the "Bulldogs" of Marine Attack Squadron Two Two Three (VMA-223), performs a vertical takeoff from the flight deck of the USS Iwo Jima (LHD 7). U.S. Navy photo by Photographer's Mate 1st Class Robert J. Fleugel.

- **Naval Fires.** Automation through FORCEnet implementation of machine to machine (M2M) technologies enables movement of targeting information between aircraft and C2 nodes. This brings aviation assets into the Navy's fires process and provides the CFMCC with an increased ability to apply force within the battlespace. As part of the fires initiative in TW05, track and chat data will flow between the CFMCC and coalition units enhancing targeting situational awareness and potential tasking of targets.

- **Information Operations (IO).** Information Operations are conducted using a variety of tools, all which need to be coordinated and synchronized. TW05 will further refine coordination and interoperability of information operations tools to conduct synchronized IO campaign mission planning for the CFMCC staff.

Findings and recommendations gathered from TW05 will be presented to the Sea Trial Executive Steering Group (STESG) to enable Navy leadership to make informed decisions on the current and future course for FORCEnet.

"Trident Warrior is essential to getting concepts and capabilities to sea, trying them out in a realistic environment, and learning from them what is useful and should be implemented or advanced in a fast track," said Vice Adm. James McArthur, commander of NETWARCOM.

The planning is already underway for TW06, which is scheduled to take place in the Eastern Pacific June 2006.

Mr. Brad Poeltler is a retired Navy captain and assistant director for Trident Warrior 05.

Dr. Shelley P. Gallup is an associate research professor at the Naval Postgraduate School, Department of Information Sciences. He has been the director for analysis of Fleet Battle Experiments and NETWARCOM's FORCEnet experimentation.

CHIPS

SSC Charleston – First SPAWAR Systems Center to Achieve CMMI® Maturity Level 2

By SSC Charleston Engineering Process Office

Achieving CMMI Maturity Level 2 for the command reinforces SSC Charleston's standing as a quality provider of systems engineering, software engineering and information technology services …

Introduction

The Space and Naval Warfare (SPAWAR) Systems Center (SSC) Charleston successfully completed phase one of its process improvement effort by achieving Capability Maturity Model Integration (CMMI®) Maturity Level 2. This achievement is a milestone not only for SSC Charleston, but for the entire SPAWAR claimancy because Charleston is the first systems center within SPAWAR to attain CMMI Maturity Level 2.

In April 2005, Richard Barbour, a senior member of the technical staff of the Software Engineering Institute (SEI), led an appraisal team that evaluated SSC Charleston processes. The results revealed that SSC Charleston had implemented the best government, industry and academic practices, reflected in the SEI's CMMI model for Systems Engineering and Software Engineering (CMMI®-SE/SW), attaining command-level CMMI Maturity Level 2.

In Pursuit of Excellence

SSC Charleston has been actively pursuing process improvement efforts since 1998 and reaffirmed this commitment in 2003 with a command-wide Process Improvement Policy. The policy directs the use of best practices from the CMMI-SE/SW model for SSC Charleston systems and software engineering projects and tasks.

The command chose to implement the CMMI because it provides a structured model for process improvement and is used to measure and improve an organization's ability to successfully manage complex projects. The model recognizes excellence in business practices, measured against a set of demanding criteria.

Michael T. Kutch, Jr., director of Engineering Operations, SSC Charleston.

The SEI has reported quantitative evidence showing how CMMI-based process improvement can result in improvements in cost, schedule, quality, customer satisfaction and return on investment. Government agencies and private industry increasingly use the CMMI model to evaluate an organization's ability to produce high-quality products on time and within budget.

James Ward, executive director of SSC Charleston, credited much of the CMMI Maturity Level 2 success to Michael T. Kutch Jr., director of Engineering Operations (Code 09K).

… [Mr. Kutch] "developed the process improvement strategy, the process improvement plan and the process improvement program. He sponsored training and an organizational infrastructure … Mike executed his plans to perfection and achieved CMMI Maturity Level 2 on time, in accordance with the schedule he provided in February 2004," said Ward.

SSC Charleston's process improvement strategy is in line with its systems engineering revitalization efforts, all of which focus on having sound processes and practices. Since SSC Charleston designs, acquires, engineers and supports technology-based systems, products and services for the warfighter, instituting a superior engineering capability is critical to the command's mission.

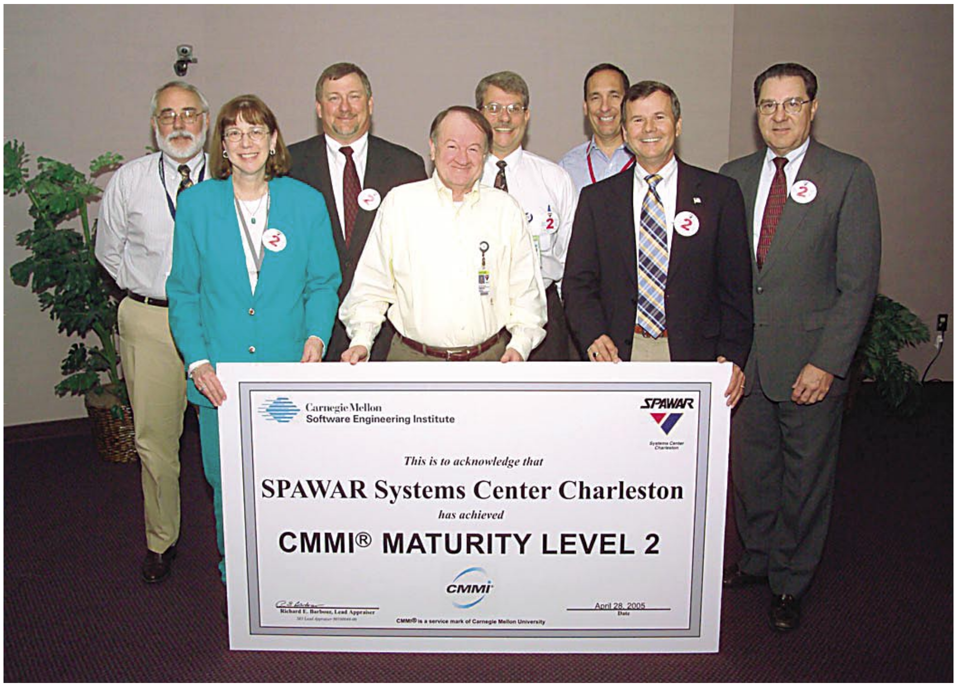
Institutionalizing Excellence

SSC Charleston designed an aggressive systems engineering program. The program includes applying key industry standards and best practices to improve both systems and software engineering processes.

Industry standards, such as the ISO/IEC 15288 systems engineering standard and the ISO/IEC 12207, which addresses software life cycle processes are the common overarching directives for all systems and software engineering projects. In addition to the CMMI, SSC Charleston applies other industry best practices including ISO 9001 and Lean Six Sigma.

Another key focus of the systems engineering program includes increasing the knowledge and skills of SSC Charleston's most competitive advantage — its employees. Engineering Operations provided SEI-authorized training for the SEI's "Introduction to CMMI" course to teach personnel how to apply the principles of the CMMI model to their respective projects.

To offer process improvement training to more employees, the department developed a self-paced online tutorial called, Process Improvement Web-Based Training (PI-WBT). Students receive a certificate upon course completion. At this time, nearly half of SSC Charleston's 2,300 employees have received process improvement training.


Carnegie Mellon
Software Engineering Institute
SPAWAR
Systems Center Charleston
This is to acknowledge that
SPAWAR Systems Center Charleston
has achieved
CMMI® MATURITY LEVEL 2
CMMI
Richard E. Barbour, Lead Appraiser
April 28, 2005
Date
CMMI® is a service mark of Carnegie Mellon University

SSC Charleston has been actively pursuing process improvement efforts since 1998 and reaffirmed this commitment in 2003 with a command-wide Process Improvement Policy. In April 2005, SSC Charleston attained command-level CMMI Maturity Level 2.

Back row, left to right: Francis Allston, deputy director for Transformation and Michael T. Kutch Jr., director, Engineering Operations, with SSC Charleston Board of Directors members: Kevin McGee, head, Command and Control Systems Department; William Paggi, head, Contracts Office; Jerry Koenig, head, Intelligence and Information Warfare Systems Engineering Department; front row, left to right: Georgia Lack, deputy chief of staff; Freddie Hicks, head, Comptroller Office; and James Ward, executive director, SSC Charleston.

In addition to providing vital process improvement training, the engineering operations department is offering the Systems Engineering Fundamentals course to both new and senior engineers.

This course continues to receive rave reviews from students because the material introduces key process concepts to new engineers and provides refresher training for senior engineers. So far, 120 employees have taken the training and additional courses are planned through 2006. Currently, SSC Charleston is preparing the Fundamentals of Software Development course.

Planning for Success

The process improvement strategy includes creating an Engineering Process Office (EPO) to provide process improvement guidance and CMMI implementation support to personnel. For example, the EPO developed sample documents, document templates and standard operating procedures (SOPs). The EPO also developed a software tool, called the electronic plan builder (EPB), an application that guides users through the process of creating project plans that are CMMI-compliant.

To help drive the process improvement effort, SSC Charleston created a Corporate Engineering Process Group (EPG). At the department level, EPGs were created to execute the process improvement effort within each department. SSC Charleston also formed several CMMI-related Integrated Product Teams (IPTs) as process area owners.

SSC Charleston's journey toward CMMI Maturity Level 2 began by implementing the model in a number of projects, which were selected by various department and division heads. To assess compliance with the CMMI model, the EPO performed mini-assessments to benchmark progress toward the attainment of Maturity Level 2 for their respective projects and for the overall command.

SSC Charleston's first successful CMMI project was the Common Information Centric Security project, which underwent a formal appraisal and achieved CMMI Maturity Level 2 in June 2004. Since that time, additional SSC Charleston projects have been formally appraised.

During the two-week (April 18-28, 2005) command-level appraisal, the appraisal team reviewed and evaluated process documentation and supporting artifacts. The appraisal team also interviewed personnel concerning CMMI implementation for their projects.

Achieving CMMI Maturity Level 2 for the command reinforces SSC Charleston's standing as a quality provider of systems engineering, software engineering and information technology services.

CMMI appraisal results revealed that SSC Charleston had implemented the best government, industry and academic practices, reflected in the SEI's CMMI model for Systems Engineering and Software Engineering (CMMI®-SE/SW) attaining command-level CMMI Maturity Level 2 …

"As a result of this historic achievement, our customers will reap multiple benefits. Empirical data from the SEI indicates that our customers can expect improved productivity, reduced defects, decreased cycle time, and delivery of products on time and within budget …," said Ward.

The Next Step

SSC Charleston is well on the way to reaching its goal of becoming a world-class systems engineering organization. The next phase in SSC Charleston's process improvement effort is to achieve CMMI Maturity Level 3. CHIPS

Can You Hear Me Now?

First Responders Rely on Land Mobile Services

By the DON CIO Telecom/RF Spectrum/Wireless Team

The value of the improved coordination for first responders will undoubtedly enhance public safety not only on federal installations but also in adjoining communities ...

The sentries posted at the armory, the crews at the fire station, and the base security patrols in their squad cars all depend upon wireless communication to perform their duties with responsiveness and effectiveness. This is not combat, but the stakes can still be high.

This article focuses on wireless solutions for first responders with specific details for Marine Corps requirements. A future article will discuss the Navy's plan to meet its unique wireless needs for first responders.

Intelligence Reform Act

On Dec. 17, 2004, President Bush signed into law the Intelligence Reform and Terrorism Prevention Act of 2004. Title VII of the Act implements certain recommendations of the National Commission on Terrorist Attacks Upon the United States, including communications-related provisions related to use of the electromagnetic spectrum by federal, state and local emergency response providers.

The Department of the Navy (DON) approached this legislation in strategic coordination with other federal agencies and has engaged in operational planning with emergency elements at various bases, posts and stations where Sailors, Marines, civilians and military family members work, live and utilize the facilities.

Land Mobile Service

The primary wireless communication solution for local, state and federal agencies supporting the public safety is called land mobile service. It provides radio connectivity between fixed base stations and land mobile stations (i.e., stations capable of surface movement) or between multiple land mobile stations.

The land mobile service is vital to supporting the public service missions of federal agencies. Unique federal requirements for land mobile service include: providing for national security; promoting public safety for traveling via air, water and land; interdicting entry of illegal aliens and substances into the United States; establishing communications between disaster areas and relief forces; ensuring swift search and rescue operations; protecting national forests, parks and farmlands; bringing to justice perpetrators of federal crimes; and ensuring the security of energy generation and distribution sources.

A U.S. Marine Corps service member using the Enterprise-Land Mobile Radio (E-LMR).

DON Use of Land Mobile Service

Non-tactical land mobile radio systems used by the DON include equipment such as base, repeater, vehicular and handheld stations in a variety of geographic environments supporting voice and data communications. Navy and Marine Corps land mobile radio systems are usually multipurpose systems, for example, law enforcement, emergency medical, administrative and public works functions may be supported by the same radio system. The radio systems, which are purchased from commercial vendors, are similar to those employed by non-federal entities.

Users communicate in a dispatch/supervisory, one-to-many or one-to-one mode while other users monitor the channel and take action as appropriate. Typical messages from mobile sources are of short duration, and typical channel hold times for these mobile communications are quite short, usually less than a minute. Under these circumstances, one or more channels can often be shared by several independent users.

Although DON personnel use common carrier services, such as cellular telephones and radio pagers to augment communication needs, they do not serve as replacements for the DON's own land mobile systems. While both the Marine Corps and the Navy have selected similar approaches to land mobile service based on open standards, specific deployment is unique for each service.

Marine Corps LMR Challenges

The Marine Corps combat team faces diverse challenges stemming from the global war on terrorism, such as conducting combat and logistic operations in Iraq and Afghanistan and providing antiterrorism and force protection inside and outside CONUS. Not altogether different from the Marine Corps combat team, the Camp Pendleton Fire Department has been fighting and winning battles with structure and wildfires on this terrain-unique base in Southern California.

The department's primary mission is to save lives and property. Even before the recent legislation, the Camp Pendleton Fire Department coordinated efforts with the surrounding communities; thus, a requirement for reliable communications that provides interoperability with neighboring federal, state and local fire departments was identified. Since off-base counterparts of the Camp Pendleton Fire Department used commercial-off-the-shelf (COTS) equipment, a Marine Corps solution pointed to similar technology.

Concurrent with the Camp Pendleton Fire Department's need was a mandate, issued by the National Telecommunications Information Administration (NTIA), to adopt new narrowband technologies that allow greater spectrum efficiency for all land mobile radios (LMRs) used by the federal government. Serving as the president's principal adviser on telecommunications and information policy issues, NTIA also manages the federal use of spectrum and resolves technical telecommunications issues for the federal government and private sector.

The mandate sought a phased replacement of all government-owned wideband commercial handheld radios (commonly referred to as walkie-talkies but technically LMRs) beginning in 2005 and finishing not later than Jan. 1, 2008. This replacement effort requires more than individual radio unit replacement; the entire backbone infrastructure of every Marine Corps CONUS installation, including integrating system equipment, antennas, cabling, and other hardware and software directly related to the system would have to be replaced.

Faced with the Camp Pendleton Fire Department requirement and the NTIA narrowband mandate, Headquarters Marine Corps (HQMC), Marine Corps Combat Development Center (MCCDC) and the Marine Corps Systems Command (MARCORSYSCOM) coordinated efforts to review, not only Camp Pendleton's requirement for land mobile radios, but all Marine Corps requirements for LMR.

Results of a study indicated that all Marine Corps installations have similar requirements for LMR. Most deal with range fires, all deal with saving life and property, all have antiterrorism and force protection roles, and all have similar requirements for crisis type actions involving natural and manmade disasters. Yet, some aspects of the basic requirements may differ.

While Camp Pendleton and Marine Corps Air Station (MCAS) Miramar routinely deal with range fires and sometimes earthquakes, Camp Lejeune and other installations along the East Coast, deal with hurricanes. The study identified that Marine Corps fire departments were ill-equipped to operate (off base) beyond the radio coverage of the existing LMR trunking systems. Furthermore, some bases lacked both intra-operable (within base) communications capabilities and interoperable off-base communications coordination with authorities. The study also identified that visiting units to other Marine Corps installations could not routinely use their own LMR equipment due to proprietary design differences.

An Enterprise-Land Mobile Radio (E-LMR) Rapid Response System (RRS) – a truck-mounted, 10-channel system, which includes 300 handheld radios.

Marine Corps E-LMR Mandate

The results of the study and the federal narrowband mandate clearly identified a requirement for a one-size-fits-all solution. HQMC C4 drafted a Statement of Need for an Enterprise-Land Mobile Radio (E-LMR) network. The Marine Requirements Oversight Council (MROC) mandated E-LMR as a program of record.

The MROC also directed three initial efforts for E-LMR: (1) Field two transportable E-LMR systems that provide interoperable communication capabilities with federal, state and local authorities for Marine Corps first responder and operating forces support outside the installation radio coverage areas; (2) Field an Immediate Interoperable Solution (IIS) that provides interoperability with off-base authorities using the existing installation LMR systems; and (3) Priority fielding of E-LMR to Camp Pendleton and the Marine Corps National Capital Region (MCNCR) that includes Marine Corps Base (MCB) Quantico.

To date, two transportable Rapid Response Systems (RRS) have been fielded. Located at Camp Pendleton and Camp Lejeune, the MARCORSYSCOM project is a truck-mounted, 10-channel, E-LMR system, which includes 300 handheld radios. The RRS provides interoperable communications to the most widely used federal, state and local LMR frequency bands. Each RRS contains a diesel generator as well as a 60-foot pneumatic antenna mast section.

The IIS, awarded in two separate MARCORSYSCOM contracts, is progressing well. The installed IIS at MCAS Cherry Point provides interoperable communications, using the existing LMR system, The Marine Corps combat team faces diverse challenges stemming from the global war on terrorism …

for up to 23 different off-base authorities. IIS projects for Camp Pendleton, Camp Lejeune and MCB Quantico are expected to be completed by the end of fiscal year (FY) 2005. The IIS contract to provide identical capabilities for all remaining Marine Corps CONUS installations was awarded in May 2004.

The third immediate effort directed by the MROC is the fielding of E-LMR to Camp Pendleton and MCNCR. The MROC determined that these two sites were exposed to the greatest threat of terrorism and posed the most significant requirement for LMR interoperability. The proposed 30-mile off-base radio coverage delivered by these systems will provide enhanced LMR capabilities. The contract will provide a new trunking system backbone that operates Voice over Internet Protocol (VoIP) allowing follow-on E-LMR expansion and roaming-like capabilities.

Because the E-LMR network adheres to an Association of Public-Safety Communications Officials (APCO) standard (Project 25), it will provide a myriad of interoperability possibilities including system-to-system and over-the-air capabilities that were previously unattainable due to proprietary vendor specifications. The entire backbone infrastructure, including the radios, is fully encrypted with the Advanced Encryption Standard (AES). Although not authorized for classified communications, AES provides a robust encryption capability.

Initially, the new E-LMR environment will provide handheld, vehicular and base station radios to Marine Corps first responders and the location's mission critical requirements, including weapons and test range operations, flight line operations, area guard and other areas that require immediate voice capabilities. The completion of the Camp Pendleton and MCNCR E-LMR systems is scheduled for the first quarter of FY 2006. HQMC has been working on the E-LMR project hand-in-hand with the Navy. Led by the Chief of Naval Installations (CNI) N46, the Navy is moving forward with a similar initiative.

The benefits of E-LMR are many: increased communication that results in increased security for Marine Corps installations, interoperable communications for first responders, which results in dynamic on- and off-base response capabilities and increased safety for operating forces training on range complexes. The cumulative E-LMR benefits and capabilities are dependent on the successful coordination of all the resources that can be aggregated through these wireless communication systems.

The DON proves each day in combat that its capacity to synchronize resources with joint partners enables greater force capabilities over the foe. The value of the improved coordination for first responders will undoubtedly enhance public safety not only on federal installations but also in adjoining communities.

For more information, contact the DON CIO Telecom/RF Spectrum/ Wireless Team at DONSPECTRUMTEAM@navy.mil. CHIPS

New Credit Alert Available for Active Duty Personnel

By Patricia Reid Huggins

Active Duty Alert Helps Combat Identity Theft

Identity theft is a growing crime in the United States. Consumers, including non-active duty personnel, can take various actions to minimize the risks of identity theft including checking credit reports regularly and keeping track of monthly bills.

Active duty personnel who are away from their regular duty stations are less able to take these steps, so they can be particularly vulnerable to identity theft. To enable personnel on active duty and activated reservists to devote their attention exclusively to the defense needs of the nation, Congress recently created a new tool to help guard against identity theft: the active duty alert.

Active Duty Alert

The active duty alert is a statement that is placed in the credit file of an active duty military consumer so that anyone checking the file for the purpose of establishing or extending credit is informed that the person is on active duty and the identity of the person requesting credit must be verified before the request can be granted.

The active duty alert is part of the Fair and Accurate Credit Transactions Act of 2003 (FACTA), which amends the Fair Credit Reporting Act (FCRA). Congress designed this alert as a protection for those deployed in locations or situations in which they are unlikely to be able to apply for credit or monitor their financial accounts. *(For more information about FACTA and FRCA, go to http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ159.108 and http://www.ftc.gov/os/statutes/031224fcra.pdf, respectively.)*

Under FACTA, if you qualify as an active duty military consumer, you can place an active duty alert in the credit file maintained on you by nationwide consumer reporting agencies. You may also designate a personal representative to place or remove the alert for you. The alert lasts for 12 months, but if you receive an extended deployment, you may place another active duty alert after the first one expires. You may cancel the alert at any time by contacting one of three credit reporting agencies (CRAs): Equifax, Experian and TransUnion. (See the text box on the next page for contact information for the CRAs.)

Credit Reporting Agency (CRA) Contact Information

Equifax	Experian	TransUnion
P.O. Box 740256	P.O. Box 2002	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

To place an active duty alert, you or your personal representative may contact one of the three CRAs, and tell them you want the alert placed in your file. You or your representative will be asked to provide certain personal information as proof of your identity, such as your Social Security Number, name, current address (and most recent previous address if you have been at your current address for less than six months) and other personal information. Be sure to keep this information current for the duration of the alert.

Once you have requested an active duty alert from one of the CRAs, that agency must:

√ Place an alert in your file indicating you are an active duty military member;

√ Remove you from marketing lists for prescreened credit card offers for two years (unless you ask to be placed back on the list before then); and

√ Alert the other two credit reporting agencies through the Fraud Exchange System.

You do not need to contact all three agencies; the CRA that you contact will contact the other two. You will receive confirmation when an alert is added to your credit file.

Once the alert is placed in your credit file, the consumer reporting agencies will notify any business that is asked to establish new credit or extend credit to you about the alert. The business must then take reasonable steps to verify that you are the person seeking credit and not an identity thief.

If you provide a telephone number for verification purposes as part of your active duty alert, the business must try to contact you using that number or take reasonable steps to verify your identity before authorizing any new credit plan or credit extension. The alert may cause some delays if you are trying to obtain credit, but it will also make it more difficult for an identity thief to fraudulently obtain credit in your name.

Credit Protection for All Consumers

Under FACTA, consumers, including non-active duty personnel, can fight identity theft using two other tools: free credit reports and fraud alerts. You can now receive one free credit report from each of the three CRAs each year. Regularly requesting and monitoring your credit report is a good way to control identity theft.

To obtain your free reports, contact the credit reporting agencies or go to http://www.annualcreditreport.com for further instructions. Note that free credit reports will be available by region through a nationwide phased rollout starting Dec. 1, 2004, on the West Coast and ending Sept. 1, 2005 on the East Coast. Check the credit report Web site above to determine when people in your state become eligible to receive reports.

If you think you have been a victim of identity theft, you can place a fraud alert in your credit file by contacting any one of the three CRAs. The alert will last for 90 days and requires any creditor to contact you directly before opening any new accounts or changing existing accounts in your name. For further information regarding identity theft, including other steps you can take to minimize the risk of identity theft, visit the Federal Trade Commission (FTC) Web site at http://www.consumer.gov/idtheft/.

The FTC has updated its popular booklet "Take Charge: Fighting Back Against Identity Theft," which offers "consumers and businesses meaningful guidance and useful tools for resolving the many different issues facing identity theft victims." The booklet is available from the Web address above.

For information specifically for military and Department of Defense (DoD) personnel, visit the Military Sentinel Web site at http://www.consumer.gov/military/. Military Sentinel is a project of the FTC and the DoD to identify and target consumer protection issues that affect members of the U.S. Armed Forces and their families.

At the Military Sentinel Web site, you can enter complaints about suspected fraud attempts and identity theft schemes. To file a consumer complaint, go to the Web site above and click on your service seal. This will link you to the appropriate consumer complaint forms.

Consumer Web sites

Fair and Accurate Credit Transactions Act of 2003 (FACTA)
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ159.108/

Fair Credit Reporting Act (FCRA)
http://www.ftc.gov/os/statutes/031224fcra.pdf/

Federal Trade Commission (FTC)
http://www.consumer.gov/idtheft/

Military Sentinel
http://www.consumer.gov/military/

Patricia Reid Huggins is on the Department of the Navy Chief Information Officer (DON CIO) Information Assurance Team.

Editor's Note: See "Identity Theft," CHIPS Fall 2004 at http://www.chips.navy.mil/archives/04_fall/PDF/identity.pdf and "Identity Theft: A True-Life Crime Story" and "Identity Theft: A Secret Crime," LIFELines at http://www.lifelines.navy.mil for more information.

The Lazy Person's Guide to Controlling Technologies Part I: E-Mailaholics Anonymous

By Retired Air Force Major Dale J. Long

Losing Control

Over the last 15 years the computing environment has changed from one dominated by the laborious production of paper-based documents to one drowning in easily published computer-generated documents. The Internet has transformed from a relatively quiet, elite, scientific and technical community to an international playground with vast stores of information (and misinformation), a wide variety of entertainment and billions of dollars of commercial activity.

Older, less computer-savvy employees have left the workforce. These were the people who checked e-mail twice a day, at the same time every day, if they bothered to check it at all. They printed and filed their e-mail in a folder, could only deal with a printed telephone book and thought that a Boolean operator was someone running a telephone switchboard in a third-world country.

Younger workers, who have used computers their entire lives, are now gaining a toehold in the workplace. Need help figuring out your personal digital assistant (PDA), cell phone, computer or any software associated with them? Just ask the new 20-something kids in the information technology (IT) department. Do not expect to understand them, just let them tweak your device and hope you can still use it later. You may even remember having to do something similar when you were younger, and someone asked you to program or set the clock on a videocassette recorder. If only the new stuff could be as simple as that old VCR.

Yes, technology is a lot smarter. Instead of cordless telephones with 10-speed dial numbers, there are cell phones that hold 500 numbers, synchronize with the contacts list in your personal computer (PC), and remind you about birthdays, anniversaries and other significant events. VCRs, which used to be the apex of home entertainment confusion and convenience, are now being replaced by digital video recorders that not only record programs, they also remember what we watch and recommend (or even automatically record) other programs their programming determines we might like.

Do you feel like you have lost control of your work environment? Do you become completely dysfunctional if you lose network connectivity or e-mail? Does your computer sound off with Eric Idle saying, "Message for you, sir!" when e-mail arrives? Then this article is for you. Controlling technology has a double meaning: There is a difference between controlling technology and technology controlling you. In this issue, we will start with the most insidious addition to the work environment today: e-mail.

E-Mail is My Life

I freely admit that I am a chronic e-mailaholic. I cannot resist the siren call of my e-mail alert sounds and have to stop what I am doing every time the alert goes off to check my mail. I cannot resist endlessly assigning individual sounds to tell me who among my family, friends and co-workers have sent me e-mail. I am getting better, though. I have cut down to only three or four e-mail accounts, and my two main inboxes have fewer than 100 messages each at least once a month. While I still respond and reflexively check my inbox like one of Pavlov's dogs when the e-mail alert rings, at least I have stopped drooling.

I am not alone. E-mail not only dominates our desktop, but thanks to remote devices like Blackberry, it can follow us anywhere 24 hours a day. With return receipts telling senders when messages are both delivered and read, we have become significantly more accountable to everyone above, below and around us in the chain of command. We have learned to use e-mail return receipts for much the same purpose as routing cover sheets on staff packages. The main differences, though, are that it is much easier to send e-mails than to send paper files. The e-mail system records all the distribution and delivery information automatically and allows multiple deliveries with a single transmission.

To describe e-mail as an enabling technology greatly understates its influence. It has unleashed a flood of communication unparalleled in human history. Where the telephone at one time supplanted text as the primary means of business communication, e-mail has brought text back on top with a vengeance. However, e-mail might also be described as a debilitating technology. Here's a trivia question for you: *Which will lower your IQ more, smoking marijuana or addiction to e-mail?* Cannabis reportedly lowers an average IQ by about four points.

But, according to research announced earlier this year by King's College London University, constant use of e-mail can lower a user's IQ by 10 points. An article, by Martin Wainwright, described the research in *The Guardian* (http://www.guardian.co.uk/online/news/0,12597,1465973,00.html). According to the article, *"Doziness, lethargy and an increasing inability to focus reached 'startling' levels in the trials by 1,100 people, who also demonstrated that e-mails in particular have an addictive, drug-like grip."*

"Respondents' minds were all over the place as they faced new questions and challenges every time an e-mail dropped into their inbox. Productivity at work was damaged and the effect on staff who could not resist trying to juggle new messages with existing work was the equivalent, over a day, to the loss of a night's sleep," according to the article.

The most telling point in the article was that respondents had an almost complete lack of discipline in handling e-mails and felt compelled to reply to each new message. Ironically, it has taken me an hour and a half to write the last five paragraphs because I have received eight e-mails, five of which I felt compelled to answer immediately, the other three were spam. Maybe they are on to something.

Through Thick and Thin

At this point in the discussion we should take a basic look at how e-mail systems work and how their operating principles affect their functionality. As with most computer-based applications, there are two main types of systems: thick client and thin client. In thick client, most of the processing is done on your PC. Most of us are familiar with Microsoft Outlook, Lotus ccMail, POP3 mail clients and similar products, which are specialized software applications loaded on a PC to manage e-mail accounts.

In thin client architecture, most of the data are processed centrally on a server and displayed on a PC. The most prevalent examples of this are Web-based mail systems where you access your account using a Web browser, e.g., Yahoo! Mail, Hotmail or Gmail. The e-mail server does all the heavy lifting, and the browser displays the results.

There are some services that support both thick and thin clients where you can access your e-mail either through a thick or thin client. For example, Yahoo! allows paid subscribers to use POP3 e-mail clients to retrieve their e-mail in addition to providing Web access to all account holders. Microsoft Outlook, the current household name in thick client e-mail, also has Web access functionality. Over the years there have been several shifts back and forth between thin client and thick client. In general, the ebb and flow between the two is regulated by yet another duality: processing power versus mobility.

Thick clients, so far, are more powerful and convenient than thin clients. The most obvious example of the power of the thick client is the ability to drag and drop objects. Click and hold on an e-mail to highlight it and then drag the mouse (or roll the trackball) to move the e-mail out of one folder and into another. You can also highlight and drag multiple files with one smooth move, clearly demonstrating the superiority of a thick client e-mail system over thin.

Then again, Web e-mail clients let you do essentially the same thing. Moving e-mail in the browser-based thin client system that I am currently using is as simple as adding check marks in boxes next to the items you want to move and then selecting the target folder from a drop-down menu. It takes me about the same amount of time as dragging and dropping without the ergonomic stress of having to hold down the mouse button while dragging.

The more sophisticated thick clients include integrated calendar and contact management features. Thick clients let you plug e-mail addresses into your message directly from your contact management address book. Thick clients automatically send e-mail reminders for scheduled tasks and appointments and let you view other people's schedules alongside your own.

Then again, I can do all that on my Yahoo! account through the Web browser. Yahoo! includes some fairly useful contact management features, including the ability to add any or all of the addresses from any message to my contacts list. I have used Yahoo!'s Web-based calendar for both personal and work appointments, including comparing schedules with my staff, because we do not yet have a thick client at work that includes a calendar. Even if we did, I would rather use a single calendar for my schedule and for access with equal ease from both work and home. Why keep multiple schedules when I can have just one that includes everything?

OK, maybe thick clients are more secure. They do get points in this area for raising the security bar if your e-mail system will only accept contacts from a particular client that has been customized for your organization. Most clients, thick and thin, are equally vulnerable to e-mail viruses like Melissa, I Love You, Sobig F and Sober.N because they target features in the computer's operating system, not just in the e-mail client. However, many of these viruses are tailored to take specific advantage of a thick client's direct access to its own e-mail address book to automatically send a new wave of infected e-mail.

Most computer security people I know will argue that thick clients are more secure. Most system administrators will tell me that they are more robust. However, I find myself using my Web client more and more for all my e-mail accounts because of convenience without any noticeable security problems. As history has shown, convenience usually wins out in the end, so once Hotmail, Yahoo! or Google starts offering Voice over Internet Protocol (VoIP) service to go with its e-mail, calendar, contact list and weather updates, the resulting thin client current may just be too strong to resist.

If I Had a Hammer

E-mail is the IT equivalent of a crescent wrench, a very useful tool that adjusts for a variety of nuts and bolts. Unfortunately, I believe in my crescent wrench so much that I often try to use it for tasks it is not well designed for.

Most of us are familiar with the semi-legendary "crescent hammer" that emerges when you have something that needs pounding and all you have handy is a crescent wrench. Fueled by desperation, unbridled optimism or sheer laziness we pound away with the wrench instead of dealing with the inconvenience or expense of finding the correct tool. Unfortunately, like the crescent wrench, e-mail is so pervasive that some people will try to use it for everything. Let's start by looking at what e-mail does well. E-mail is good if:

- *You want to send text.*
- *You need to send one or more attached files or links to files.*
- *You want to broadcast a message to a lot of people simultaneously.*
- *Your communication does not have to be real-time.*
- *You do not need immediate feedback from your recipient(s).*
- *You need to retain a copy of a message you have sent or received.*

E-mail is less effective as you move from these core competencies. For example, some people try to use e-mail as a poor man's workflow system to coordinate group discussions or staff work. Here are some of the basic principles of successful workflow:

What we need is a 12-step program for e-mailaholics …

- *The workflow process, including all actions and resources, should be both visible and transparent from beginning to end.*
- *Everyone should work from the same set of documents.*
- *Everyone, including team members who join in the middle of a project, should be able to see the work of everyone else at any point in the process.*
- *The workflow engine should centralize document and record management while allowing decentralized work by participants.*

Unfortunately, every e-mail system I have used, whether it has been on a mainframe, thick client or Web-based, suffers from the same basic problems preventing its effective use as a workflow system:

- *Because everyone has their own copy, no one can see anyone else's work until they are manually reconciled.*
- *Everyone gets their own copy of every message and attachments, which occupies a lot of storage space.*
- *All the e-mail files are stored in individual accounts, each of which may not include a complete set of documents associated with the workflow.*
- *Every new e-mail reply in a workflow iteration increases everyone's archive by the number of previous e-mails in the thread plus what was added. Even if the new comment is only, "Yes, that sounds good." you consume a lot of hard drive space with redundant information.*

Learning to distinguish between useful and not so useful can be difficult, particularly given the earlier comments about our tendency toward e-mail addiction. Yes, you can successfully complete simple, short workflows using e-mail. But, for any process that requires more than a few steps and participants, e-mail is best used only as a notification that there is work waiting for you in the system, and only if your portal or dashboard does not indicate this separately.

I am sure there are people who will disagree with me on this. But, unless you can show me how to run a large-scale business like eBay or Amazon using an e-mail system instead of a database as the primary workflow engine, you are not talking about true workflow.

Take Control of the Beast

In the introduction I made a passing reference to people who only check their e-mail twice a day. While it may seem that I was poking fun at them, I am actually envious that they have the self-discipline to tame their e-mail beast by refusing to jump every time it calls. What we need is a 12-step program for e-mailaholics:

1. *Schedule e-mail time like you do meetings. Check it at set times and for set periods.*

2. *Turn off your e-mail alert sound.*

3. *Prioritize. When you check your e-mail, delete the obvious junk first. Then read the informational messages and delete them. Then read and answer the ones that need answering. You will find it is easier to concentrate on the important stuff if the entire inbox is less cluttered.*

4. *Resist the urge to check for any new messages until you have cleared out all the current ones.*

5. *When your e-mail time is up, leave your e-mail alone and work or talk to people face to face.*

6. *When composing e-mail, if your message becomes longer than one message window can display, pick up the telephone and call the sender. If after making a phone call you still need to send an e-mail, send anything longer than one screen as an attachment with a summary in the body of the e-mail.*

7. *When you read an e-mail that makes you mad, do not start typing. If you must respond, pick up the phone (or walk) and talk to the sender. If you are angry or annoyed while drafting an e-mail, do not push the Send button right away. Save the draft of your e-mail, go home, get a good night's sleep, and read it again the next morning. If it still looks good, fire away, but nine times out of 10 you will change it.*

8. *Do not try to use e-mail as a conferencing or workflow system unless you are willing to accept its limitations for group work.*

9. *Choose an e-mail concept of operations that matches your organization's operation instead of forcing your organization to conform to what everyone else appears to be doing.*

10. *If you have a mobile e-mail device, turn it off if you are in a meeting, theater, the bathroom or any other place where having it beep might be embarrassing or annoying for you or those around you.*

11. *Do not check your work e-mail while on vacation. You will live a longer, happier life.*

12. *Repeat after me: "If it is really important, they will call me, not send an e-mail."*

Over the last 20 years we have gone from happily living without e-mail to miserable living without it. E-mail has brought a much greater ability to communicate and fundamental social and cultural changes. It has also consumed an unaccountable amount of money, time and resources. *But, it does not have to take over your life unless you allow it to.* We will continue the discussion of how to take control of the technologies that often control us in the next issue.

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.

In September 2001, the ESI was approved as a "quick hit" initiative under the DoD Business Initiative Council (BIC). Under the BIC, the ESI will become the benchmark acquisition strategy for the licensing of commercial software and will extend a Software Asset Management Framework across the DoD. 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: 30 Mar 06

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Collaborative Tools

Envoke Software (CESM-E)

Envoke 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

Click to Meet Software (CT-CTM)

Click to Meet Software - Provides software license and support for Click to Meet collaboration software (previously known as CUSeeMe and MeetingPoint), in support of the DoD's Enterprise Collaboration Initiatives. Discounts range from 6 to 11 percent off GSA Schedule prices.

Contractor: ***First Virtual Communications, Inc.*** (W91QUZ-04-A-1001)

Ordering Expires: 05 Nov 08

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 ESQL/C Development, IBM Informix ESQL/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 05

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Microsoft Products

Microsoft Database Products - See information provided under Office Systems below.

Oracle (DEAL-O)

Oracle Products - Provides Oracle database and application software licenses, support, training and consulting services. The Navy Enterprise License Agreement is for database licenses for Navy customers. Contact Navy project managers on the next page for further details.

Contractors:
Oracle Corp. (DAAB15-99-A-1002)
Northrop Grumman – authorized reseller
DLT Solutions – authorized reseller
Mythics, Inc. – authorized reseller

Ordering Expires: 31 Aug 05

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

www.it-umbrella.navy.mil

Special Note to Navy Users: On Oct. 1, 2004, and May 6, 2005, the Navy established the Oracle Database Enterprise License, effective through Sept. 30, 2013. The enterprise license provides Navy shore-based and afloat users to include active duty, Reserve and civilian billets, as well as contractors who access Navy systems, the right to use Oracle databases for the purpose of supporting Navy internal operations. Navy users in joint commands or supporting joint functions should contact Bill Huber, NAVICP Mechanicsburg contracting officer at (717) 605-3210 or e-mail William.Huber@navy.mil, for further review of the requirements and coverage.

This license is managed by the Space and Naval Warfare Systems Center (SPAWARSYSCEN) 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:

a. as part of a system or system upgrade, including Application Specific Full Use (ASFU) licenses;
b. under a service contract;
c. under a contract or agreement administered by another agency, such as an interagency agreement;
d. under a Federal Supply Service (FSS) Schedule contract or blanket purchase agreement established in accordance with FAR 8.404(b)(4); or
e. by a contractor that is authorized to order from a Government supply source pursuant to FAR 51.101.

This policy has been coordinated with the Office of the Assistant Secretary of the Navy (Financial Management and Comptroller), Office of Budget.

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/deal/Oracle/oracle.shtml

Sybase (DEAL-S)

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

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

Ordering Expires: 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 to include 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

Popkin (AMS-P)

Popkin Products and Services - Includes the System Architect software license for Enterprise Modeling and add-on products including the Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) Extension, which provides specific support for the U.S. Department of Defense Architecture Framework (DoDAF), Envision XML, Doors Interface and SA Simulator as well as license support, training and consulting services. Products vary from 3 to 15 percent off GSA pricing depending on dollar threshold ordered.

Contractor: ***Popkin Software & Systems, Inc.*** (DABL01-03-A-0001); (800) 732-5227, ext. 244

Ordering Expires: 12 Jun 06

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

Merant Products

Merant Products - Includes PVCS Change Management Software used to manage change processes in common development environments, release procedures and practices across the enterprise. All software assets can be accessed from anywhere in the enterprise. All changes can be entered, managed and tracked across mainframes, Unix or Windows platforms. The PVCS family also includes products to speed Web site development and deployment, manage enterprise content, extend PVCS to geographically dispersed teams and integrate PVCS capabilities into custom development workbenches.

Contractor: ***Northrop Grumman*** (N00104-03-A-ZE78); (703) 312-2543
Ordering Expires: 15 Jan 06
Web Link: http://www.serena.com

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); (960) 776-8283
Ordering Expires: 30 Jun 05
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, which is inclusive of software accumulation discounts. For maintenance, training and installation services, discount range is 3 to 10 percent off GSA. Credit card orders are accepted.

Contractor: ***ProSight, Inc.*** (W91QUZ-05-A-0014)
Ordering Expires: 19 Sep 06
Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Telelogic Products

Telelogic Products - Offers development tools and solutions which assist the user in automation in the development life cycle. The major products include DOORS, SYNERGY and TAU Generation. Licenses, maintenance, training and services are available.

Contractors:
Bay State Computers, Inc. (N00104-04-A-ZF13); Small Business Disadvantaged; (301) 306-9555, ext. 117
Northrop Grumman Computing Systems, Inc. (N00104-04-A-ZF14); (240) 684-3962
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 for 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 45.*

PeopleSoft

PeopleSoft - Provides software license, maintenance, training and installation and implementation technical support.

Contractor: ***PeopleSoft USA, Inc.*** (N00104-03-A-ZE89); (703) 364-2351
Ordering Expires: Effective for term of the GSA FSS Schedule
Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/peoplesoft/peoplesoft.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) 312-3571
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 DoDactivities. 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); (703) 885-6020
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

Symantec

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, 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 maintenance for numerous Adobe products, including Acrobat (Standard and Professional), Approval, Capture, Distiller, Elements, After Effects, Design Collection, Digital Video Collection, Dimensions, Frame Maker, GoLive, Illustrator, PageMaker, Photoshop and other Adobe products.

Contractors:

ASAP (N00104-03-A-ZE88); Small Business; (800) 248-2727, ext. 5303
CDW-G (N00104-03-A-ZE90); (877) 890-1330
GTSI (N00104-03-A-ZE92); Small Business; (800) 942-4874, ext. 2224

Ordering Expires: 30 Sep 05
Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/adobe/adobe-ela.shtml

CAC Middleware

CAC Middleware - Provides Common Access Card middleware.

Contractors:

Datakey, Inc. (N00104-02-D-Q666) IDIQ Contract for DATAKEY products; (301) 261-9150
Spyrus, Inc. (N00104-02-D-Q669) IDIQ Contract for ROSETTA products; (408) 953-0700, ext. 155
Litronic, Inc. (N00104-02-D-Q667) IDIQ Contract for NETSIGN products; (703) 905-9700

Ordering Expires: 6 Aug 05
Web Link: http://www.it-umbrella.navy.mil/contract/middleware-esa/index-cac.shtml

Microsoft Products

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

Contractors:

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) 502-2431
Hewlett-Packard (N00104-02-A-ZE80); (800) 535-2563 pin 6246
Softchoice (N00104-02-A-ZE81); Small Business; (877) 333-7638 or (703) 469-3899

Softmart (N00104-02-A-ZE84); (610) 518-4000, ext. 6492 or (800) 628-9091 ext. 6928
Software House International (N00104-01-A-ZE86); (304) 725-6110
Software Spectrum, Inc. (N00104-02-A-ZE82); (800) 862-8758 or (509) 742-2308

Ordering Expires: 30 Mar 07
Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/microsoft/ms-ela.shtml

Red Hat

Red Hat (formerly owned by Netscape) - 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, 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: Mar 06 (includes one one-year option)
Download provided at no cost.
Web Link: http://dii-sw.ncr.disa.mil/Del/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 SmartBUY 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 (SSTEW)

SUN Support - Sun Support Total Enterprise Warranty (SSTEW) offers extended warranty, maintenance, education and professional services for all Sun Microsystems products. The maintenance covered in this contract includes flexible and comprehensive hardware and software support ranging from basic to mission critical services. Maintenance covered includes Sun Spectrum Platinum, Gold, Silver, Bronze, hardware only and software only support programs.

Contractor: ***Dynamic Systems*** (DCA200-02-A-5011)
Ordering Expires: Dependent on GSA Schedule until 2011
Web Link: http://www.ditco.disa.mil/hq/contracts/sstewchar.asp

Research and Advisory 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: Gartner Group: 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

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:
28 Jul 05 for all CLINs/SCLINs; 28 Jul 07 for Support Services and Spare Parts

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

Direct Ordering to Contractor

SSC Charleston Order Processing: (757) 445-1493 (DSN 565)
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:

Control Concepts (N68939-97-A-0001); (800) 922-9259
Dell (N68939-97-A-0011); (800) 727-1100, ext. 61973
GTSI (N68939-96-A-0006); (800) 999-4874, ext. 2104
Hewlett-Packard (N68939-96-A-0005); (800) 727-5472, ext. 15614

Ordering Expires:
Control Concepts: 03 May 07 (includes two one-year options)
Dell: 31 Mar 06 (includes one one-year option)
GTSI: 31 Mar 06 (includes one one-year option)
Hewlett-Packard: 8 Oct 05 (includes two one-year options)

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:
Control Concepts
http://www.it-umbrella.navy.mil/contract/tac-solutions/cc/cc.shtml

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) 225-2412; Awarded 7 May 97; Ordering expires 31 Mar 06, with two one year options

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:

Lockheed Martin (N68939-97-A-0017); (240) 725-5012; Awarded 1 Jul 97; Ordering expires 30 Jun 06, with one one-year option

Northrop Grumman Information Technology
(N68939-97-A-0018); (703) 413-1084; Awarded 1 Jul 97;
Ordering expires 11 Feb 06, with one one-year option

SAIC (N68939-97-A-0020); (703) 676-2388; Awarded 1 Jul 97; Ordering expires 30 Jun 06, with one one-year option

TDS Inc., a Centurum Company (Small Business) (N00039-98-A-3008); (619) 224-1100; Awarded 15 Jul 98; Ordering expires 14 Jul 05, with two one-year options. Call the Project Management Office for extension date.

Authorized Users: All DoD, federal agencies and U.S. Coast Guard

Web Links:
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

TDS
http://www.it-umbrella.navy.mil/contract/itss/tds/itss-tds.shtml

The U.S. Army Maxi-Mini and Database (MMAD) Program Listed Below

The MMAD Program is supported by two fully competed Indefinite Delivery Indefinite Quantity (IDIQ) contracts with IBM Global Services and GTSI Corp. The program is designed to fulfill high and medium level IT product and service requirements of DoD and other federal users by providing items to establish, modernize, upgrade, refresh and consolidate system environments. Products and manufacturers include:

	IBM Global Services	GTSI
Servers (64-bit & Itanium)	IBM, HP, Sun	Compaq, HP
Workstations	HP, Sun	Compaq, HP
Storage Systems	IBM, Sun, EMC, McData, System Upgrade, Network Appliances	HP, Compaq, EMC, RMSI, Dot Hill, Network Appliances
Networking	Cisco, WIMAX Secure	Cisco, 3COM, HP, Enterasys, Foundry

Ancillaries include network hardware items, upgrades, peripherals and software. Services include consultants, managers, analysts, engineers, programmers, administrators and trainers.

MMAD is designed to ensure the latest products and services are available in a flexible manner to meet the various requirements identified by DoD and other agencies. This flexibility includes special solution CLINs, technology insertion provisions, ODC (Other Direct Cost) provisions for ordering related non-contract items, and no dollar/ratio limitation for ordering services and hardware.

Latest product additions include WiMAX Secure Wireless Networking and DolphinSearch Datamining Software.

Awarded to:
GTSI Corp. (DAAB07-00-D-H251); (800) 999-GTSI
IBM Global Services-Federal (DAAB07-00-D-H252); CONUS: (866) IBM-MMAD (1-866-426-6623) OCONUS: (703) 724-3660 (Collect)

Ordering: Decentralized. Any federal contracting officer may issue delivery orders directly to the contractor.

Ordering Expires:
GTSI: 25 May 06 (includes three option periods)
IBM: 19 Feb 06 (includes three option periods)

Authorized Users: DoD and other federal agencies including FMS

Warranty: 5 years or OEM options

Delivery: 35 days from date of order (50 days during surge period, Aug-Sep) No separate acquisition, contracting and technical fees.

Web Link: GTSI and IBM: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

CHIPS Article Submission Guidelines

CHIPS welcomes articles from our readers. Submit articles via e-mail as Microsoft Word or .txt file attachments to chips@navy.mil or by mail to Editor, CHIPS, SSC Charleston, 9456 Fourth Ave, Norfolk, VA 23511-2130. If submitting your article by mail, please send the article on disc with a printed copy. To discuss your article with a CHIPS editor, call (757) 444-8704 or DSN 564-8704.

Relate the subject matter of your article to information technology (IT) and how IT is helping to accomplish your command mission, improve services, perform a task or automate or enhance a process. Provide lessons learned from your experience. Our motto states: *"CHIPS: Dedicated to Sharing Information, Technology, Experience."* The theme of your article should meet the intent of our motto.

An article is more interesting when you can convey a personal experience; it is also easier to read. When writing use active rather than passive voice. Avoid technical terms that only a few readers would understand. Write out the full name or title before using an acronym the first time; thereafter, use only the acronym. Avoid using a myriad of acronyms throughout your article since they can be confusing to the reader.

Articles may contain illustrations. Do not embed photos or images in your MS Word document, please send them as separate file attachments. Make sure photos and illustrations add value to your article and are mentioned in the text. Please do not use Web-based or MS PowerPoint graphics because they do not have a high enough resolution to reproduce clear, quality illustrations in publication. Please save graphic files with a resolution of 300 dpi.

Please submit your article to your public affairs officer and chain of command for release authority before you submit your article to CHIPS.

While we do not require a standard length for articles, we prefer articles one to two pages in length. Typically, one magazine page equals two and a half pages of typed text using a standard 12-point font or approximately 700-1,000 words.

We reserve the right to edit articles, which is a necessary step in the production process. Our goal is to enhance your style — not change it. We use the Associated Press Stylebook, the U.S. Navy Style Guide and guidance from the Chief of Navy Information (CHINFO) for editorial management.

Subject matter experts review each article for technical accuracy and to ensure conformance to CHINFO guidelines. We may make changes to your article to conform to magazine production guidelines and the CHIPS style manual and format. If an article requires extensive changes, we will contact you.

CHIPS is published quarterly. Our deadline dates are: Feb. 1, April 1, Aug.1 and Oct. 1.

Thank you for your interest in CHIPS magazine.

DON IT
umbrella program

Thanks to our customers for 17 great years!

The DON IT Umbrella Program offers a full range of IT services and solutions to meet any requirement, including software, hardware, information assurance, project management, security, engineering, training, data warehousing, consulting and research. Using enterprise acquisition agreements translates into substantial cost avoidance savings for the Navy and Department of Defense.

ENTERPRISE SOFTWARE AGREEMENTS

- Business and Modeling Tools
- Collaborative Tools
- Database Management Tools
- Enterprise Architecture Tools
- Enterprise Resource Planning
- ERP Systems Integration Services
- CAC Middleware
- Research and Advisory BPAs
- Section 508 Tools
- Information Technology Support Services

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