

# CHIPS

magazine



APR-JUN  
2005



# MARITIME DOMINANCE



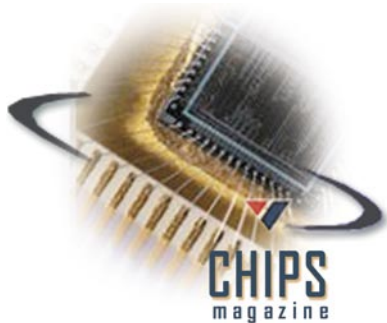
DEDICATED TO SHARING  
INFORMATION-TECHNOLOGY-EXPERIENCE

HNP April 1, 2005

**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 John W. R. Pope III**



**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](mailto:chips@navy.mil). We reserve the right to make editorial changes. All articles printed in CHIPS become the sole property of the publisher. Reprint authorization will be granted at the publisher's discretion.

Requests for distribution changes or for other assistance should be directed to Editor, CHIPS, SSC Charleston, 9456 Fourth Ave., Norfolk, VA 23511-2130, or call (757) 444-8704; DSN 564. E-mail address: [chips@navy.mil](mailto: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

*"When the nation invests in a Coast Guard boat, that single boat can save a life, catch a drug runner, bust a migrant smuggler, or patrol and protect a port, and can very quickly respond to any of those missions as an event occurs."*

Vice Adm. Harvey E. Johnson Jr.  
Commander, Coast Guard Pacific Area  
U.S. Maritime Defense Zone Pacific  
Regional Emergency Transportation  
Coordinator



Page 10

*"We intend to provide one-stop-shopping, to deter, prevent or — should it come to that — defeat attacks against our homeland, and help civil authorities mitigate situations that threaten our lives and our property when the Secretary so directs."*

Adm. Timothy J. Keating  
Commander, North American  
Aerospace Defense Command and  
U.S. Northern Command



Page 14

*"Maritime Domain Awareness is all about generating actionable intelligence, the cornerstone of successful counterterrorist and maritime law enforcement operations."*

Vice Adm. John Morgan  
Deputy Chief of Naval Operations Information, Plans and Strategy



Page 16


*"Successful companies have long understood that an effective human capital strategy provides a tremendous competitive advantage, and the leadership of our Navy-Marine Corps team recognizes that this is true in our world as well."*

Mr. David Wennergren  
Department of the Navy  
Chief Information Officer



# CHIPS Apr-Jun 2005

Volume XXIII Issue II

- 
- 4 **Editor's Notebook**  
By Sharon Anderson
- 5 **From the DON CIO**  
By Dave Wennergren
- 6 **Interview with Vice Adm. Harvey E. Johnson Jr.**  
Commander, Coast Guard Pacific Area  
U.S. Maritime Defense Zone Pacific  
Regional Emergency Transportation Coordinator
- 10 **USNORTHCOM**  
By Adm. Timothy J. Keating
- 13 **A Spectrum Fable: How AESOP and XML**  
Improve Naval Operations  
By Jack Gribben
- 14 **Enhancing Awareness in the Maritime Domain**  
By Vice Adm. John Morgan and  
Cmdr. "Bud" Wimmer
- 16 **Interview with Mr. David Wennergren**  
Department of the Navy Chief Information Officer
- 19 **Beyond Iraq**  
By Adm. Walter F. Doran
- 21 **Interview with Capt. Kevin R. Hooley**  
Commanding Officer  
Center for Information Dominance
- 24 **The DON IT Umbrella Program Turns 17!**  
By the DON IT Umbrella Program Team
- 26 **MBGIE 2005**  
By Sharon Anderson
- 29 **A Design Process for FORCEnet Experimentation**  
By Brad Poeltler and Dr. Shelley Gallup
- 32 **The Naval Personnel Development Command**  
Bringing Human Capital Strategy to Life  
By JO1(SW/AW) John Osborne
- 33 **FORCEnet Functional Concept ...**  
the future of Naval Warfare  
By JOC(SW/AW) Joseph Gunder
- 35 **DON CIP: A Comprehensive Solution to Improve**  
Cyber and Physical Security of DON Critical Assets  
By Donald Reiter
- 38 **Transformational Communications -**  
The Space Segment  
By the DON CIO Telecom/RF Spectrum /Wireless Team
- 40 **Scuzzy and Beyond - Part II**  
By Patrick G. Koehler and Lt. Cmdr. Stan Bush
- 42 **The Lazy Person's Guide to Internet**  
Hoaxes, Myths and Legends  
By Retired Air Force Maj. Dale J. Long
- 45 **Under The Contract**  
By the DON IT Umbrella Program Team
- 51 **CHIPS Article Submission Guidelines**

On the cover: The U.S. Navy amphibious assault ship, USS Nassau (LHA 4). U.S. Navy photo by PH2 Daniel J. McLain. A U.S. Coast Guard 25-foot Transportation Security Boat. The crew is patrolling the Port of Ash Shuaiba, Kuwait. U.S. Coast Guard photo by PA1 Matthew Belson.

## Editor's Notebook

The construct of maritime dominance contains many elements, and it includes much more than situational awareness of the world's seaports and oceans. Beginning on page 6, Vice Adm. Harvey E. Johnson Jr., Adm. Timothy J. Keating, Vice Adm. John Morgan, Cmdr. "Bud" Wimmer and Adm. Walter F. Doran, explore the many facets of maritime dominance and how the services and Department of Homeland Security are united in building maritime domain awareness across the globe.

The *CHIPS* assistant editor, Nancy Reasor, and I had a fascinating visit to the USS Kearsarge (LHD 3) and Tactical Training Group Atlantic (TACTRAGRULANT) for the Joint and Combined Multi-Battle Group Inport Exercise (MBGIE) in February. United Kingdom and U.S. joint forces replicated a composite warfighting scenario achieving an unprecedented dimension in virtual wargaming.

Thanks to the crew of the USS Kearsarge, Commander, U.S. Second Fleet and Capt. Mark Nesselrode, commanding officer of TACTRAGRULANT, and his staff for the opportunity to witness the strides the Navy is making in Strike Group training. Go to page 26 to read about MBGIE 2005.

Oh, to be 17 again – just like the Department of the Navy Information Technology (DON IT) Umbrella Program! This historic program has been bringing substantial cost avoidance savings for Navy and Department of Defense (DoD) customers for 17 years.

With our nation fighting a global war on terror, now more than ever, it is vital to save valuable resources to support the Department's warfighting mission. Go to page 24 for more information or visit online at <http://www.it-umbrella.navy.mil/>.

Welcome new subscribers!

Sharon Anderson



*Don't miss a single issue of CHIPS! To request extra copies or send address changes, contact CHIPS editors at [chips@navy.mil](mailto:chips@navy.mil) or phone (757) 444-8704, DSN 564 or fax (757) 445-2103, DSN 565.*



*Atlantic Ocean (March 26, 2005) – Sailors assigned to the Deck Department aboard the amphibious assault ship USS Kearsarge (LHD 3), watch as a Landing Craft, Air Cushioned, assigned to Assault Landing Craft Unit Four (ACU-4), enters the well deck carrying vehicles from the 26th Marine Expeditionary Unit (MEU). The 26th MEU is departing Camp Lejeune, N.C., for a regularly scheduled deployment in support of the global war on terrorism. U.S. Marine Corps photo by Sgt. Roman Yurek.*



*Norfolk, Va. (March 25, 2005) – Sailors aboard the USS Kearsarge (LHD 3) man the rails as the ship departs in support of the global war on terrorism. U.S. Navy photo by PHA Sarah E. Ard.*

*Several of the business warriors of the DON IT Umbrella Program (l to r) – Barbara Johnson, DON IT Umbrella Program Manager, Peggy Harpe and Margie Smith, assisting Umbrella customers at the Space and Naval Warfare Systems Command (SPAWAR) corporate exhibit for the AFCEA West conference in San Diego, Calif., February 2005. Go to <http://www.it-umbrella.navy.mil/> for more information about the Umbrella Program.*



We live in a networked world, and a networked Navy-Marine Corps team has become a reality. Information sharing with collaboration across command elements and national boundaries, coupled with increasing speed, accuracy and efficiency, characterize this 21st century network-centric environment.

Network-centric warfare creates a decisive warfighting advantage to sustain our continued maritime dominance. However, network-centric warfare also has the potential to expose vulnerabilities. Compromised identity of personnel, systems and services could be catastrophic in both strategic and tactical warfighting operations. Furthermore, the global war on terrorism is redefining network and data sharing boundaries. With the likely potential for those boundaries to continue expanding, Identity Protection and Management (IPM) becomes more critical as a means to support information sharing with authenticity and non-repudiation.

Identity protection, or safeguarding of identities, and the sensitive information that characterize people, systems and services, is a crucial capability in a network-centric warfighting environment. IPM enables the Department of Defense (DoD) to realize joint information superiority, both on and off the battlefield, and it will enable secure, integrated, interoperable and scalable information sharing solutions for people, systems and services in a network-centric warfare environment. Sound IPM must leverage the evolution and convergence of robust capabilities associated with biometrics, smart card, Public Key Infrastructure (PKI), Radio Frequency Identification (RFID) and other technologies, to positively assert and strongly protect trusted identities, processes and assets with integrity.

Our Department of Defense joint warfighting team has already made great progress on this front. Accomplishments thus far include:

- Issuance of over 4.5 million Common Access Cards (CACs) and over 14.5 million DoD PKI certificates
- Enablement of DoD Web sites to use Secure Socket Layer protocol for non-public communications
- Adoption of the FBI's Integrated Automated Fingerprint Identification System standard as the DoD method for collecting, exchanging and validating fingerprint biometrics data of detainees, enemy combatants, and persons of interest

The DON is expanding IPM initiatives to include enabling unclassified networks to support cryptographic logon from DoD PKI credentials stored on CACs, and requiring PKI credentials rather than passwords for Web site access. We are rapidly approaching a future where the information sharing that enables maritime dominance is secure and trusted.

Our commitment to a robust identity management solution across the Department of Defense will serve as the crucial foundation to achieve our vision of network-centric operations and knowledge dominance.

Dave Wennergren



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

# Vice Admiral Harvey E. Johnson Jr.

## Commander, Coast Guard Pacific Area

### U. S. Maritime Defense Zone Pacific

### Regional Emergency Transportation Coordinator



*Vice Admiral Harvey Johnson assumed the duties of Commander, Coast Guard Pacific Area in June 2004. The area of operations for the Pacific Area encompasses over 73 million miles west of the Rocky Mountains and throughout the Pacific Basin to the Far East. Prior to this assignment, he was the Commander, Seventh Coast Guard District and served as the Director, Homeland Security Task Force-Southeast, where he directed Operation Able Sentry, the Department of Homeland Security response to the crisis in Haiti. In addition to these duties, Vice Admiral Johnson served as the Executive Director of the Coast Guard's transition into the Department of Homeland Security (DHS), Director of Operations Capability and Director of Operations Policy.*

**CHIPS:** *Can you discuss the Coast Guard's homeland security mission in terms of the greater role the USCG now has in national defense?*

Vice Adm. Johnson: The Coast Guard is designated as the lead federal agency for maritime homeland security. This has become a visible representation of our contribution to the safety and protection of America. Maritime Security now stands alongside search and rescue as primary missions for the Coast Guard and demonstrates that we are a multi-mission service. So, while we bring a sharp operational focus to maritime security, we continue to meet the American public's expectations to protect domestic fisheries and the marine environment, prevent illegal drug and alien migrant flow, and provide service aids to navigation, along with all our other missions.

The Coast Guard has new responsibility and authority to meet the challenges of maritime security. Passage of the Maritime Transportation Security Act (MTSA) of 2002 expanded Coast Guard authorities to require security plans from ships that trade with our nation as well as for the maritime facilities in our ports. The Act also established Coast Guard Captains of the Port as Federal Maritime Security Coordinators. This mission fits well with the Coast Guard because we have a lot of experience in working with federal, state and local agencies, DoD, the maritime industry and the public.

We have also added new capabilities. For example, we have added almost 4,500 people, acquired new patrol boats, and new response boats, and commissioned 13 Maritime Safety and Security Teams (MSSTs). MSSTs consist of small boats and crews specially trained in maritime security tactics. Within these teams, we have — for the first time — an undersea detection capability, with divers and specialized sensors to scan piers and other structures to ensure that facilities and moored vessels are safe.

The MSSTs also have canine teams that can detect the presence of explosives. We have fielded Sea Marshals and have new vessel and facility inspectors. We have greatly expanded our partnerships with federal, state and local agencies as well as those in the maritime industry. When you add all of these capacities together, you can understand how the Coast Guard has helped to bring about a far greater level of safety and security in our maritime environment since 9/11.

**CHIPS:** *Are these new capabilities part of your transformation process?*

Vice Adm. Johnson: That's an interesting question. Transformation generally connotes a fundamental change in an organization's approach to a task, perhaps transforming from one paradigm to another. In that respect, I view the changes the Coast Guard is experiencing as more of an adaptation than a transformation, as we adapt to a more aggressive readiness posture to meet the challenges of maritime security.

One of the strengths of the Coast Guard is that we maintain a broad set of organizational competencies and are flexible enough to adapt them to rapidly meet the emerging maritime safety and security needs of our nation. Over the past few years, we have drawn on our law enforcement and maritime safety competencies to very quickly acquire and employ the new capabilities that we just discussed. We then took the same approach to adapt vertical insertion and armed helicopters from drug enforcement to the broader challenge of maritime security. I think that is one reason the American people find such value and ascribe such credibility to the Coast Guard.

**CHIPS:** *How does the Coast Guard's mission complement the U.S. Navy's role in maritime defense?*

Vice Adm. Johnson: The Coast Guard's maritime homeland security mission and our maritime homeland defense responsibility are complementary to the Navy's maritime homeland defense responsibilities. This is so by design, and by more than a century of practice between our services in meeting maritime challenges.

Our service chiefs, Admiral Collins and Admiral Clark, are leading us in implementing a National Fleet concept. This is a concept that was initiated by their predecessors, but one they have taken to a new level. It essentially recognizes the value of a synergistic relationship between the Navy and Coast Guard such that we work together expressly to pursue a course of building and sustaining complementary capabilities.

We each harbor specific assets, capabilities and competencies that, together, meet the full spectrum of the nation's maritime requirements. We work well in either a supporting or supported relation-

ship and understand and manage the seams between those roles very well. For example, one of my strongest partners in providing maritime security in the Pacific area is Admiral Mike McCabe, commander of the Third Fleet.

Conversely, I stand ready to assist Admiral McCabe in meeting his maritime defense responsibilities. And our relationship is more than just that of a wiring diagram or abstract organizational plan. Admiral McCabe and I confer frequently on a personal level and our staffs talk, plan and act together every day. We have total visibility of our combined forces, so that if a maritime event occurs in the Pacific area, Admiral McCabe and I will work collectively. Whether the mission is homeland security or homeland defense, we must cooperate to ensure we bring the right capability to bear.

You will find the same relationship in the Atlantic between the Coast Guard's Atlantic Area and the Navy's Second Fleet. So, across the Atlantic and Pacific, the Coast Guard and Navy have created a complementary relationship with visibility of appropriate chains of command, which for homeland defense is under the operational control of Admiral Keating at U. S. Northern Command. All of this reflects a well-constructed command and control structure that Admiral Keating has worked hard to formalize, exercise and refine so that the nation will be secure in all domains, maritime as well as air and land.

*CHIPS: Can you discuss the USCG Maritime Strategy?*

Vice Adm. Johnson: Shortly after 9/11, the commandant directed development of the Coast Guard's Maritime Strategy for Homeland Security because he saw a need to provide a clear sense of strategic direction to strengthen security within the maritime domain. The nation was rightfully laser-focused on enhancing aviation security, and we had not yet concentrated on maritime vulnerabilities.

This visionary document brought synergy and alignment from a number of different and complementary views on the steps required for the Coast Guard to set a true course. We are conducting enhanced maritime security operations with new capabilities and with far greater capacity than we had a short time ago. The nation and the world maritime community, following a port-by-port round of vulnerability assessments, have taken positive steps to close port security gaps.

We have leveraged partnerships across the board with significant results in mitigating security risks. All of these efforts resulted in enhanced readiness to meet maritime security challenges. While we have made progress in building essential capabilities and competencies, there is still some distance to go to meet the maritime security expectations of the American public.

Dec. 21, 2004, President Bush signed the National Security Presidential Directive 41/Homeland Security Presidential Directive 13 (NSPD 41/HSPD 13) that tasked the Department of Defense and the DHS to jointly prepare a Maritime Security Strategy for our nation. The President doesn't sign many Presidential Directives, but by signing this one he raised maritime security to the center stage for our nation. He set an aggressive time line for a deliverable within 180 days. Teams of talented people from both Departments are working very hard to make that deadline. They will develop an overall

strategy as well as a family of supporting plans that focus on elements essential to meeting the strategy's objectives. I think these teams are better positioned for success because of the initiatives taken and thought generated by the Coast Guard's strategy.

*CHIPS: Can you discuss the role that the USCG Research & Technology Center is playing to increase the effectiveness of the Coast Guard?*

Vice Adm. Johnson: The Coast Guard's Research and Development Center has been very successful in supporting the fast pace with which we have embraced our new mission challenges. I have worked with them over the years and appreciate their unique talent for understanding our operational requirements from the field perspective, and scouring the full range of potential technological solutions, and then being creative in finding ways to bridge between the two: adapting existing and near-term technology to help solve emerging operational challenges.

Now that we are part of DHS, our R&D Center falls under the DHS larger umbrella of the Science and Technology Directorate, and that has expanded the horizons across which our staff can scan technology. This has brought tremendous new resources and you don't need to look very hard to see evidence of success. In Miami, the center brought together a number of surveillance systems, which serve as a baseline for command center integration of sensor technologies. They are examining radiation detection and explosive detection equipment to find the right combination for the maritime environment. In other areas ranging from ferry security and swimmer interdiction to risk modeling and human system integration, they are finding ways to guide the Coast Guard in more effective mission performance.

*CHIPS: Can you talk about the new Coast Guard vessels and specialized maritime and security units?*

Vice Adm. Johnson: Let me focus on three aspects that I think tell a representative story about how our capabilities strengthen the nation's homeland security posture. The first is our 13 new MSSTs. Each unit is comprised of 75 professional men and women who operate their new homeland security boats in our most significant ports and waterways. They are deployable on short notice anywhere in the United States, and have even been deployed overseas to the waters of other nations.

MSST personnel are highly trained in law enforcement waterborne tactics, use of force with both lethal and non-lethal weapons, and they employ specialty capabilities such as canine handling, undersea security, vertical insertion and radiation detection. On a typical day, they will spend a preponderance of the 24-hour period on the water conducting surveillance patrols, escorting vessels, enforcing security zones and providing a deterrent presence. These teams provide so much visibility that I think they are a major reason that many people feel confident about our maritime security.

Not quite as visible, but equally important at emphasizing the element of prevention of attack, we have a whole new cadre of vessel and facility inspectors. These folks are also highly trained and expertly knowledgeable about all of our new MTSA vessel and facility security regulations and requirements. They board foreign flag vessels, often miles out to sea, and conduct verification examinations

to ensure that each vessel complies with our comprehensive new security requirements. They also board marine facilities in our ports to work with facility owners and operators to ensure that the required level of security, mariner credentialing and contingency planning have been completed. These are the people who make certain that commercial cruise ships are safe and that vulnerability is mitigated. They do this every day, at all hours of the day. These teams of inspectors offer visibility and convey a reason to feel confident about our maritime security.

As the third aspect, we focus not only on new vessels and capabilities, but also on the many current capabilities of our stations, air stations, patrol boats, aids to navigation teams, buoy tenders, large cutters and all of the other Coast Guard forces that continuously stand ready in a prevention and response posture to perform whatever mission may come their way. For example, while many Americans have seen a significant increase in Coast Guard presence in our ports and coastal approaches, a significant element of our National Homeland Security Strategy is to press the borders out to engage threats as far from our shores as possible.

The Coast Guard does this every day with our cutter fleet and long-range aircraft. Our young Coasties man 38-year-old cutters from the Bearing Sea in Alaska to the Eastern Pacific off the coast of Colombia, throughout the Atlantic and into the Caribbean Sea and even to the Persian Gulf. They detect, deter, interdict and defeat threats posed by those who would like to exploit the maritime domain for illegal purposes. This challenge will be made easier over the next couple of decades as our Deepwater project begins to replace aging and obsolescent platforms with new and more capable assets. But the point is, all of the Coast Guard, new and old is keenly intent on meeting the nation's maritime challenges.

*CHIPS: Can you talk about Coast Guard interoperability with the other services and federal, local and state agencies?*

Vice Adm. Johnson: I was hoping you would get to that issue. Interoperability is so very important to ensuring that we have a coordinated and effective presence of all maritime capabilities in the threat environment. I'll mention two aspects. First, interoperability presumes we know whom we need to work with, so we're talking about identifying key partnerships with agencies across the federal, state and local spectrum as well as those in the maritime community and with the public.

One of the primary vehicles for this is the Area Maritime Security Committees that have been established in each of our major ports as required by the Maritime Transportation Security Act of 2002. These committees have been formed under the leadership of our Captains of the Port acting in their new roles as the Federal Maritime Security Coordinators. Each committee has prepared an Area Maritime Security Plan that has been approved, and we are now in the process of beginning to exercise those plans. Of course, the action to write and execute a plan is an excellent process to wring out any areas of non-interoperability and fix them.

The second issue is to address the elements of interoperability with our partners and resolve any gaps. That is sometimes harder to do because it requires resources to adapt communications systems, integrate databases and bring into alignment differing processes

of planning and execution. There are a number of excellent initiatives that are helping to eliminate gaps. The most significant is the recent DHS requirement that all agencies begin to use the National Incident Management System (NIMS) as a process for organizing and conducting incident response. We are working with other agencies on a range of other command and control capabilities to increase the degree of interoperability across the board.

*CHIPS: Does the Coast Guard participate in exercises with the other services and coalition forces?*

Vice Adm. Johnson: We certainly do. We have always followed an aggressive exercise regime for oil spill response as well as participating in military defense exercises on a national and international scale. The oil spill regime took on a greater degree of fidelity following the Exxon Valdez catastrophe. And as I mentioned, we will soon begin an aggressive exercise regime in each of our major ports as they begin to exercise their Area Maritime Security Plans. On a national scale, U.S. Northern Command will soon conduct TOPOFF 3, a multiregional exercise that will test response capabilities and command and control structures. Several of these vignettes will have a maritime nexus and will involve a number of federal, state and local maritime agencies working together under some very challenging situations.

Here on the West Coast, the Pacific Area and the Navy's Third Fleet will sponsor Exercise Lead Shield/Rogueux in the Port of Los Angeles – Long Beach in May. This will involve federal, state and local agencies as they work with maritime partners to evaluate our ability to respond to a homeland security threat scenario in a major port. There will be exercises coming up in August in Alaska where we will work with DoD services to test our response capabilities. And, we will exercise later in the year with some of our international Pacific Rim partners. So as you can see, exercises are a very important element in maintaining readiness for the Coast Guard as well as for creating broader collective maritime security capabilities.

*CHIPS: Can you talk about how Coast Guard training and doctrine have changed to meet your new mission requirements since 9/11?*

Vice Adm. Johnson: One of the threads that runs through my responses to your questions is the degree to which all of our Coast Guard forces — and I mean all to include our boat forces, marine safety offices and aids to navigation teams and others — have attained a heightened homeland security response posture. We have more armed Coast Guard forces, boats and people in our domestic ports and coastal approaches now than at any time in our recent history, likely since World War II.

Our boat forces are still being trained in high speed, tactical operations. Some of our helicopter crews are being qualified in aviation use of force tactics and outfitted with weapons for fire support. We have boarding teams skilled at vertical delivery for some of the most challenging homeland security scenarios. Many of these skills are not just employed in domestic ports, they also have expeditionary capabilities such as the patrol boats and Law Enforcement Detachments deployed to the Persian Gulf. So when you put all of this together, you can see that the nature of our operations and our operational environment have changed significantly since 9/11, and so have our capabilities and supporting training and doctrine.



*CHIPS: Has the Coast Guard increased in size?*

Vice Adm. Johnson: I am pleased to say that the Coast Guard has grown in size in the last three years at a pace almost as fast as our mission growth. The President, former Secretary Ridge, and now Secretary Chertoff, have been very strong advocates for the Coast Guard. And, the Congress has responded. We have grown by more than 4,500 people in the last three years to a force size of approximately 42,000. While still not a huge number of people given our broad mission requirements, this is a significant step in the right direction.

This rapid growth has presented a number of challenges for us. As you know, our system brings people in at the entry level and they gain experience through formal training and through engagement in various operational missions. None of the needed experience comes overnight. So we have a lot of junior people who are working hard to learn and gain seasoning as fast as they can. And, we have a lot of senior people who are taking more time to nurture and mentor the junior folks to bring them along faster to meet our mission requirements. This would be a more significant challenge were it not for the quality of people we have in the Coast Guard today. I have to tell you that it is inspiring to go out and visit our operational units and witness these fine young people in action. They are positive, engaged and proud of what they do.

*CHIPS: In terms of recruiting, what types of people are attracted to serving in the Coast Guard?*

Vice Adm. Johnson: The Coast Guard attracts bright young people who want to serve their country by accomplishing one or more of the exciting missions they see in our military, multi-mission, maritime service. The Coast Guard has core values of Honor, Respect and Devotion to Duty. We attract people who affinitize to those values. And we serve all of America, so we attract people from all aspects of American society to meet our diversity objectives to look like the America we serve.

As I mentioned a few moments ago, our people are just fantastic. They are highly trained; they are highly educated. They want to do good for America. They're loyal and they're patriotic. Just by nature, a Coast Guard member wants to help other people. They come into the Coast Guard because of our broad safety and security mission. They see rescue swimmers and lifesavers; they see maritime security boats and port security experts. They see that we protect the environment. They see our large cutters deploy to enforce fishery laws and bust drug and migrant smugglers. They want a piece of the action. And on an almost daily basis, they get to participate in interesting missions and challenges.

I tell our young people that there has never been a better time to be in our service. We are more visible and appreciated by America than at any time in my 34 years of service. We have new equipment and good training as we have discussed. And, we are beginning to see the entry of new equipment and systems from our Deepwater project that will transform our capacity and capability to meet the maritime requirements of our nation. Just last week, Secretary Chertoff and the commandant presided at the keel laying ceremony for our National Security Cutter, the first of many Deepwater cutters that will replace our 38-year-old High Endurance Cutters.

We are a key component in the new Department of Homeland Security, which is increasingly providing value for the nation as it draws together 22 different agencies. And we are on the cusp of implementing the President's evolving National Maritime Security Strategy. It is an exciting time to be in the Coast Guard, and we are attracting talented people motivated to meet these challenges.

*CHIPS: I read that the Coast Guard responded to the tsunami disaster in Southeast Asia, delivering over 350,000 pounds of food, medical supplies, water purification equipment, assessment teams, and even toys to the tsunami-stricken countries of Sri Lanka, Malaysia, Indonesia, and Thailand. I am just stunned by how much the Coast Guard mission has expanded and how well it responds.*

Vice Adm. Johnson: Our mission portfolio has expanded, a reflection I think of the growing appreciation for the importance and the particular challenges of the maritime domain. You are not unlike a lot of people who for one reason or another have viewed the Coast Guard through the lens of just one of our missions. Then, when exposed to the full range of our missions are impressed and appreciative.

We believe we provide a good return on investment for the American taxpayer. When the nation invests in a Coast Guard boat, that single boat can save a life, catch a drug runner, bust a migrant smuggler, or patrol and protect a port, and can very quickly respond to any of those missions as an event occurs. And we leverage that investment because of the leadership role we play with other federal, state and local agencies, the maritime community and the public. While I'll admit that I'm a bit biased, I think the Coast Guard is an amazing service. And most people who join the Coast Guard love it for that reason.

*CHIPS: All Americans have a deep appreciation for the Coast Guard. Just think about the statistics. Today, the Coast Guard will: save 15 lives; assist 117 people in distress; protect \$2.8 million in property; interdict 30 illegal migrants at sea; conduct 90 search and rescue cases; seize \$21 million worth of illegal drugs; respond to 11 oil and hazardous chemical spills and board and inspect 122 vessels. You are heroes, and you prove it every day.*

Vice Adm. Johnson: Thank you for your love of the Coast Guard, but more importantly, thank you for your support of the Coast Guard through the service and information you provide to Coast Guard people and to the public at large.

*CHIPS: Would you like to do a roll call of the diversity of your mission in closing?*

Vice Adm. Johnson: Maritime Safety, which includes search and rescue, marine safety, recreational boating safety, international ice patrol, port security. Maritime Mobility, including aids to navigation, icebreaking services, vessel traffic/waterways management, bridge administration, rules of the road. Maritime Security, including drug interdiction, alien migrant interdiction, marine resources preservation. General Maritime Law Enforcement, including law/treaty enforcement. National Defense, including general defense duties, homeland security, port and waterways security, marine pollution education, foreign vessel inspections, and marine and environmental science.

CHIPS

# USNORTHCOM

The Department of Defense established U.S. Northern Command in 2002 to consolidate, under a single unified command, existing missions that were previously executed by other military organizations. USNORTHCOM's mission is homeland defense and civil support, specifically:

- Conduct operations to deter, prevent, and defeat threats and aggression aimed at the United States, its territories and interests within the assigned area of responsibility.
- As directed by the President or Secretary of Defense, provide military assistance to civil authorities including consequence management operations.

U.S. Northern Command plans, organizes, and executes homeland defense and civil support missions, but has few permanently assigned forces. The command is assigned forces whenever necessary to execute missions as ordered by the President. Approximately 1,200 uniformed personnel (representing all service branches) and civil service employees provide this essential unity of command from U.S. Northern Command's headquarters at Peterson Air Force Base in Colorado Springs, Colo.

Admiral Keating assumed command of the North American Aerospace Defense Command and U.S. Northern Command Nov. 5, 2004.



Adm. Timothy J. Keating  
Commander, North American  
Aerospace Defense Command and  
U.S. Northern Command

... The need for transformation is hardly new ... Pointing at the bad guys and saying, "You're not fighting fair" has nothing to do with winning the fight ... Transformation is about organizing and equipping to beat today's and tomorrow's threats.

On Sept. 11, 2001, the hijackers had knives that they knew they could get through airport security. They gained access to the airliner cockpits because the cockpit doors at that time were flimsy and pretty easy to enter. The terrorists then took over the airplanes. Some had trained here in our schools, and *just* to a degree sufficient for their purpose. Three of the aircraft made it to their targets, killing thousands.

Neither the Federal Aviation Administration (FAA) nor the North American Aerospace Defense Command (NORAD) was organized or trained for shooting down domestic airliners. One group of hijackers failed to reach their target, either the Capitol Building or the White House, because brave passengers, with sufficient information, said "Let's roll" and were able to counterattack.

Now, as much as the military promotes unity of command, on that day we didn't have it for the military defense of our homeland. Why is that? If you will re-

member, we just did not think we needed it. Now we know we do.

On that Tuesday morning Sept. 11, a gorgeous day in New York and Washington, it started out as just another day for NORAD. Canadians and Americans were watching the skies and space beyond our continent for potential threats. We were looking outward. But it became tragically apparent that we could no longer focus only on those external threats. We had to start looking inward — and in a hurry.

Today, we do. The FAA and NAV CANADA interior radars now feed our air defense sectors. We launch jets when we see a problem. If a hijacking should become evident, we are not still sitting on the bench. We are going to engage directly, coordinating closely with the FAA and other relevant agencies.

We now have formidable, layered air defenses around the National Capital Region. It is an integrated air defense system including NORAD fighters, Department of Homeland Security jets and helicopters, and ground-based missiles, a good number of them, all closely coordinated with the FAA and other agencies.

We have NORAD aircraft on alert or con-

ducting irregular patrols all over the country, seven days a week, 24 hours a day ...

NORAD has flown almost 40,000 Noble Eagle sorties to protect Canadian and American airspace with not one severe mishap or accident. That's a credit to the people in NORAD and the young men and women who are doing the heavy lifting in the field. About three-quarters of the sorties have been flown by Air National Guard and Reserve forces. We are proud of that.

We want potential terrorists to know that they are not going to succeed. But you need to know that when we put an armed jet behind a civilian aircraft, our choices, by that point are limited, and they are not pleasant. If it's an airliner that has been hijacked and it's full of innocent passengers, we are already in trouble because other security measures have failed.

I recommend that we not kid ourselves. The noble passengers on United Flight 93 that day over Pennsylvania did what they had to do. We, in NORAD, will do everything we can to prevent a similar circumstance. But there could come a time when you, as a private citizen, traveling in an airplane, may have to step up to defend yourself.

It is not convenient to stand in a long line at the airport. But our airport security is a critical part of our nation's defense against terrorists. Those security personnel are just one part of a very complex, elaborate and sophisticated system that is structured to do the important job of identifying potential threats before those threats can do any harm.

NORAD armed jets are not the first option for dealing with hijackers; those fighters are just about the last option. But it is an option that we have today that we didn't have before 9/11. Fighting terrorists is a lot more than just organizing and training ourselves to handle a 9/11 situation better. And that leads us to your U.S. Northern Command.

On Sept. 11, the President and the Secretary of Defense had multiple commanders to talk to throughout the Defense community. Shortly after that they created one unified, regional combatant command for homeland defense. Just like the European Command, the Pacific Command or the Central Command, except there's one big difference: Northern Command's job, since its activation in October 2002, is to defend our homeland and to provide support to civil authorities whenever directed by the President or Secretary of Defense.

At U.S. Northern Command, I report to the Secretary of Defense, not the Secretary of Homeland Security. We intend to provide one-stop-shopping to deter, prevent or — should it come to that — defeat attacks against our homeland, and help civil authorities mitigate situations that threaten our lives and our property when the Secretary so directs.

Homeland defense doesn't mean we're just sitting around staring at our borders every day. We are as much *or more* interested than any other military command in what goes on around the world, in anything and everything that might be aimed at threatening Americans here at home. We want our fellow combatant commanders and interagency partners to capture or kill terrorists, before they come our way. We want this to be an *away* game.

While homeland defense is job number one, defense support of civil authorities takes a good deal of our effort, day-in

and day-out. At all times we are poised, dressed out, on call, ready for orders from the President or the Secretary. We will do this in support of a primary or lead federal agency. It could be the FBI, Department of Homeland Security, even the National Interagency Fire Center in Boise, Idaho.

We do not do any of this uninvited or without top-down direction. We are not going to ride into town, as you see in the movies, saying to local officials, "Step aside boys, there's a new sheriff in town." Everything we do at Northern Command is by law, under the Constitution we swear to protect. And everything we do is part of a broader national security team.

A lot of folks seem to fall into one of two groups when they think about Northern Command: those who are afraid we will read their mail and spy on them, and those who fear we won't have enough authority or assets to do our job.

First, we are not allowed to collect intelligence, and we do not. We do not spy on anyone in the United States or Canada. Second, I assure you, we do not need to change statutory limitations, including the Posse Comitatus Act, to do our job. Why is that?

In this national team effort, we don't need the authorities that are already resident in federal, state and local law enforcement agencies and the U.S. Coast Guard. The Coast Guard is both a law enforcement agency and one of our five armed services upon whom we depend heavily and with whom we work closely at Northern Command. Northern Command supports these partners as directed and under law.

Your U.S. Northern Command is composed of people from all five military services, National Guard, Reserves, many fine civil servants and a fair number of contractors. Defending our homeland is not a new job. The National Guard and the Coast Guard have long and valuable experience doing just that, and we are capitalizing on their experience in every way that we can.

You may be familiar with the massive changes under way in our Coast Guard. The National Guard is also transforming its homeland defense role. In addition to providing a good number of the U.S. forc-

es currently deployed to Iraq, the National Guard is building toward the 55 individual weapons of mass destruction civil support teams authorized by Congress for our states and territories. We have 32 of them in existence, trained and equipped. Twenty-three more have been funded.

In addition, on their own initiative, 12 states have formed larger Guard teams, made up of about 100 highly trained personnel, for enhanced assistance to citizens in the event of a weapons of mass destruction incident. So, you might be asking, what does Northern Command have, and what does it really do? We have very few assigned forces at our disposal every day.

But we can draw on the huge resources of the entire Department of Defense, everything from battalions that can fight forest fires to airlift and staging bases for Federal Emergency Management Agency (FEMA) disaster-responders; from satellite pictures of floods to C-130s that drop fire retardant; from Marines highly trained to detect ricin and anthrax on Capitol Hill to bomb dog teams that help protect the U.N. General Assembly. We can reach out and get all of that and much more.

At our headquarters in Colorado Springs, we have a Combined Intelligence and Fusion Center, a unique combination of talented professionals and sophisticated capabilities focused on sharing information and analysis with intelligence and law enforcement agencies ... the whole gamut: FBI to CIA; National Security Agency (NSA) to the Coast Guard; from the National Counterterrorism Center in McLean, Va., to the counterintelligence field activity that includes both American and Canadian experts.

We use this Intelligence and Fusion Center with resident experts and representatives from many agencies via an extensive secure digital network. We are watching and sharing analysis on subjects from rogue state missile activity, attempts to procure weapons of mass destruction, to the travel of known or suspected terrorists from one country to another.

We are intent on staying one step ahead of the bad guys, and we work hard with our interagency partners. If our job is to

defend you, you understandably expect us to be pretty good at our job. We think we are. More importantly, we are working hard to get better.

Also in Colorado Springs, we've established a Standing Joint Force Headquarters-North, a staff led by a general officer, focused on current events and ready to deploy on short notice to provide or support incident management leadership in the 48 contiguous states and Alaska. This portable headquarters has full-spectrum military and civilian communications capability — an impressive vehicle that we roll onto a C-130 that is always on alert.

At Fort Monroe, Va., we have our Joint Task Force Civil Support focused on incident management support to civil authorities if a terrorist uses a weapon of mass destruction. We have seen anthrax and ricin used in our country, so we know that this is a very real and formidable threat.

We have also formed a Joint Force Headquarters for the National Capital Region, to focus the efforts of all the armed services in protecting the seat of our federal government. For example, our command center in Colorado Springs had chat rooms linked with more than 120 agencies during the President's State of the Union Address. Last year, the system did not exist.

In Texas, we have established a Joint Task Force North, expanding on our 16 years of military support to more than 430 different federal, state and local law enforcement agencies fighting illegal drugs. They also address a broader counterterrorism issue we have learned: Today, drug smugglers and terrorists have more in common than they did five years ago.

We are working closely with the National Guard to dual-hat Guard officers as joint task force commanders, so they can simultaneously command state and federal troops in support of major events. We have used this dual-hat structure to great effect for the G8 Summit, both political conventions, Operation Winter Freeze along the Canadian-U.S. border and the state funeral of President Reagan.

We also sent forces to Jacksonville, Fla., for the Super Bowl. A lot of forces have been

deployed for your protection, most of which you did not see.

We have created a Technology Partnership Council with the Department of Energy, its national laboratories and other leaders in science and technology to make sure that there is cooperation among agencies in supporting the technological advances that will help us do our job in protecting you.

We have joined with nearly 100 academic institutions to build a Homeland Security and Defense Education Consortium to help grow the intellectual capital we need to defeat global terrorism.

U.S. Northern Command assisted other federal agencies in hurricanes, wildfires, the Space Shuttle Columbia tragedy, domestic terrorism events like the National Capital Region snipers and ricin in the Senate offices. And we have responded to increased national alert levels dictated by the Secretary of Homeland Security.

We have conducted seven major exercises that have helped us earn our spurs as a major combatant command. To date, 115 federal, state, local, tribal [Native American] and multinational organizations have participated, including seven of the 10 FEMA regions, and we have conducted field-training exercises in seven separate states. Our exercise program is completely interwoven with the Department of Homeland Security's national exercise program; and we participate frequently in unilateral exercises as a coordinated team. You should expect nothing less as taxpayers.

In support of the U. S. Strategic Command's global integrated missile defense mission, we are preparing to provide command and control for the initial ground-based mid-course missile defense of our homeland.

At NORAD and U.S. Northern Command, we are doing much that is new. We grow into solutions with hard work and experience. Now, it is naïve to think that you can purchase answers. So we are not going to over-invest in unproven technologies or new approaches. We always try to think big initially, start small, and scale as fast as necessary.

We work with many other partners: fed-

eral, state and nongovernment organizations, such as the Red Cross and private industry. On any given day at Northern Command, we have 59 resident representatives from other agencies. They are available full-time, working in [or near] our headquarters.

More than ever before, we are redefining jointness and interoperability. It is not a good idea to shake hands for the first time and exchange business cards at the scene of a disaster site. So we are spending a lot of time working across the interagency community to form new important partnerships.

Critical to our work is the sharing of intelligence and information. Every day, we analyze all sorts of intelligence data to understand what terrorists are doing, and to lead-turn upcoming seasonal and national events. For example, you may not be able to predict a hurricane or a forest fire, but you can predict hurricane and wildfire seasons. And, at the macro level, you can prepare for them. That is also what we are trying to do in our global war on terror.

Those of you in business [like us] do not like surprises. In defending our homeland, we do not care for them one bit. Since private businesses own 85 percent of the critical infrastructure in America, and since businesses are hit by disasters too, and since industry produces the vast majority of our equipment, we are very interested in partnering with business.

General Omar Bradley once said, "Wars are won by the great strength of our nation, the Soldier and the civilian working together." If your command or company has an idea or product that you think could help us defend our homeland or support civil authorities, we are anxious to talk to you.

Let us all remember that today we are a nation at war. Our fight against terror will be a long one, fought against an enemy with no desire to negotiate terms of surrender. This war is going to test more than our strength. This war will test our resolve to defend and encourage freedom around the world ...

*Editor's Note: Edited from Adm. Keating's remarks to AFCEA West, Feb. 3, 2005. CHIPS*

# A Spectrum Fable: How AESOP and XML Improve Naval Operations

By Jack Gribben

If you remember what it was like to be a preschooler, you'll recall *Aesop's Fables*, short stories with moral lessons passed down from ancient times. However, mention the word "AESOP" around the Naval Sea Systems Command (NAVSEA) these days and a tale of Extensible Markup Language (XML) and the electromagnetic spectrum will emerge. And before the day is through you just might find yourself re-examining the tale of "The Tortoise and the Hare."

The Afloat Electromagnetic Spectrum Operations Program, or AESOP, is a surface Navy spectrum management software tool for managing radar and communications frequencies of shipboard equipment. It is a critical task. Poor spectrum management leads to undue interference that can cripple systems meant to bolster warfighting capabilities like tracking enemy aircraft or jamming enemy radar.

AESOP covers a wide range of situations, from single ship training to large-scale multiple Strike Group operations. In Strike Group operations, the tool's three core components (Communications Planning module, Radar Planning module and Participant module) work in concert to ensure effective spectrum usage. The Communications and Radar Planning modules are used to establish frequency plans for the Strike Group, while the Participant module allows other units to provide inputs in the form of frequency and mode settings for radar and weapons systems.

The current version of AESOP (Version 1.0) is not problem-free. An absence of automation between the Participant and the Radar Planning modules requires large volumes of manual data entry. Ship spectrum data are periodically printed from AESOP and a Sailor must manually key, or "fat-finger," data into the Naval Text Message System. AESOP's fat finger process is an extreme liability in a warfighting environment. It is very time consuming and increases the likelihood of human error.

Enter XML. Last year the Naval Surface Warfare Center Dahlgren Division (NSWCDD), which develops and maintains AESOP, created a new version of the software incorporating XML technology. XML is just right for AESOP because of its unique properties that enable shared vocabularies between systems. The shared vocabularies ensure that authoritative data are visible, available and usable for improved access and accelerated decision making.

Under NAVSEA's direction, NSWCDD introduced the latest AESOP (Version 1.1) using a single XML schema to replace text messages and eliminate the fat finger process required to exchange information between the two modules. NSWCDD tested the new software in October as part of the two-week Trident Warrior 2004 exercises. For TW04, the developers created an XML interface enabling automated generation and parsing of XML-based participant messages as part of a simulation designed to mimic enemy radar jamming.

*"Even though it was only experimental, having the ability to test the new version of AESOP during Trident was hugely important,"* said Mike

Mearns, an NSWCDD project engineer. *"As we had hoped, XML was very effective in helping us to achieve greater interoperability through automation and significantly reduced the time needed to transfer and decipher data."*

TW04 was important to AESOP for another reason — it highlighted the growing need for XML reliability standards. During the exercise, the NSWCDD found a great deal of variation in XML components — elements, attributes, types and schema — being used by different developers. Problems arise when multiple XML-based systems can't agree on common components. For example, during Trident Warrior developers used AESOP to communicate with a radio frequency modeling tool called Builder. They were unsuccessful because the two applications were relying on significantly different XML components.

The NSWCDD developers are back at work. This time they have the benefit of the Department of the Navy (DON) XML Naming and Design Rules (NDR) issued in January 2005. The NDR provides a catalog of reusable XML components that facilitate the discovery and use of common data across the DON enterprise. The rules give developers the tools to ensure components are based on open standards that support net-centricity in alignment with the Federal Enterprise Data Reference Model and the Defense Department's Global Information Grid.

*"The NDR's support for net-centric operations is helping us to realize the benefits of expanded interoperability,"* said Bob Green, lead for the DON CIO Data Management Team. *"The rules guide the effective and efficient use, and reuse of XML technologies, and allow us to move beyond the old point-to-point data transfer paradigm. The result is that the Naval warfighter has access to the right data at the right time — and in an understandable format. This will contribute to better decision-making capabilities in both our business and warfighting mission environments."*

Over the next few months, AESOP's XML data elements and schemas will be reformulated from Version 1.1 to Version 2.0 to comply with the NDR. The changes provide a common structure and language for making spectrum assignments and allow a more rapid response to changing requirements. The goal is to have an NDR-compliant AESOP Version 2.0 ready for fleet-wide release by summer 2005. With proper implementation following the NDR framework, XML will enable spectrum managers to truly account for all electromagnetic spectrum-dependent equipment in near-real time.

The moral of this spectrum and XML story: Just as in the fable of the tortoise and the hare, steady progress is what really wins the race.

*Jack Gribben is a Research Fellow at LMI, a not-for-profit government consulting firm dedicated to improving public sector management. LMI provides support to the DON's XML and electromagnetic spectrum program initiatives.*

CHIPS

# Enhancing Awareness in the Maritime Domain

By Vice Admiral John Morgan and Commander "Bud" Wimmer

Maritime Domain Awareness is all about generating actionable intelligence, the cornerstone of successful counterterrorist and maritime law enforcement operations.

## Introduction

The challenges facing our Naval and Coast Guard forces have changed dramatically over the past decade and make the future security environment increasingly complicated and uncertain. This new environment, highlighted by the events of Sept. 11, 2001, shows that terrorists will exploit access to our open society, economy, and commercial systems to bring about damaging and potentially catastrophic effects on our homeland.

With a more globally connected economy and our nation's continued reliance on the global maritime environment for trade and commerce, ensuring a safe and secure maritime environment is critical to national security and economic well-being.

An emerging set of diverse, increasingly networked adversaries pose security challenges every bit as threatening as what we would encounter if confronted by a peer adversary. In addition to a few hostile or potentially hostile states — some armed with nuclear weapons — the United States is threatened by terrorists, a proliferation of illegal weapons, organized crime affiliates, drug traffickers and cyber outlaws.

Whereas the enemies of yesterday were predictable, homogeneous, rigid, hierarchical, and resistant to change; today's enemies are dynamic, unpredictable, diverse, fluid, networked and constantly evolving.

They benefit from the many technologies

and materials that are readily available for sale on the world's illicit markets to disrupt systems and fabricate weapons of mass destruction (WMD). These enemies do not operate on conventional battlefields, but thrive in weak states and gray areas where terrorists ride the back of transnational crime.

To counter the multitude of threats presented by these conditions, we must deny our adversaries the use and exploitation of the maritime environment, including its transportation systems. The first step toward enhancing our Maritime Security is achieving increased awareness of activities in the maritime domain.

## Enhancing Awareness

To achieve increased awareness, the Coast Guard, in partnership with the Navy and other agencies, is developing an initiative called Maritime Domain Awareness (MDA). The Navy has achieved MDA for years at the tactical level to dominate areas surrounding Carrier and Expeditionary Strike Groups, but in the context of the global war on terrorism (GWOT), MDA takes on a strategic dimension.

MDA is the collection, fusion and dissemination of enormous quantities of data — intelligence and information — drawn from U.S. joint forces, U.S. government agencies, international coalition partners and forces, and commercial entities. Eventually, the depth of information collected from these various sources will be weaved together to enrich a comprehensive common operating picture (COP) that is envisioned to be fully distributed among users with access to data that is appropriately classified.

The purpose of MDA is to generate *actionable* intelligence. Without actionable intelligence, counterterrorist or maritime law enforcement operations are seldom fruitful. With it, the range of options available to Navy and Coast Guard forces expands significantly to permit much more effective investigation and

interdiction of potentially threatening vessels, either overseas or as they approach the United States.

Additionally, MDA acts as a key enabler for other critical security measures, such as the Proliferation Security Initiative, Container Security Initiative, United Nations sanctions enforcement, counter-narcotic operations, and anti-piracy patrols. Response options available range from intensified surveillance and tracking, to Expanded Maritime Intercept Operations (E-MIO), to the application of lethal and non-lethal force, if necessary.

The ultimate goal of MDA, in the context of Homeland Security/Homeland Defense, is to identify threats as early — and distant from American shores as possible. This will buy time to determine an appropriate course of action.

The Navy and Coast Guard have defined MDA to be the effective understanding of anything associated with the global maritime environment that could impact the security, safety, economy or environment of the United States.

The Navy, with its significant maritime intelligence, collection, fusion and dissemination capabilities, plays a leading role within the Defense Department for developing MDA and orchestrating the process by which information is shared with coalition partners, and other agencies and departments of the U.S. government.

Sharing information is absolutely essential if this growing network is to effectively detect, identify and track the most dangerous threats, including terrorists, WMD, narcotics, piracy, mass migrations, and arms traffickers. Awareness generated through information sharing will enhance understanding of the global maritime environment, including adjacent ungoverned areas in which terrorists operate, thereby providing opportunities to deal with threats as far away from America's borders as possible.

MDA consists of two key components: information and intelligence. These components will combine in the COP to create a substantive, layered presentation of the global maritime environment. Numerous governmental and military organizations already possess a COP of some sort; however, no one source captures all of the maritime information needed or currently available.

The challenge will be to effectively integrate and fuse the various inputs to achieve the synergies offered by a comprehensive situational awareness picture, while being responsive to the information needs of participating agencies. Through the COP, specialists will eventually be able to monitor vessels, people, cargo and designated missions, areas of interest within the global maritime environment, access all relevant databases, and collect, analyze and disseminate relevant information. Efforts are underway to determine the capabilities existing COPs have to accomplish these tasks and to assess the complexity of integration.

For the foreseeable future, technological and fiscal constraints will not support global tracking of every vessel, nor would doing so be useful in of itself. Based on fused data, intelligence and information, the most threatening vessels will receive priority cueing in order to focus our assets in the right areas. As better, less expensive solutions are developed, we can improve our ability to achieve maritime transparency.

## Potential Technological Solutions

Technological advances may offer solutions to a number of the most difficult challenges encountered in the MDA development effort. Areas where technology can directly contribute to enhancing MDA are in the improved detection and tracking of vessels and crafts in the global maritime environment; the ability to monitor the movement of people and cargo in the maritime environment; the development of a comprehensive COP; and enabling appropriate access to the myriad databases and information sources which can make valuable contributions in detection and prevention.

To enhance our ability to detect and track vessels and craft on the high seas, existing capabilities and new technologies are being examined to determine the most effective way to proceed. For example, large commercial vessels now carry a collision avoidance and harbor traffic control device called Automatic Identification System (AIS), which is analogous to Identification Friend or Foe (IFF) transponders fitted aboard commercial airliners.

Expanded maritime traffic networks could use this system to identify participating vessels overseas or approaching our shores. Also, sensing systems such as long-range, over the horizon radars; high-altitude, long-dwell unmanned aerial vehicles (UAV); lighter-than-air craft; oceanic surveillance buoys; and acoustic systems show great promise for enhancing our ability to detect vessels and craft in the open ocean environment.

Integral to enhancing MDA are screening technologies used for verification of shipments and people prior to their departure from foreign ports. Many of these technologies are being implemented by agencies such as the U.S. Customs and Border Patrol performing nonintrusive inspections.

Technologies under development include "smart boxes," which will have built-in sensors that can detect prohibited items, threatening substances, potential WMD materials and unauthorized entry.

As an enabler, technology will be instrumental in the development of the envisioned comprehensive Maritime Domain Awareness COP by permitting the fusion of various information and intelligence sources.

The information exchange between government agencies and with private industry, in particular, sharing common databases, is the real power behind a global Maritime Domain Awareness COP.

Developing, and in some cases restricting, the layers of information available in the COP pose daunting challenges. Initiatives in this area have been in motion for some time, for example, the development of the Law Enforcement Information

## Sharing common databases is the real power behind a global Maritime Domain Awareness common operating picture.

Exchange (LiNX) program by the Naval Criminal Investigative Service, the FBI, and a number of state and local law enforcement agencies. Further advanced command and control tools and decision-making systems such as data-mining and anomaly detection software will serve as the backbone for a realistic and tailorable COP.

Capabilities discussed here are expected to feed end users at locations ranging from Coast Guard Sector Command Centers to Navy Fleet Headquarters to federal teams of Navy, Coast Guard and other law enforcement personnel.

## Conclusion

Great strides can be made toward improving Maritime Domain Awareness through efforts to enable and enhance information sharing among governmental agencies and by incentivizing private industry participation. While the effort to enhance MDA is certainly built upon the many relationships needed to establish the free flow of relevant information and intelligence, developing technologies will provide the framework needed to achieve maximum situational awareness of all activities in the maritime domain that may adversely impact the national interests of the United States.

No doubt, there will be significant technological and policy challenges to overcome. But by leveraging existing capabilities and prudently focusing our technology development efforts, we can successfully chart a course through the tumultuous waters that comprise the current strategic environment and emerge a prosperous, more secure society.

*Vice Admiral Morgan is Deputy Chief of Naval Operations for Information, Plans, and Strategy. Commander Wimmer works in the Strategy and Policy Division in the Office of the Chief of Naval Operations. CHIPS*

# Interview with Dave Wennergren

## Department of the Navy Chief Information Officer



*Mentoring young professionals and guiding and inspiring the workforce is a top priority for the Navy-Marine Corps leadership team. In addition to technology certifications and academic degrees, CHIPS asked the DON CIO, Dave Wennergren, to talk about the skill sets and personal qualities needed to be a successful part of the Navy-Marine Corps team.*

*CHIPS: What is your definition of success?*

**Mr. Wennergren:** Success is one of those things that is hard to quantify, but easy to see ... if you look for the right things. Success is when an organization is effective; when the mission of an organization is achieved. Today, success is very rarely about personal accomplishment or ambition, but much more the result of teamwork. People who realize this do a much better job of building teams for success. People who are solely focused on personal success have a more difficult time because that kind of success is illusory and usually comes at the expense of others. Achieving success by bringing others along with you provides more value to the organization and is far more satisfying.

When I think back on my career, before my days as CIO, I was involved in regionalizing Navy shore infrastructure services to gain efficiencies and effectiveness. I led a team that went to a certain region to help develop a new organizational structure; one that could operate more effectively by sharing resources. About two or three years later I went back to that same region of the country and met with the folks that were actually working in the new streamlined organization. They described to me what they had done and how they had turned their idea into reality. Of course, they had no idea that I had led the team that initiated the regionalization plan; this was a new group of people.

From their viewpoint, it was their plan that they had accomplished, and I thought that was the true measure of the success of the effort. It was far more important that they felt the idea was theirs and they owned it, rather than remembering that some other group of people helped them create the idea. As a result, they had a strong interest in seeing the plan succeed. They were so proud of what they had done. They didn't know that I was part of the team that came up with that idea, and that was fine because the success of the organization is what is really important.

Sometimes personal goals and personal ambitions can stand in the way of trying to help people do the right thing. While it is not always obvious, it seems clear in retrospect that what is important is what you do to help make a team successful, what you do to help empower others and what you do to help train lead-

**“Success can be measured by your position in the organization, your association with a team, your happiness in the work you do, the relationships you have made, or the people you have mentored.”**

ers. Giving people opportunities to understand their gifts and putting them to work is a trait of successful organizations.

*CHIPS: What advice do you have for an individual just beginning a career, someone who wants to stand out in an organization?*

**Mr. Wennergren:** I guess I would ask them what sort of results they want to achieve because success means so many things to so many people. Success can be measured by your position in an organization, your association with a team, your happiness in the work you do, the relationships you have made, or the people you have mentored.

Success should actually be the by-product of having achieved results. Everybody is not built for the same kind of job. Some people are better at supervising while others are better at technical skills. I would want to understand where their passion is and then help them think about the learning and professional opportunities, skills they could hone, and knowledge they need to gain to be able to fully take advantage of their skills and abilities.

If you are contributing the talents that you possess, in a way that makes you happy, then you will be successful. Follow your dreams. You'll spend a lot of time at work. If your career aligns with your gifts and your passion, then every hour you spend working will be both fulfilling and energizing.

*CHIPS: What advice do you have for those who want to develop executive-level skills?*

**Mr. Wennergren:** Interestingly, there are certain general skills that are really important to have. If you are going to be a senior manager, it is often far less important that you have profound technical knowledge and far more important that you



understand the organization, its mission and its culture. These are basic skills that are important no matter where you work. You need to understand how the personnel process works. You must hire good people and then motivate them, nurture them, sustain them and then help them to grow.

You need to have an understanding of how the financial and procurement processes work. You must understand what your own strengths and weaknesses are, and how to be a good leader. If you don't understand these things, then it will be difficult to rise above the ranks of being an expert in your field.

The kinds of challenges that face an organization like the Navy and Marine Corps are so broad, and they tend to cross traditional organizational boundaries. Therefore, people who get to leadership positions often get there because they have a broad set of management skills. Executive leadership is about being able to manage for results, recognizing how to lead others, how to get the most out of workers, and how to work across organizational boundaries to form teams that can coalesce around successful answers.

*CHIPS: What are some of the common traits and skills of successful people?*

**Mr. Wennergren:** My former boss, mentor and great friend, Dan Porter, once told me that 'A' people hire 'A' people and 'B' people hire 'C' people. Something that you often see in good leaders is the ability to recognize the strengths and skills of an individual so that you get the 'right people on the bus.'

If you don't have skills at finding good people and then energizing them, it is very difficult no matter how visionary you are. Finding good people and then putting them in a supportive environment where they can grow and excel, is one of the traits that great leaders that I have known exhibit.

Obviously, it is important to have leadership skills. While some skills may be innate, there are many things that you can learn and spend some time developing. You have to learn to listen and communicate well. These are basic skills that you see in leaders. You have to be able to communicate. That's why I often point to a book written by Howard Gardner, *The Power of Story Telling*. Gardner discusses how successful leaders are able to tell effective stories. They use stories to help people understand ideas, concepts and organizational vision.

Successful individuals know how to empower people because the higher you are in a leadership position, the less you can afford to micromanage the efforts of people. You will not only stop them from being the successes they could be, you will disenfranchise them and de-motivate them. You need to know when to coach, when to encourage, when to offer advice and when to get out of the way, and let the people who work for you go be the successes that they can be.

*CHIPS: When you are selecting a book to recommend to the Navy-Marine Corps team, do you look at it as a kind of cookbook solution or are you saying that you have to pick and choose what you need? Do you use these books for inspiration?*

**Mr. Wennergren:** I think it's a little bit of all those things. I think at the most basic level it's about cultivating a learning organization, an environment where learning is valued. We ask everybody that works in the CIO organization to do some type of learning experience each year, and we are really flexible as to what a learning experience might be. It could be taking a college class, taking a training course, or attending a conference or seminar. It should be something that helps you broaden your horizons and opens your mind to the art of the possible; something that gets you to step out of your comfort zone and broaden your horizons.

Sometimes, I have a secondary motivation when I recommend books. For example, when I tell people that I think that they should read the book *Execution: The Discipline of Getting Things Done* by Larry Bossidy and Ram Charan, part of my motivation is that we oftentimes have not done a good job at execution.

It's easy to get excited about a new idea, but then some of the initial excitement wears off and people want to move on to the next big idea rather than following through on the original idea, measuring its effectiveness and making sure that we are getting the results we desire. I often point out these books hoping that people will read and get some valuable lessons out of them.

Sometimes reading a book can help you have a common language so that you can talk about the issues that we sometimes have a hard time articulating. Sometimes it's about cookbooks, sometimes it's about stepping out of our comfort zones, but more often it is about coming up with ideas about the things that we ought to be thinking about to help an organization change.

*CHIPS: Have any of these books changed the way you work?*

**Mr. Wennergren:** I like to think that we grow each time we read and that we find something in each of these books. We, in the CIO office, read *Fish!* by Stephen C. Lundin, Harry Paul and John Christensen a couple of years ago. It's a great little story about being positive. It had some simple tips about how to be successful. The tips can be applied to your personal life and your professional life. The people that read *Fish!* together seemed to have this bonding experience. They began to talk about it, and its lessons started to permeate the attitude of the organization.

Reading together as a group is a powerful thing for an organization. We try to pick a couple of books that we are going to read together as an organization each year. We talk about it and incorporate



*February 2005, the DON CIO, Mr. David Wennergren in his office.*

“If you are not reading something that is helping you to improve, then you are probably not reading the right kind of books.”

the ideas contained in the book into our vocabulary at work. If you are not reading something that is helping you to improve, then you are probably not reading the right kind of books.

*CHIPS: I've been reading about the Department's Human Capital Strategy, which is designed to ensure that the Department has the right people with the right skills for 21st century national security needs. What are some of the benefits of the Human Capital Strategy? Will it help the Navy-Marine Corps team in terms of professional development and career planning?*

**Mr. Wennergren:** A well understood and articulated human capital strategy is crucial for a number of reasons. It will help to ensure that our 'total force' — Sailors, Marines, civilians and contractors — have the competencies essential to fight and win in the 21st century. Successful companies have long understood that an effective human capital strategy provides a tremendous competitive advantage, and the leadership of our Navy-Marine Corps team recognizes that this is true in our world as well.

In terms of the IM/IT workforce, our team leader, Ms. Sandy Smith and a number of her colleagues across the Department have done an outstanding job in developing a Department of the Navy strategy that addresses both workforce planning and human capital management. This work has been embraced by a number of other agencies and has proven very helpful in aligning people's skills, experiences and capabilities to the current and future IM/IT needs of the Department.

*CHIPS: Is it important to have a well-structured career plan?*

**Mr. Wennergren:** Somebody told me once that there are two schools of thought about managing your career. One is the very organized person who says, 'I'm going to do this for two years and then I am going to do that.' These people try to plan their whole life's journey. That works well for some people. Others take a much more seemingly chaotic approach to planning their careers.

But at the heart of the matter, it's about doing a good job and building up networks and having people recognize that you are doing a good job; and as a result, new opportunities present themselves. I don't know that there is one right answer. I know that I have clearly fallen more into the second camp than the first camp.

I think either path can be successful as long as you know yourself and know what you like to do so that you can develop the skills, find the opportunities and get involved in the activities that will help you get to the place you want to be. This can happen with a whole lot of advance planning or it can happen by just making the most of the opportunities that are presented to you. Both ways can get you to your goal of being successful, particularly if your measurement of success is working at something you really enjoy and where you feel like you are making a difference. CHIPS

## Must-Reads from the DON CIO

*David Wennergren, the Navy's chief information officer, has put together a recommended reading list for the Navy's information technology workforce.*

✓ *Execution: The Discipline of Getting Things Done* by Larry Bossidy and Ram Charan

✓ *Leadership is an Art* by Max Dupree

✓ *Good to Great: Why Some Companies Make the Leap ... and Others Don't* by Jim Collins

✓ *First, Break All the Rules: What the World's Greatest Managers Do Differently* by Marcus Buckingham

✓ *The Power of Story Telling* by Howard Gardner

✓ *Leading Change* by John Kotter

✓ *The Power of Alignment: How Great Companies Stay Centered and Accomplish Extraordinary Things* by George Labovitz and Victor Rosansky

✓ *The Thin Book of Appreciative Inquiry* by Sue Annis Hammond

✓ *Who Moved My Cheese? An Amazing Way to Deal with Change in Your Work and in Your Life* by Spencer Johnson

✓ *The 21 Indispensable Qualities of a Leader: Becoming the Person Others Will Want to Follow* by John Maxwell

And finally, straight from the Department of the Navy's CIO team:

✓ *The Power of Team: The Making of a CIO* by Dan Porter, Alex Bennett, Ron Turner and Dave Wennergren. This book from the leaders of the Department of the Navy CIO organization, shares the experiences and insights about constructing and implementing an agenda for the newly formed Chief Information Office. It serves as a reference for organizations that are charged with the responsibility of implementing and managing information technology or leading change in an IT organization.

*The Power of Team: The Making of a CIO* is available from the DON CIO Web site at <http://www.doncio.navy.mil/>. Click the Products tab and select "View Online" to download the PDF. Select "Request This Product" and complete the online request form to request a hard copy.

# Beyond Iraq

By Admiral Walter F. Doran, Commander, U.S. Pacific Fleet



*Adm. Doran addressing representatives of the media in San Diego, Feb. 2, 2005.*

I'm going to give you a picture about what the U.S. Pacific Fleet is doing beyond Iraq and how we are getting transformation right.

Keeping the direction the Chief of Naval Operations has given in mind, I would like to outline some of the contributions that the Pacific Fleet is making to our nation's defense. Specifically, how we are working to prevent the development of a strategic void by changing our behavior patterns while concurrently conducting a wide array of missions across the security spectrum.

The U.S. Army and Marine Corps remain heavily engaged in Operations Iraqi Freedom and Enduring Freedom — and for good reason. They are doing exceptional work and making tangible progress every day. Our national and military leadership are dedicating tremendous energy to supporting these critical missions, and you see this reflected daily in the media worldwide.

Others read and hear this same media coverage and might be inclined to view this focus of American attention as an opportunity for malevolence in other potentially volatile regions of the world. This would be a grave miscalculation. The current U.S. level of effort in Iraq must not be misinterpreted as a diminishing of focus elsewhere.

Beyond Iraq, today's U.S. Navy holds significant strategic relevance to the defense of our nation. We are providing "presence with a purpose," preventing any would-be adversary from making the mistake of perceiving that a strategic void exists in U.S. military policy or capability. Nowhere is this more evident than in the Western Pacific, where the U.S. Pacific Fleet is actively working to "dissuade and deter" any potential threat.

To this end, we continue to transform our Navy into a more persistent and agile force for the 21st century, a force better prepared to overcome future security challenges. As a result, we have changed our behavior patterns to increase our visibility in the Western Pacific, and we are preparing and operating our forces much differently than we have in the past.

For the last decade, the preponderance of Pacific Fleet units have trained and worked along the western coast of the United States, then sailed straight through the Pacific en route to the Arabian Gulf region. This is no longer the case. Pacific Fleet training and deployment efforts are now focused on our most difficult, po-

tential theater warfighting scenarios. Across naval warfare communities, and with the close coordination of our Numbered Fleet Commanders – 3rd and 7th Fleets – we are conducting increasingly complex training at both the unit and integrated levels to refine the skill sets necessary to execute these challenges.

This new deployment pattern displays our commitment to maintaining a responsive, highly credible, persistent presence in the Western Pacific. The 2004 deployment of the John C. Stennis Strike Group was the vanguard of this multifaceted effort. Following completion of an intensive pre-deployment workup, Stennis participated in a series of exercises: Northern Edge in the Gulf of Alaska, RIMPAC in the Hawaiian area of operations, and the Joint Air Sea Exercise (JASEX) in the Western Pacific. Each exercise had increasingly complex tactical elements embedded in the event.

Additionally, the exercises demonstrated U.S. support for multilateral/combined maritime operations. Forty ships and submarines from seven nations participated in a robust RIMPAC exercise showing our capacity to conduct advanced dual-carrier strike group operations forward in the Pacific as displayed in JASEX. To ensure we continue to enhance the effectiveness and reach of naval forces, we have instilled an equally strong commitment to technological experimentation and rapid technology insertion.

During the Stennis deployment, we operated with several emerging technologies that industry provided, and they are helping improve the coordination, integration and implementation of our warfighting efforts. Some examples of what we were able to operate and train with are the variety of new sensors and equipment particularly in the area of antisubmarine warfare (ASW). These included the Automated Rapid Periscope Detection and Discrimination (ARPDD) System, Low Frequency Active (LFA) Sonar, and net-centric programs such as the Composeable FORCenet and the Undersea Warfare Decision Support System, to name just a few.

The results were encouraging and will provide invaluable vectors for future programmatic decisions, for example, accelerating investment in sonar processing improvements and training, such as Advanced Active Analysis Adjunct (A4I) for PC Interactive Multisensor Analysis Training (PC-IMAT) to reduce false contact generation rate over legacy systems. I observed A4I in action aboard Stennis Strike Group ships and it works; moreover, our Sailors believe in it based on performance at sea.

The Undersea Warfare Decision Support System facilitated sonar planning in the Stennis Strike Group, and it is an excellent example of a system with the potential to improve the flow of information, environmental modeling and prediction, data fusion

and contact correlation. These tools and applications will allow us to better integrate our ASW assets and get the best use from our sensors in the water column of interest. I'm encouraged by our technology progress and hungry for further developments.

The Pacific focus of the Stennis Strike Group deployment was not a one-time event. The flexibility inherent in the Navy's Fleet Response Plan was showcased when the Abraham Lincoln Strike Group commenced a surge deployment this past fall. Following completion of integrated training in the Middle Pacific, Lincoln moved forward to operate in WESTPAC waters. Lincoln's deployment reinforced to both our friends and potential adversaries, that despite the intensive level of effort in Iraq, the U.S. military — specifically the U.S. Pacific Fleet — continues to be fully committed to the security of this critical region.

As a result of the tragic December earthquake and tsunami in South Asia, Lincoln formed the centerpiece of the Navy's significant contribution to the international humanitarian assistance/disaster relief operation, which included the Bonhomme Richard Expeditionary Strike Group, Maritime Patrol Aircraft, Maritime Preposition shipping, logistics forces and medical personnel. Working closely with our coalition partners and host nation, the State Department, United Nations and nongovernment (NGO) officials, Navy forces provided invaluable support to Operation Unified Assistance including delivery of more than 4 million pounds of food, water, and medical and relief supplies to affected areas.

The Navy's contribution to this relief effort is a persuasive display of U.S. military responsiveness to the farthest reaches of the globe, and as with all of our operations, technology played a crucial role. Unified Assistance was an impressive display of Sea Basing. The surveillance, command, control and communications capabilities embedded in Navy platforms, were critical to the success of the expansive relief effort, providing maximum capabilities with no supporting infrastructure or footprint ashore.

While we are continuing to compile lessons learned, technological challenges were handled swiftly and effectively. The need to send broadcast quality video over a finite quantity of satellite bandwidth was expertly handled by SPAWAR fleet systems engineers and Navy Combat Camera with the rapid application of new video compression and transmission software.

Looking past the relief effort and across the spectrum of military operations, Pacific Fleet forces are engaged in a myriad of efforts. In support of the National Ballistic Missile Defense (BMD) System architecture, we are expanding the horizons of naval warfare. Pacific Fleet AEGIS combatants recently completed modifications to support long-range ballistic missile surveillance and tracking. These ships have begun periodic operations in designated patrol areas to support mission risk reduction and exercise joint command and control in preparation for National BMD System activation.

To further enhance our capability and system reliability, we are working closely with the Naval Systems Commands and the technical community to provide additional pathways for missile track data, as well as radar and support system improvements. We are also preparing to introduce a sea-based defensive capa-



*Jan. 10, 2005 - A U.S. Marine Corps amphibious vehicle prepares to bring Marines and Sailors aboard a Landing Craft Utility (LCU) at the end of the day's relief efforts in Colombo, Sri Lanka. Helicopters from USS Bonhomme Richard (LHD 6) and Marines and Sailors assigned to 15th Marine Expeditionary Unit are supporting Operation Unified Assistance. U.S. Navy photo by Lance Cpl. Joseph Ward.*

bility with the fielding of the SM-3 (AEGIS Ballistic Missile Defense) later this year. Maritime Interdiction Operations is another maritime-centric effort in our contribution to the global war on terrorism and forms perhaps our greatest area for strengthening our fight. We are advancing innovative uses of existing technologies and platforms to develop and refine tactics, techniques and procedures (TTPs) for maritime interception applications using an Afloat Staging Base concept.

Recently, the Pacific Fleet participated in several efforts to further the growing partnership resulting from the Regional Maritime Security Initiative or RMSI. Willing nations are recognizing our collective need to enhance and leverage capabilities that can identify, monitor and intercept transnational maritime threats. Our goal is to gain increased information sharing and enhanced situational awareness to facilitate international cooperation and synchronization to improve security and cue effective threat responses. Development and fielding of Maritime Domain Awareness tools and applications will be central to this effort.

Command and control remains critical to the execution of RMSI mission sets and the Combined Enterprise Regional Information Exchange System (CENTRIXS) is helping us overcome the challenge. In the Pacific, we witnessed recent successes with CENTRIXS during RIMPAC and ANNUALEX in 2004 with the Japan Maritime Self-Defense Force (JMSDF). CENTRIXS remains the primary means for coalition command and control. The realization of RMSI will depend on the technical community and your ability to develop enabling technologies.

As the Navy transforms, we need you to transform our technology, so we are able to acquire speed of response for all operations in the maritime domain. As you work, rest assured that the Pacific Fleet remains fully engaged and highly visible to both our friends and potential adversaries in the Asia-Pacific region.

*Editor's Note: Adm. Doran's article is based on his remarks to the AFCEA West Conference Feb. 2, 2005.*

CHIPS

# Interview with Captain Kevin R. Hooley

## Commanding Officer

### Center for Information Dominance



The merger between the Center for Information Technology (CIT), headquartered in San Diego, Calif., and the Center for Cryptology (CC) Corry Station, located in Pensacola, Fla., to form the Center for Information Dominance (CID) Corry Station, integrates training responsibilities for four key disciplines of information dominance — exploit, attack, defend and operate — under one learning center. Prior to the merger, CIT was responsible for the training of personnel specializing in network operations for the United States and allied forces, while CC Corry Station had oversight responsibilities for the training of signals intelligence. CC Corry Station commanding officer Capt. Kevin R. Hooley will assume command of the new Learning Center, which commenced operations Jan. 31, in a provisional status until formally established.

CID responsibilities include administering more than 225 courses and managing a staff of 897, with the charge of training nearly 16,000 members of the armed services, including the U.S. Coast Guard and allied forces each year. There are 17 CID learning sites and detachments throughout the United States and worldwide.

*CHIPS asked Capt. Kevin R. Hooley to talk about what the stand up of the CID means to the Navy.*

*CHIPS: Can you explain the significance of the merger between the Center for Information Technology and the Center for Cryptology?*

**Capt. Hooley:** In its purest form, the significance is effectiveness, efficiency, alignment and operational readiness — Sea Warriors developed through blended training solutions to optimize the power of information. To achieve information dominance there are four major attributes that we work. Those are the ability to exploit information and to attack information, while at the same time defending and operating our information within our networks.

Prior to the merger of these centers, these skills were taught at various locations throughout the Navy. As a result, information dominance was not operating as a synchronized, interdependent training function.

Operating networks was taught at the Center for Information Technology in San Diego. The exploitation of information for intelligence purposes was taught at the Center for Cryptology in Pensacola. Training for information warfare and information operations, which deal with information assurance (the defense of systems and the attack of enemy systems), were not taught under the oversight of any particular learning center. As a primary warfare skill of the Navy, run principally from the Naval Network Warfare Command, information warfare skills were taught via Mobile Training Teams in a just-in-time training methodology.

While all these organizations did an outstanding job in training, our overall capability in information dominance was compromised by this dispersal of intellectual capital and less than optimal alignment. With this merger, we have taken all of these principal attributes of information dominance and aligned the training responsibilities for each into one center. Now a fleet

unit or fleet commander or type commander can reach to one place, one center, “one-stop-shop,” per se, to leverage our expertise to answer any questions within the realm of information dominance.

Also, we had a lot of intellectual capital in the Navy that was dispersed at many centers and many sites. But they were not really leveraging off each other to move our mission forward. By bringing them under one center we are able to do that. We are also able to diminish the size of the staffs, since there were some redundant positions that we were able to eliminate and reinvest into other principal jobs in the Naval Personnel Development Command domain. As I mentioned up front, effectiveness and efficiency are the biggest benefits to the Navy.

What it means to the Navy is the ability for us to provide them with a better trained information warrior and, therefore, a better warfare capability in the fleet. That’s truly the bottom line of what we are all about — developing warriors to dominate information in the maritime maneuver and battlespaces.

*CHIPS: How will this merger ensure information dominance for the warfighter?*

**Capt. Hooley:** I think ensuring information dominance for the warfighter involves a blending of training, along with the robust tactics, techniques and procedures that are developed and implemented in the fleet. There is no single answer — it’s a continuum of training and operations.

CID’s mission is to deliver the right training, at the right time, in the right place, utilizing technology, innovation and the science of learning, to provide the fleet with optimally trained Sea Warriors who will create a tactical advantage for mission success in

the information domain. We will provide a very strong foundational training base that will give the fleet the best qualified Sailor to ensure information dominance through expert planning and execution of operational tactics. So, that assurance of information dominance comes from a continuum of us (as trainers) and the operators in the fleet.

*CHIPS: Are courses instructor-led or online?*

**Capt. Hooley:** There is a great combination of both. Just for a little bit of clarification, at Corry Station we have the center, which is actually the CID headquarters, housing the management staff and policy-making arm of our training enterprise. Most of the training is dispersed throughout the globe at 17 Learning Sites that we oversee, including our Corry Station Learning Site, which is our largest training facility. The other sites are located in all of the major fleet concentration areas such as San Diego, Norfolk, the Pacific Northwest area, Mayport, Fla., and all the way to Yokosuka, Japan where we have forward deployed naval forces. It is very critical that we have training for them as well.

We employ a blended learning solution in everything that we do. Some of our training has to be classroom-based with an instructor interacting with the students, some of it is Web-based, video-based — or page-turning in a manual. There are many different solutions in the way we train — there's no one answer.

*CHIPS: Do personnel receive certifications comparable to industry certifications like Microsoft provides?*

**Capt. Hooley:** Let me give you two answers to that. They do receive certifications – apprentice, journeyman and master – within the Navy's 5 Vector Model construct. When Sailors complete courses in certain training continuums, they will receive credit, and it will be properly annotated in their 5 Vector Model.

When you compare it to Microsoft training, there are some instances in which we do leverage from industry. If we build a system that has a Unix-based operating system, for example, we may send the Sailors to Unix operating system training in private industry.

We are currently working on an initiative to get the capability to receive private industry certification. Right now, within the public law, the Navy does not have the capability to use our funds to pay for the certifications that are available in the private sector.

The Naval Personnel Development Command is working on a major effort called "certifications and qualifications" with the Office of the Chief of Naval Operations in an attempt to get that law changed so we can start to give our Sailors credit for those courses and the applicable civilian certifications. That will be a wonderful program once we get that in place. But it has to go through all the appropriate legislative paths.

*CHIPS: Are classes only available to personnel through rate training or job description?*

**Capt. Hooley:** That is a great question. We are really going to



*Center for Information Dominance (CID) commanding officer, Capt. Kevin R. Hooley (2nd from left), talks with Navy, Army and Air Force students attending the Intermediate Communications Signals Analysis Course March 2, 2005, as course instructor, Chief Cryptologic Technician Collection (SW) Cedric Rawlinson (standing, far right), looks on. The students are attending the 16-week "C" school at CID Learning Site Corry Station, Pensacola, Fla., to learn intermediate stages of signals search, analysis, target identification and reporting. Photo by Darlene Goodwin, CID Corry Station Public Affairs Officer.*

have to take a critical look at this. Currently, the training is driven by rate and the skill qualifications you must achieve for your job. There is not a great capacity for people to say, "Hey, I'd like to have that training." Now, there are good reasons for that because we cannot afford to train people just because they would like to have it. It is a need-based system.

However, as information proliferates throughout the Navy, as everything that we do becomes truly an information-based capability on information technology systems, we are going to have to expand our student base and be even more dynamic in the way we train and determine who we train.

Let me give you one example. We received a call the other day from personnel on the USS Nimitz. Within the nuclear-power propulsion plant, they have a local area network (LAN) for engineering systems support called the propulsion plant LAN. The people that operate the propulsion plant LAN are Electronic Technicians and nuclear-qualified. They are not Navy Information Systems Technicians or Information Professional officers.

They came to us and said, 'Although we are not a source rating for your class, and we do not get the Navy enlisted classification code out of that class, we need that training. Can you help us?' I made the decision, 'Sure.' We cannot let the rules encumber progress in operations, so we are allowing whoever needs the training to come to this course. So the short answer is that right now there is a prescribed methodology, but we are expanding and flexing that as best as we can to best serve the fleet.

*CHIPS: Can you explain how the center is a part of Sea Power 21 training?*

**Capt. Hooley:** Sea Power 21 is the concept for 21st century naval operations. The naval command and control component of Sea Power 21 is FORCENet. The very heart of FORCENet is information — the ability to ‘own’ information and enable communication between commanders and fleet operators. It encompasses maintaining and defending our communications, while at the same time, exploiting the enemy's abilities to our tactical intelligence advantage. The construct of Sea Power 21 is highly dependent upon the command and control that integrates all that together. That is what we teach here. By teaching people how to be FORCENet operators, we are combining the integration tactics that pull Sea Power 21 together in the fleet.

*CHIPS: Have there been any successes for the CID in its short time in existence?*

**Capt. Hooley:** Yes, there are a couple of things that I would like to highlight. Number one is how rapidly the Center for Information Dominance is already starting to show progress in what we do. We have brought together the information technology and information professional folks around the world, and all of the intellectual capital that they bring, along with the information operations folks, and have blended them together. We have been able to integrate into one place that operating knowledge.

It has already, in a very short term, paid off in dividends regarding the quality of our training, the integration of our assets and the capability of our force. We are really happy with what we have seen. This very swift initial gain tells us that the return on investment is going to be a substantial operational profit margin.

Another point that I would like to bring up is that the Center for Information Dominance is not only a component training facility for the Navy, we also teach Army, Marine Corps, Air Force and Coast Guard personnel. We have students from the Department of Defense and non-DoD government agencies that come here for training, as well as some students from allied forces.

Our training in information dominance is not only used within the Navy, it also helps our students become better joint warriors as they learn the information systems of the five services and press forward.

Our next step that we really want to look at and work harder, is the coalition piece because every effort that we do today and in the future in the global war on terrorism — or any fight that we take globally — is going to be fought as a coalition with our allied forces. Our ability to integrate with coalition information-based systems is absolutely essential, and we are moving forward in that area as well.

We are also working a lot of different efforts with language skills and regional area and cultural training, which is vitally impor-

“Our training in information dominance is not only used within the Navy, it also helps our students become better joint warriors as they learn the information systems of the five Services and press forward.”

tant. Our Navy is built with a global-reach capability. We can reach anywhere and perform a mission in any place in any capacity. Our human capital also has to have the same global-reach capacity as our systems. This is enhanced by language skills, regional knowledge and cultural familiarity of the people throughout the world. I’m very pleased with the initial successes in our recent language training enhancements.

You asked earlier about the different ways that we train. We talked about blended training. That is something that we are doing in our fleet concentration areas that is making a major change to the way we train.

We used to have, in cryptology, on the waterfront, 23 classroom courses of instruction that people effectively had to take a forced march through so that they could certify to go to sea. These classes were one-size-fits-all, which in my mind means ‘fits nobody.’ Folks often went through these classes whether they needed them or not.

Now what we are doing is going through a process of evaluating every potential student and learning their strengths and weaknesses, and then training to those strengths and weaknesses. For cryptologists, we may have 65 of them in a Strike Group, and what we will do is provide them with 65 different, individual training packages in a blended training solution. This is much better for the Sailor and a more effective and efficient use of training time and dollars.

There are a lot of great initiatives going on here at CID Corry Station, and across our domain by a lot of great folks, and I’m grateful to *CHIPS* for the opportunity to tell our story. I’ve been telling my staff that we have just had, in my estimation, the single largest mission increase in our history, and it’s going to take a lot of hard work on the part of every team member to pull this off successfully.

And, they are charged up and ready to go. We are going to continue to work hard, and I am confident that our progress and rapid return on investment are going to benefit our fighting forces to a great degree, giving them the tools they need for mission success in the information domain.

*For more information about the Center for Information Dominance Corry Station, log on Navy Knowledge Online at <https://www.nko.navy.mil/>. For related news, visit the Center for Information Dominance, Corry Station Navy NewsStand page at <http://www.navy.mil/local/corry>.*

CHIPS





# DON IT umbrella program

## The Umbrella Program meets the objectives and requirements for the FORCEnet architecture.

We are just 17, if you know what I mean! That's right; the Department of the Navy Information Technology (DON IT) Umbrella Program celebrates 17 years of bringing substantial cost avoidance savings for DON and Department of Defense (DoD) customers.

It was June 1988 when the Assistant Secretary of the Navy for Financial Management chartered the establishment of the Umbrella Program. In his chartering letter, he delineated the benefits of using a Department-wide acquisition strategy with "umbrella contracts" to reduce procurement time and costs, achieve substantial discounts and promote cost-effective standardization.

These historic joint service contracts successfully brought desktop computing to Navy users. But since that time the number of Navy IT acquisitions has grown exponentially — and increased in complexity — as the DON systematically continues to improve automated business and operational processes, and build a standardized, flexible architecture for tactical and non-tactical operations.

The Umbrella Program's business strategies are compatible with the FORCEnet Functional Concept. Supporting the warfighter must include the business elements of logistics and shore infrastructure. Agile business operations require robust knowledge management and information. Net-centric operations include forward and home-based support, and that's where the Umbrella Program shines at serving DON and DoD customers. Further, the Umbrella Program meets the objectives and requirements for the FORCEnet architecture by offering standards-compliant tools.

As a key component of the DoD Enterprise Software Initiative (ESI), the Umbrella Program fulfills the Navy's duties as the Executive Agent for Office Automation Tools and Enterprise Resource Planning (ERP) software. This includes the entire Microsoft product line, Section 508 tools, Adobe software, Common Access Card (CAC) middleware and ERP software by PeopleSoft and SAP. Oracle ERP software is available on the Army's Oracle Enterprise Software Agreement.

The IT Umbrella Program serves as a storefront for Defense customers through the Information Technology Electronic Commerce Direct (ITEC-Direct) online catalog at <http://www.itec-direct.navy.mil/>. Purchases can be made via the Government Purchase Card.

# The DON IT U

*The Umbrella Program fulfills the*

Since 1988, the Umbrella Program has supported all DON technology initiatives in conjunction with DoD initiatives, policies and procedures. These include providing:

- DoD Enterprise Software Initiative (ESI) support for enterprise-wide licensing of COTS software and ESI COTS System Integration agreements. DoD is using the ESI as a strategy to implement SmartBUY, the federal-wide licensing initiative. The ESI continues to work closely with the SmartBUY Program Management Office to provide best value pricing to customers.
- IT-21 desktops and software to the fleet via program office requirements.
- Consolidation of personal computer (PC) purchases and a common desktop for the fleet.
- Predecessor acquisition efforts to the Navy Marine Corps Intranet (NMCI) and the outside of the continental U.S. Base Level Information Infrastructure (OCONUS BLII) – now ONE-NET.

"Since the inception of the Umbrella Program, we have required and provided hardware and software that is compliant with commercial, open architecture standards and military standards where applicable, for example, the Government Open Systems Interconnection Profile (GOSIP), DoD Common Operating Environment (COE), Joint Technical Architecture (JTA), the IEEE, etc., to meet the interoperability requirements of the Navy and DoD," said Barbara Johnson, DON IT Umbrella Program Manager.

"Our acquisition solutions offer fleet customers who are not NMCI-ready, a bridge to a myriad of IT products and services until NMCI is there for the fleet," said Johnson.

"We work closely with the Assistant Secretary of Defense for Networks and Information Integration organization, or NII/CIO, working on the Global Information Grid (GIG) architecture, policies and guidance, along with our peer organizations within the Army and Air Force. We strive to incorporate joint visions into our acquisition strategies. In addition, we are working with the Department of the Navy Chief Information Officer (DON CIO) and the Functional Area Managers (FAMs) within the Navy to provide acquisition strategies for standard software requirements," said Johnson.

Through the years the Umbrella mission has remained the same, but by using best practices guidance, team members are able to buy smarter, ensure a positive return on investment, reduce procurement times and cost, promote standardization and interoperability, and mitigate the risks associated with government acquisition. The team reviews requirements, and seeks to serve the



# Umbrella Program Turns 17!

## *Navy's duties as ESI Executive Agent for Office Automation and Resource Planning*

majority of customers by establishing acquisition vehicles that meet enterprise requirements.

But even the smallest programs can reap the cost savings of a volume buy, according to Johnson. With our nation fighting a global war on terror, now more than ever, it is vital to save precious resources to support the Navy's warfighting mission.

"Savings vary, but are in a range of 2 (minimum) to 60 percent off GSA Schedule pricing. Some of the DoD ESI vehicles have discounts above 75 percent. This can be significant savings. So if you are talking about database software or Microsoft products, etc., the discounts are in the high range. When we put a vehicle in place, we try to think of the small agency, which may have only 10 to 20 employees so that it can receive a similar (at least minimum) discount as an agency placing large orders. Of course, if you are talking about large purchases — \$100,000 and up — these customers will get a substantially bigger discount, but small agencies (small orders) will at least get the minimum discount," said Johnson.

By working jointly with the Army, Air Force and other ESI members, the Umbrella team is able to aggregate requirements and achieves greater discounts in partnering with industry. The program also avoids duplication of effort within DoD and allows the team to concentrate on its assigned area of expertise.

The Umbrella Program team is made up of acquisition professionals from several organizations: SSC San Diego, SSC Charleston, Naval Inventory Control Point (NAVICP) Mechanicsburg, Naval Air Systems Command (NAVAIR) Patuxent River and the Naval Undersea Warfare Center (NUWC) Newport.

"The work we are accomplishing within the Navy and the wider scope of DoD and the federal government is both compatible and cohesive with current Navy initiatives and facilitates the net-centric goals of these initiatives as well as others undertaken within DoD," said Johnson.

Standards-based ordering vehicles, technical support for products through the life of the contract, integrated logistics support (ILS), e.g., software asset management, license transferability, extended warranty periods, customer support help desks, spare parts and OCONUS support are all truly some of the best value features for Umbrella contracts customers.

**For more information about the DON IT Umbrella Program, go to page 45 or the Umbrella Web site at <http://www.it-umbrella.navy.mil/>.**

CHIPS

## **Department of Defense Enterprise Software Initiative**

The Enterprise Software Initiative (ESI) is a joint project designed to implement a true software enterprise management process within the Department of Defense (DoD). By pooling commercial software requirements and presenting a single negotiating position to leading software vendors, ESI provides pricing advantages not otherwise available to individual services and agencies. The ESI is expanding efforts to include "selected services" and information technology (IT) hardware.

The DoD implements the SmartBUY federal-wide licensing initiative through the ESI. The ESI works closely with the SmartBUY Program Management Office with respect to pricing models used by industry for preferred terms and conditions, software asset management and reporting mechanisms, and to aggregate DoD requirements into volume purchases when applicable to obtain optimal pricing.

Twenty-three software best practices have been identified and adopted by the ESI Working Group, leading toward a DoD-wide business process for acquiring, distributing and managing enterprise software. The ESI vision is "Point and Click IT Shopping at the Lowest Cost" using the Internet. The ESI can use the Defense Working Capital Fund (DWCF) to provide "up-front money" for initial wholesale software buys. This funding process assures maximum leverage of DoD's combined buying power, producing large software discounts.

The ESI was incorporated into the Defense Federal Acquisition Regulation Supplement (DFARS) Section 208.74 on Oct. 25, 2002, and DoD Instruction 5000.2 in May 2003. This guidance describes the procedures required for contracting officials in DoD departments and agencies to use when purchasing software and related services through the ESI agreements.

Agreement negotiations and retail contracting actions are performed by IT acquisition and contracting professionals within participating DoD Services and agencies, as ESI Software Product Managers (SPM). For more information visit the ESI Home Page: <http://www.don-imit.navy.mil/esi/>.

ESI is extending Software Asset Management to the DoD Component level, and establishing a Virtual Information Technology Marketplace (VITM) for online purchasing. Go to the VITM Web site at <http://www.vitm.gov/> for more information.

*ESI Working Group Co-Chairs*

*Jim Clausen*

*Floyd Groce*

CHIPS

# MBGIE 2005

*The Joint and Combined Multi-Battle Group Inport Exercise achieves new level of excellence in wargaming simulation*

By Sharon Anderson

U.S. Navy and UK-coalition forces reached a new dimension in virtual wargaming around the globe when they replicated a composite warfighting scenario, Feb. 7-11, 2005, during the Joint and Combined Multi-Battle Group Inport Exercise (MBGIE). This was the first time joint (Army and Air Force) and coalition forces used the Navy's Continuous Training Environment infrastructure and Joint Forces Command's Joint Training and Experimentation Network for training.

The NCTE and JTEN enabled real-time battle simulation aboard ships and with Air Force and Army training simulators. The Joint Semi-Automated Forces and Battle Force Tactical Training systems realistically simulated at-sea warfighting conditions.

The 56-hour virtual exercise duplicated all the fierce intensity of warfare attaining an unprecedented level of reality in wargaming simulation, according to Capt. Mark Nesselrode, commanding officer of the Tactical Training Group Atlantic (TACTRAGRULANT) in Dam Neck, Va.

"It was a new experience for everyone involved. For example, in previous simulations, if someone ran out of fuel, that was OK, they could stay in the game. But in this exercise, people had to watch their fuel and speed. If they began to run low, we could restrict their speed, and they had to tell us how they were going to refuel to stay in the game," said Nesselrode.

Forces participating in the exercise included: in Norfolk, Va., Kearsarge Expeditionary Strike Group staff, embarked in USS Kearsarge; U.K. Marine Forces, representing the UK battle staff, embarked in USS Kearsarge; USS Anzio (CG 68); USS Roosevelt (DDG 80); USS Kearsarge (LHD 3); USS Ashland (LSD 48); USS Ponce (LPD 15); USS Normandy (CG 60); USS Gonzalez (DDG 66); USS Kauffman (FFG 59); USS Mitscher (DDG 57); USS Mahan (DDG 72); USS Hawes (FFG 53); USS Scranton (SSN 756); in Mayport, Fla., USS John F. Kennedy (CV 67); in Tinker, Ok., Air Force 552nd Operation Support Squadron; in Niantic, Conn., Air Force 103rd Air Control Squadron; in Ft. Bliss, Texas, Army 31st Air Defense Artillery Brigade; and UK-coalition forces in Portsmouth, England, HMS Edinburgh and HMS Westminster.

UK Royal Navy Lt. Cmdr. Alasdair Ireland, staff operations officer for the UK maritime battle staff said the value of virtual training is centered in the opportunity to ensure seamless interoperability between partners — before a crisis occurs.

"This was the first time that our simulations have been integrated, and it has given us a higher level of understanding of how to work together," Ireland said.



*Norfolk, Va. (Feb. 9, 2005) - United Kingdom Royal Navy Lt. Cmdr. James Buck, representing the UK battle staff embarked aboard the USS Kearsarge (LHD 3), participates in the MBGIE. U.S. Navy photo by Photographer's Mate 2nd Class Greg Roberts.*

According to Capt. Nesselrode, having British naval commanders participating provided valuable insight into the UK's rules of engagement.

"In the past, we would just act as if British forces were doing a certain part of the scenario, but it didn't happen that way in this exercise. We had to work within the UK's naval warfighting doctrine," said Nesselrode.

The MBGIE scenario encompassed continuous wartime planning and execution and allowed participants the opportunity to train at all levels. It promoted coordination between warfare commanders, executed joint and combined battle force operations, and familiarized crews with real-time joint and combined operations in both a high-tension and combat environment.

On the Kearsarge, watchstanders in the combat information center (CIC) and flag plot room were deeply engaged in the battle rhythm of the interactive scenario. Lt. Cmdr. Sean Anderson, assistant operations officer, and training and readiness officer, said the simulation duplicated the feeling of being underway.

"We are using SIPRNET, which is for U.S. forces only, datalinks, Voice over Internet Protocol (VoIP), radio circuits, chat, satellite communications and the Combined Enterprise Regional Information Exchange System (CENTRIXS) to communicate with the UK — the same networks and communications we would use in real combat," said Anderson.

It took two weeks to install the complex simulation technology on the USS Kearsarge, but the training benefits were enormous, according to Capt. Edward Barfield, commodore for Amphibious Squadron 8.

“Virtual training is cost effective and saves valuable time,” said Barfield. “What is unique about MBGIE is that our joint and coalition forces were geographically dispersed worldwide. With the level of sophistication of this technology, we had all the urgency and reality of real combat. The systems we used are exactly the same systems we would use in warfare.”

Expeditionary Strike Group Training involves the tactical operational levels of war. The commodore and Marine Expeditionary Unit (MEU) commander ensure their staffs’ ability to utilize the organic forces of the ESG and collaborate effectively with other naval forces, joint forces and coalition partners. To achieve the high performance capabilities envisioned for the ESG more complex training is required.

Another advantage of simulation training involves a quality of life benefit for Sailors: Personnel do not have to leave home. On the Kearsarge (which deployed in support of the global war on terror in March), Operations Specialist 1st Class (SW/AW) Chris Shields said virtual training gives him more time with his family.

“In the past, to get this level of training the ship would deploy for three weeks, but with simulation training we can get the same training and not have to leave port,” said Shields.

Results and training effectiveness were measured at TACTRAGRULANT’s impressive 15,000 square-foot modeling and simulation facility. Three huge screens dominated the Tactical Floor and a changing, highly charged staff of about 25 monitored the events of the exercise. In contrast to the quiet intensity of the watchstanders on the Kearsarge, the Tactical Floor seethed with excitement as evaluators responded to the events of the exercise.

According to Capt. Nesselrode, there were 1,350 individual simulations conducted over 56 hours of game play with unique metrics applied to each event.

“Each event was built into a scenario that played over a geographic area that stretched from Jacksonville, Fla., to Norfolk, Va., inland as far as Tennessee, and out to about 300 miles at sea,” Nesselrode said. “This scenario provided a back drop for four different Strike Groups under evaluation.”

On the Tactical Floor, TACTRAGRULANT’s Cmdr. Tom Pieluszczak, Joint Force Air Component Commander (JFACC) Module Head, and Cmdr. Al Kohnle, Modeling & Simulation Department Head, said watchstanders and battle commanders responded to the same types of scenarios that they would encounter in real warfare.

About 75 percent of ship combat operations can be reproduced synthetically, according to Pieluszczak. “But there is about 25 percent that can’t be simulated. You can simulate Tomahawk strikes and the Anzio can track the missiles on radar. Real mistakes can even be made in simulation, but some things, like cer-



*The combat information center (CIC) aboard the USS Kearsarge. The 56-hour virtual exercise duplicated all the fierce intensity of warfare achieving an unprecedented level of reality in wargaming simulation. The simulation had an “underway feel” without pulling up anchor, according to Capt. Edward Barfield, commodore for Amphibious Squadron 8.*



*Capt. Allyson Caddell, Joint Force Air Component Commander (JFACC) and Capt. Mark Nesselrode, commanding officer TACTRAGRULANT on the Tactical Floor at TACTRAGRULANT where MBGIE results and training effectiveness were measured.*

tain ship movements or tactical maneuvers can’t be duplicated,” said Pieluszczak.

Participants received immediate feedback on each completed event.

“We used a spreadsheet for evaluation. There was also room for editorial comments to further explain results. We saw what went

well and what we needed to do better," said Nesselrode, "and if we saw something that we are not getting right, we know we have to improve training."

Capt. Allyson Caddell, JFACC, said that if an event does not go as planned after several attempts, it means that training thus far has not been effective. "It doesn't mean the watchstanders or ESGs did something wrong; it's a clear signal to us that we didn't provide the right training, and we have to fix that," Caddell said.

"We can currently capture about 280 different Navy Tactical Tasks, with about 950 individual measurements for a Strike Group," said Nesselrode. "Air wing operations were also measured, and there were about 400 specific tasks that were evaluated. We targeted 236 of these tasks for the Kearsarge ESG evaluation. Since an ESG has a far different type of air component and involves a U.S. Marine Corps Expeditionary Unit, there are different tasks, and tasks that are Marine Corps-specific that we do not yet measure."

"We also evaluated the Mahan/Mitscher/Hawes Surface Strike Group (SSG), but they were evaluated against a much smaller number of tasks (approximately 80 at the present time) since they have a much narrower mission scope. Finally, we are beginning to evaluate returning Strike Groups, and we are working on the tasks that are appropriate for a group, such as the USS John F. Kennedy Strike Group while they are sustaining readiness. Eventually, we will evaluate the same number of tasks (about 280 for the SSG without its air wing) for a returning group just as we do when a Strike Group is certified to deploy," Nesselrode said.

The results of the exercise will be combined with previous evaluations for the Kearsarge ESG and then a recommendation for certification and further training requirements will be sent to Rear Adm. Reubin Bookert, Commander, Amphibious Group Two, Rear Adm. Richard Gallagher, Commander, Strike Force Training Atlantic and finally to Vice Adm. Mark Fitzgerald, Commander Second Fleet for approval.

"Any recommendations for changes to the training or conduct of the exercise are also forwarded the same way," Nesselrode said.

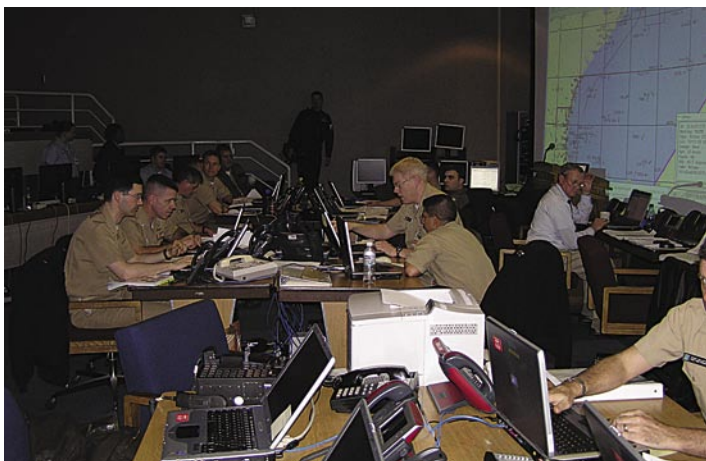
Capt. Nesselrode explained how the metrics are evaluated against the Fleet Response Plan (FRP). The FRP provides a logical framework to successfully train Strike Groups. Each major event, whether live or synthetic, permits observation and evaluation. As a Strike Group moves from being emergency surge capable to deployable, the level of complexity of the training is increased, as is the necessity to actively integrate with and sometimes control both joint and coalition forces.

"There are metrics which apply throughout this process, some apply only in a live environment, some can only be tested in a synthetic environment, and some require the inclusion of joint and coalition forces," Nesselrode said.

The metrics for each event are tailored to either reinforce major training requirements or to capture those events that are required at each successive level of complexity. Typically, by the end of training at least 90 percent of all possible training is ob-



*TACTRAGRULANT's Cmdr. Tom Pieluszczak (left) JFACC Module Head and Cmdr. Al Kohnle Modeling & Simulation Department Head closely monitored MBGIE results and training effectiveness.*



*TACTRAGRULANT's Tactical Floor where staff monitored the progress of MBGIE participants as they responded to 1,350 individual simulations conducted over 56 hours of game play. Unique metrics were applied to each event with participants receiving immediate feedback after each event was completed.*

served, and the ability to send a Strike Group forward, for whatever phase of the FRP is required, is well-understood.

"At the conclusion of the exercise, participants were debriefed with our immediate recommendations," said Nesselrode. "This is the same process followed for Carrier Strike Groups and now Surface Strike Groups."

Wargaming extends precious training dollars and, more importantly, saves valuable time in combat, since forces have already tested and integrated technology into the battle plan. Joint and coalition communications can be tested to ensure seamless interoperability, and joint and coalition forces will be disciplined and synchronized to respond to a multitude of global threats.

*Ms. Anderson is the CHIPS senior editor. Thanks to the TACTRAGRULANT staff and Capt. Mark Nesselrode, commanding officer of TACTRAGRULANT for his invaluable assistance with this article.* CHIPS

# A DESIGN PROCESS FOR FORCENET EXPERIMENTATION

By Brad Poeltler and Dr. Shelley P. Gallup

FORCENet is the core of Sea Power 21 and Naval Transformation, and it is the Navy and Marine Corps vehicle to make the CNO's vision of network-centric operations/warfare an operational reality. FORCENet is the command and control pillar that gives speed and agility to the commander. The commander can then optimally employ Sea Strike, Sea Shield and Sea Basing by integrating weapons, sensors, reachback centers and warfighters at all levels into a secure networked, distributed combat force — the Naval contribution to the Global Information Grid (GIG).

Navy leadership must have accurate and timely data to make well-informed decisions about future FORCENet capabilities. The Naval Network Warfare Command (NETWARCOM), the operational agent for FORCENet, has created a series of annual events to supply these data points. These events are collectively called Trident Warrior (TW).

"What makes Trident Warrior different from other naval assessment events is the level of detail of the analysis data. That level of detail can be attributed to the Trident Warrior process," says Capt. Chris Abbott, director of FORCENet Innovation and Experimentation. "The strict compliance to this process is what ensures event consistency and allows us to maintain a high standard in our FORCENet assessments."

A 13-step process was established to produce the experimenta-

tion objectives, experiment design, planning requirements and assessment needs, shown in Figure 1. This process was not simply invented from scratch. It evolved from experience with former Fleet Battle Experiments, from the Modular Command and Control Evaluations System (MCES) and from the Code of Best Practices in Experimentation (COBPE), produced by the Command and Control Research Program (CCRP).

This process may look fairly routine by most research standards, but what makes it unique is the in-depth development of the objectives (step 5), the detailed models that are developed for each objective (step 6), and the computer-based, enterprise environment designed for Trident Warrior planning and execution, the FORCENet Innovation and Research Enterprise (FIRE).

As mentioned, the TW process begins as any large event with planning team development, concept design, target technology/procedural selection and asset identification. But beginning with step 5, objective development, TWs begin to differ. "This step is critical to the success or failure of the event," says Cmdr. Tony Parrillo, director of TW05. "Each critical question that is identified as a FORCENet issue is developed as a TW objective with the final assessment always in focus. That is what we call the 'so what' element of Trident Warriors. If it does not meet the so what test, that is, answer a major FORCENet question, we drop that objective and move on."

Figure 1. Trident Warrior Process

Phase	1	2	3	4	5	6
<b>Due Dates</b>	Pre-CDC	CDC	Pre-IPC	Pre-IPC	Pre-MPC	Pre-MPC
<b>Step</b>	Establish Team	Concept Development	Technology/TTP Harvest	Asset Identification	Develop Experiment Objectives	IDEF/OSD/Process Action Maps
<b>Required Product</b>	Defines Names and R/R	Defines Experiment Scope and Focus Areas - Insure aligns with Naval Vision	Defines and Researches selected Tech and TTPs	Platforms Ded and Install Scheduled	Defines the <i>So What</i> and how to measure	Turns the words into design diagrams

Phase	7	8	9	10	11	12	13
<b>Due Dates</b>	Pre-MPC	Pre-FPC	Pre-FPC	TBD	TBD	TBD	TBD
<b>Step</b>	Experiment Design	Event Definition	Data Collection Plan	Execution	Final Report	Assessment OAA	MUA
<b>Required Product</b>	Lays out the flow and applicable scenarios to meet objectives	Defines the detailed execution plan	Maps the data to be collected to the means	Insure plan is flexible to changing environment	Must be quick and good	Necks down analysis to assessment	Necks down assessment to DOTMLPF recommendations

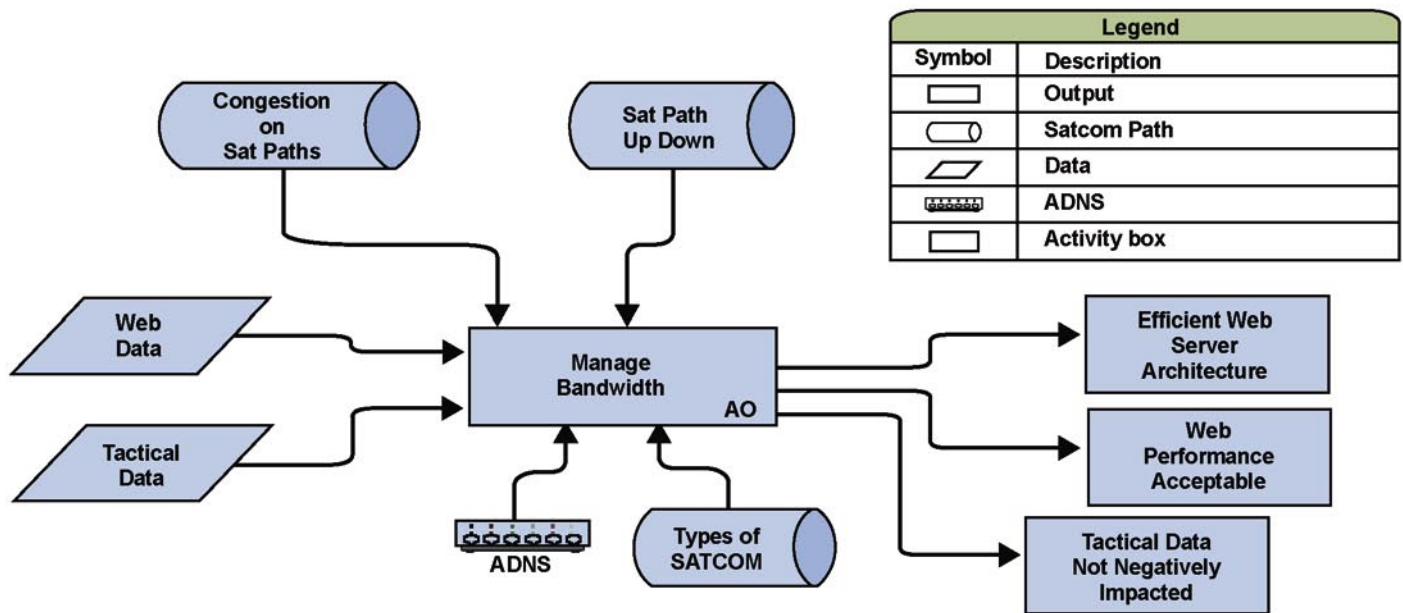


Figure 2.

TW objectives are broken down into exceptional detail by decomposing each into the following eight categories: (1) objective statement (a high-level description of what the objective is intended to produce); (2) FORCENet questions to be answered; (3) the information goal (intent of the assessment); (4) operational conditions required to produce valid data relevant to the question being asked; (5) systems conditions required; (6) information conditions required; (7) measures and metrics that will be collected and; (8) the data required to produce the assessment which meets the objective statement. This step can take several months to complete because a typical TW can generate up to 150 separate objectives. But when these questions are correctly focused at the right level of detail the rest of the event design is optimized.

Once the objectives are identified then the TW planners begin step 6 – construction of models. For each of the objectives, a model is produced, beginning with a generalized model using Integrated Definition 0 (IDEF0) as a basis, shown in Figure 2. This is followed typically by an Operational Sequence Development model. This work has obvious purposes, such as identifying requirements that drive planning. But another purpose is to produce common descriptions for each objective that are then used for collaboration across all TW objectives. This process produces a much higher integration of experiment design and supports the “system and system-of-systems” view that is at the core of FORCENet.

Modeling, common to systems analysis and systems engineering, is designed with the final assessment in mind, and it can incorporate emerging planning requirements. This focus helps identify the critical points for training, event design and data collection. Figure 2 shows TW04 diagrams for the FORCENet bandwidth management objective.

The IDEF model uses a standard syntax and set of simple rules in which a verb phrase in the central box describes what is to

be achieved. Inputs enter the left side of the box, controls enter from the top, resources from the bottom and output to the right. At the highest level, each IDEF0 models the requirements for an objective.

From the initial IDEF0 model, a more complete description of the system components and their relationships to each other can be combined in an Office of the Secretary of Defense (OSD) view, such as the one shown in Figure 3. This view does not replace other architecture, engineering and systems views common to systems engineering; however, as a high level description of the system, it is invaluable to further planning and experiment design.

These two modeling diagrams become the principal visual reference used in the remaining TW planning steps including event design and development of the data collection plan. Another benefit of this TW step is that many of the objectives developed for a TW are cognitive in nature rather than technical. These diagrams when applied to human system interface (HSI) questions provide insight into refinement of tactics, techniques and procedures (TTP) data collection and assessment requirements.

The final unique feature of the TW process is the FORCENet Innovation and Research Enterprise (FIRE). FIRE was developed out of the need for structured data collection, data reconstruction for analysis and generation of TW analysis reports. No such system previously existed, and the Naval Postgraduate School (NPS), the analysis lead for TW, was asked to examine different approaches. NPS developed FIRE as an enterprise computing solution, based on Oracle 9i and Oracle 10g technology, with unique artificial intelligence (AI) applications included in the design.

Final results from TW reports are connected to FORCENet concepts, experiment objectives and modeling diagrams down to the data. In the past, constructing this design was exceedingly time consuming and manpower intensive. But FIRE makes this process quick and easy.

### 1.1.1N

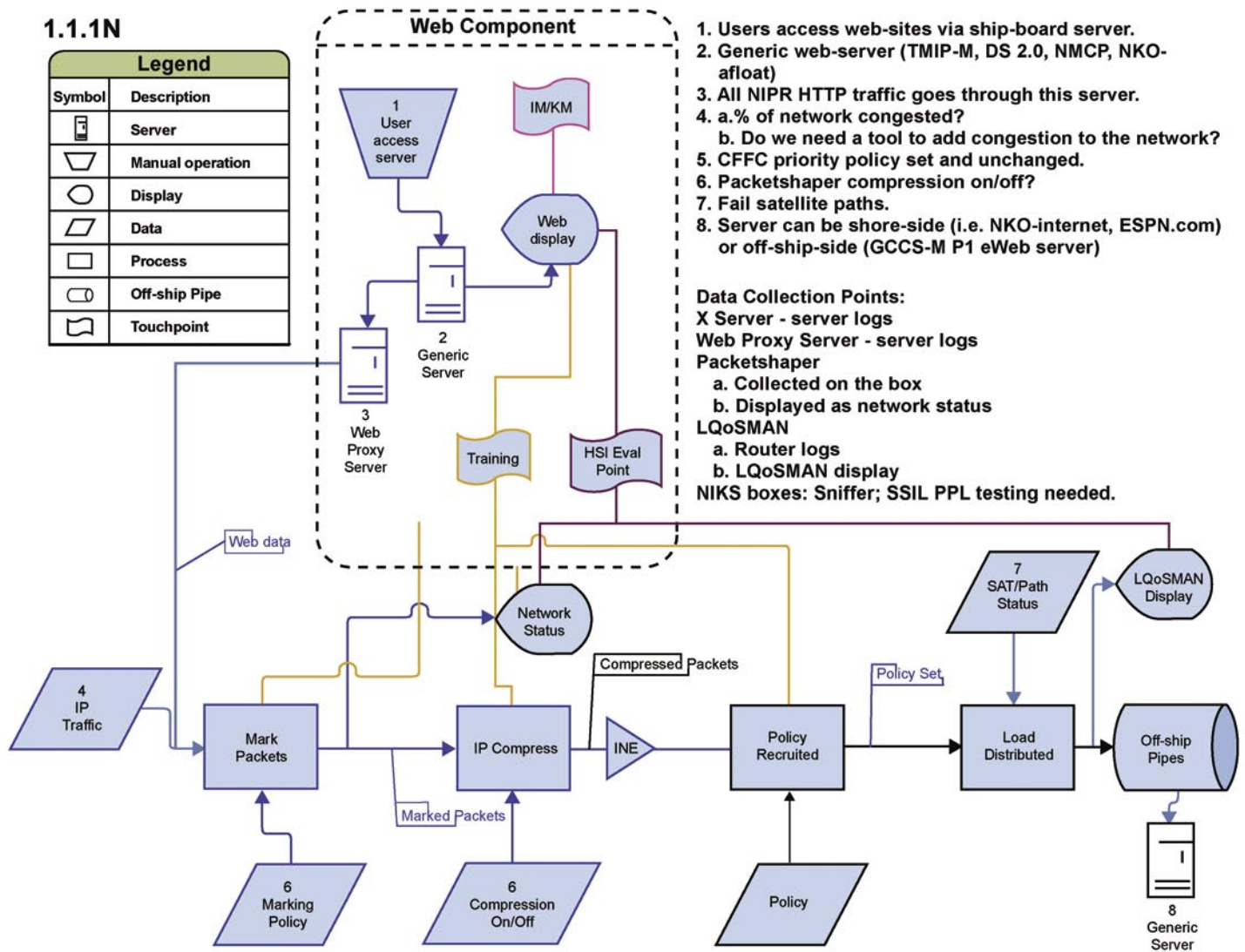


Figure 3.

TW planning is greatly dependent on collaboration among a wide range of experts, military, government and contractor personnel, who all need to access data. FIRE uses artificial intelligence tools to search across a broad set of information, for example, lengthy documents and chat files, where planners are trying to pull specific data that typically take a long time to manually search. Fuzzy logic tools are used to gather the best approximation of the required data from the document.

Although requirements may seem unduly strict, this degree of rigor results in a level of detail that is necessary for making critical FORCENet decisions. Several of the recommendations resulting from earlier TW exercises have resulted in major modifications to ship installation schedules and future FORCENet capability procurements.

"I have come to rely on Trident Warrior information and assessments," says Vice Adm. James McArthur, commander, NETWARCOM.

Furthermore, the Chief of Naval Operations Future Requirements Division (N7) has begun to utilize Trident Warrior as a primary

means for field testing Naval Capabilities Development Plan (NCDP) issues prior to critical Program Objective Memorandum (POM) decisions.

Trident Warrior 05 is currently being planned for a November/December 2005 execution utilizing the Iwo Jima (LHD 7) Expeditionary Strike Group in the Virginia Capes Operating Area (VACAPES). The FORCENet analysis objectives range from operational level command and control decision aids to coalition network design.

A detailed article describing TW05 will appear in the next edition of CHIPS.

*Mr. Brad Poeltler is a retired Navy captain and assistant director for Trident Warrior 04 and Trident Warrior 05. 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.*

# The Naval Personnel Development Command Bringing Human Capital Strategy to Life

*Human Capital Strategy is all about putting the right Sailors in the right place at the right time ...*

By JO1(SW/AW) John Osborne, Naval Personnel Development Command, Public Affairs

At the beginning of the year, Chief of Naval Operations Adm. Vern Clark challenged Navy leaders in his 2005 Guidance to develop a Human Capital Strategy (HCS) that would provide the Navy with tools to remedy the imbalances in community manning and retention, revise the ratio of restricted line officers to unrestricted line officers, and adjust infrastructure manning to better mesh with future technologies, concepts and initiatives.

The task of bringing HCS to life is the responsibility of many Navy commands that are already working in concert to demonstrate the potential power this strategy will have when brought to fruition. In order for HCS to be successful, it must be incorporated into the Navy's Revolution in Training (RIT) and Sea Warrior initiatives, a task that has, in part, fallen to the Naval Personnel Development Command (NPDC).

"We are moving with as much speed as possible toward the CNO's goal," said Rear Adm. Ann Rondeau, commander of NPDC. "We have Navy Knowledge Online (NKO), which is the delivery portal to Sailors for communication, mentorship, education and career progression tools. We have developed the Learning Centers, which are the homes for communities of practice where they can go to find resources they can utilize in their day-to-day work," she said.

"We are also developing the 5 Vector Model (5VM) in an automated fashion so that the Total Force leaders, supervisors and mentors can access the resumes of their personnel and ensure the individual is matched up correctly to the job he or she is being assigned. This is very important because we want to tie the training directly to the skill sets the Navy needs," said Rondeau.

With all of these developmental tools available and more on the way, it is not hard to understand why HCS is a major focus for the Navy in 2005. The strategy is based upon mission focus, total force, and achieving a work/life balance in a wartime Navy that delivers the right Sailors with the right skills at the right time for the right work.

Simply put, HCS is a view of how the Navy values its people and how leadership can use the genius of its people — the human capital resource — in a way that gives the best possible alignment to the current mission. This meshes directly with the RIT and falls under the larger umbrella of the Sea Warrior initiative.

Fred Bertsch, assistant chief of staff for Functional Integration Management (FIM) at NPDC, explained that the RIT brought two

models to the table that are in use today. The first was the human performance systems model, and the second was the 5VM. Understanding the symbiotic relationship between the two models is essential to understanding how the HCS will create a Sea Warrior who has the capability to access, develop, maintain, optimize and provide the human capital to meet the mission of the Navy.

"The human performance systems model said whenever you develop a solutions set for optimizing performance, you always start with the requirements. You then look at the solutions available to fulfill those requirements, and then you determine how best to integrate and implement it," Bertsch explained. "Next you execute — and the most important piece is to obtain feedback to measure and analyze. The final step is to provide feedback into the system. It's a closed loop process, which allows us to start to look at things through a systems model."

The 5VM provides the ability to look at a person in terms of skill set performance. Human capabilities are divided into four areas with a Performance Vector that allows leadership to measure how well a person is doing. The four other vectors are professional, leadership, personal development, and certifications and qualifications.

"We are trying to craft the 5VM as a spiral development process," Rondeau said. "The 5VM allows Sailors to see their development and allows leaders to see how the skills of Sailors, both officer and enlisted, fit mission needs and requirements. The more we can match Sailors' choices with mission requirements the better we can maximize mission capability and force capacity toward Sea Power 21."

The human performance systems model and 5VM, along with RIT and HCS, are part of the foundation for Sea Warrior. Sea Warrior brings together fleet requirements, distribution of manpower, personnel development and acquisition of new weapons systems. This ensures the Navy has the right inventory of people and equipment that are developed correctly from both a cultural (Navy basic training) and skills standpoint.

"When we put our people in a particular situation, we want to feel confident that they can handle the work that has been assigned to them at a standard that is acceptable to the Navy," Bertsch said. "We also want to make sure we are not spending money, time and effort on things that are not important to the Navy's core competencies."



Bertsch said a primary focus now in bringing HCS to life is automating learning capabilities in the schoolhouses. He concedes that the Navy will never and should never totally get away from having instructors and facilitators, but points out that shaping training into a “reusable format” that can be launched through an Integrated Learning Environment (ILE) is beneficial to both Sailors and the taxpayers who support them.

“In an ILE, Sailors have a far broader access and don’t have to be temporarily detailed or delayed en route to their units as much,” he said. “This saves the Navy and taxpayers money and also takes some of the burden off the back of Sailors. Sailors can move at their own pace, and those who take initiative can shine. That is what HCS is all about: Putting the right Sailors in the right place at the right time.”

Bertsch said they are also starting to align other systems to integrate with the 5VM. The Job Advertising and Selection System (JASS), once aligned, will allow Sailors to move seamlessly between the 5VM (the resume) and the available billets the detailer offers so they can have more choice as to where they go in the future.

Future counseling tools that are now in the works will integrate with Fleet Readiness Programs (FRP), such as the TYCOM Readiness Management System (TRMS), enabling Sailors to see where they fit into the larger picture. There are also plans for HCS to integrate with Resources in Distance Learning (RIDE) and the Joint Operational Information Network. Each of these initiatives will proceed with the objective of giving the Sailor as many options as possible in his or her career.

Rondeau sees HCS as a personification of the CNO’s covenant to provide Sailors with every opportunity to make the most of their careers. “The more we can provide Sailors choice and the capability to make decisions at the lowest level for their personal development, the better off the Navy is going to be,” Rondeau said.

“The Human Capital Strategy will provide a means by which Sailors take charge for their own careers, as well as their personal and professional development. It is the means by which we tie end-to-end Sailor capacity with strategic and tactical implications of Sea Power 21. It will allow us to link acquisition, force architecture and human systems integration with training and skills architecture. It will give our servicemembers the power to become the best possible Sailor, leader, technical expert or even parent or whatever that Sailor wishes to excel in,” Rondeau said.

*For more information on the Human Capital Strategy and the 5VM, visit Navy Knowledge Online at <https://www.nko.navy.mil/>. For more information about the Naval Personnel Development Command, Sea Warrior and the Revolution in Navy Training, go to NPDC’s Web site at <https://www.npdc.navy.mil/>.*

CHIPS



Naval Network Warfare Command (NETWARCOM) is leading a revolution in the way the Navy and Marine Corps will fight and operate. As Navy’s operational type commander for global C4 (command, control, computers and communications), naval networks, space and information operations, NETWARCOM spearheaded the drafting of the FORCEnet Functional Concept with the Marine Corps Combat Development Command (MCCDC).

The document, signed Feb. 7 by the Chief of Naval Operations and Commandant of the Marine Corps, focuses on exploiting the power of networking decision-makers at all levels, from an individual in the field to a command headquarters, giving naval forces the speed and agility to dramatically improve overall combat effectiveness and mission accomplishment.

The Functional Concept is viewed as a critical step in delivering fast and agile Naval Forces for the future. It sets in motion a new era for Navy and Marine Corps operations, one where networks will move and share information to provide unprecedented situational awareness, firepower and seamless alignment with joint and coalition forces. The functional concept identifies 15 capabilities which the Navy and Marine Corps will use to build the supporting architecture, doctrine, organization, training and supporting systems for FORCEnet. The concept serves as the naval command and control component of Sea Power 21 and expeditionary warfare. Specifically, the FORCEnet Functional Concept:

- Supports Navy leadership’s demand for speed and agility to implement the Services’ future warfighting visions;
- Outlines enterprise-wide systems and processes supporting the Sea Power 21 warfighting pillars: Sea Shield, Sea Strike and Sea Basing as well as the Sea Power 21 enabling processes: Sea Warrior, Sea Trial and Sea Enterprise;
- Enhances alignment of a FORCEnet operational fleet-centered perspective with acquisition and programmatic efforts into a coherent co-evolution of organization, processes and technology;
- Accelerates fleet implementation of FORCEnet capabilities for command and control through requirements development and experimentation;

- Aligns enterprise business processes with fleet readiness;
- Ensures the Navy and Marine Corps operations are consistent with Joint Vision 2020, Joint Operating Concept, and Joint Battle Management Command and Control; and
- Empowers our Sailors and Marines by providing unprecedented operational agility accelerating the pace of combat through speed of maneuver and increased range of engagement.

The FORCENet Functional Concept was developed under the Joint Capabilities Integration and Development System (JCIDS) process; derived directly from the Naval Operating Concept (2015-2020) for Joint Operations. It fully supports the Department of the Navy vision of Naval Power 21 and the supporting strategies of Sea Power 21 and Marine Corps Strategy 21.

Commanders will use FORCENet “infostructure” to make the best possible decisions faster, according to the concept’s operational definition. Infostructure is the fusion of information and C4 systems, supported by enterprise-wide doctrine, organization, training, material, leader development, personnel and facilities (DOTMLP-F).

“Enterprise-wide refers to not just the ‘trigger pullers’ within the Navy and Marine Corps, but also other aspects of the naval force and throughout the Services,” said Capt. Rick Simon, deputy director for FORCENet at NETWARCOM, headquartered in Norfolk, Va.

“I’m talking supply, medical, meteorology, etc., . . . all those things that support the warrior pulling the trigger. Additionally, it directly relates to how naval forces will ‘plug into’ and share information with coalition and joint partners,” said Simon.

FORCENet will accelerate command and control (C2) capabilities by changing the way information moves. FORCENet will improve the performance of the OODA (oo-DAH) Loop, Observe, Orient, Decide and Act, through shared situational awareness and feedback, decentralized command and a collaborative approach to problem-solving that opens new ways for the commander’s intent to be executed.

FORCENet creates opportunities for commanders by providing them with processed, timely, actionable information — knowledge, not just data. Better processing of available data to provide time-sensitive information will allow the commander to know where to put his carrier strike group, or better yet, where not to. “If you’re approaching a bad guy’s coast and he’s got subs, you’re going to want to know more about those areas so you can better plan where the enemy might be hiding,” Simon noted.

“With FORCENet capabilities, you’ll be able to steer your strike group away from those places where subs could be and keep your ships out of danger, or you may be able to go on the offensive when the enemy least expects it and from a direction he least anticipates. FORCENet should allow the commander to choose the terms of the engagement and to do it in such a way that the enemy cannot tolerate our actions,” said Simon.

FORCENet will also use future technology to allow a smaller, more efficient Navy to meet national security objectives. FORCENet will permit a smaller Navy to conduct more efficient use of its intelligence, surveillance and reconnaissance (ISR) working with its Air Force and Army equivalents: C2 Constellation and Land-WarNet, respectively.

A major issue the Navy faces today is that the information-gathering ability of sensors is evolving faster than the network’s ability to carry the information to the warfighter. FORCENet will enhance the Navy’s situational awareness by enabling improved ISR through an increased data-carrying capacity of naval networks so the networks can “catch up” to the capacity of ever-evolving sensors. The increased capacity will, in turn, allow users in the fleet to reach-back to analysts who can interpret the data.

FORCENet will ensure naval networks are built with compatible components used by the other Services to allow seamless interaction between all the branches, as well as with the Global Information Grid (GIG), the much larger-scale network run by the Department of Defense. FORCENet is the naval component of the GIG, which will be connected to the more than 160 major military installations worldwide. According to Simon, FORCENet is born joint. “It’s meant to be interoperable with the GIG. It’s meant to share the same protocols, backbone, satellites and bandwidth expansion as the other Services. In fact, all of the architecture we’re developing is being integrated into the joint vision.”

FORCENet will allow commanders as well as individual units to fully exploit the GIG. “We’re at the crossroads, the merger of all aspects of FORCENet,” explained Vice Adm. James D. McArthur, NETWARCOM commander. “Success will require aligning the systems, the processes, the acquisition, the programmatic and the experimentation needed to bring speed to capability.”

The FORCENet Functional Concept takes aim at the years 2015-2020. 2020 is the target point for all the Services to be interoperable and compliant with Joint Vision 2020, which is the Joint Staff’s strategic direction for achieving joint force full-spectrum dominance using a smaller, faster, smarter and more lethal military service. By choosing this time frame, the functional concept aims to field FORCENet capabilities past the current Planning/Programming/Budgeting/Execution process, yet be close enough to allow industry an objective to build toward.

FORCENet is the naval component of Joint C2 and expeditionary warfare. FORCENet is also the business component of the Naval Enterprise Network. Supporting the warfighter must include the business element of logistics and shore infrastructure. Agile business operations require robust knowledge management and information. Net-centric operations include forward and home-based support. FORCENet will facilitate the best possible decisions, and will use future technology to allow a smaller, more efficient Navy to meet national security objectives.

*For additional information on the FORCENet Functional Concept, contact the Naval Network Warfare Command Public Affairs Office at (757) 417-6796 or visit the FORCENet Web site at <http://forcenet.navy.mil/>.*

CHIPS

# DON CIP: A COMPREHENSIVE SOLUTION TO IMPROVE CYBER AND PHYSICAL SECURITY OF DON CRITICAL ASSETS

By Donald Reiter, Lead for the Department of the Navy CIP Program

A primary goal of the Department of the Navy Information Management/Information Technology (IM/IT) Strategic Plan is "providing Full Dimensional Protection (FDP) that ensures Naval warfighting effectiveness." FDP involves three initiatives: Critical Infrastructure Protection (CIP), Information Assurance and Privacy. This article provides an overview on the DON CIP initiative.

## What is Critical Infrastructure Protection?

CIP is mission assurance: the identification, assessment and assurance of cyber and physical assets essential to the mobilization, deployment and sustainment of U.S. military operations. Effective critical infrastructure protection identifies vulnerabilities and risks to critical assets supporting warfighting missions, remediates those validated vulnerabilities to protect against compromise, and, if compromised, minimizes impact to mission performance with effective consequence management plans and procedures.

## The DON Approach to CIP

The Department of the Navy Chief Information Officer (DON CIO) was appointed the collateral duties of the DON Critical Infrastructure Assurance Officer (CIAO)

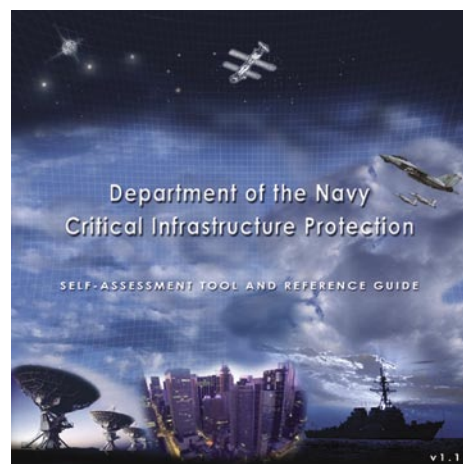
in 1999 by the Secretary of the Navy to "provide a comprehensive approach to protecting the Department's critical infrastructures."

Following federal government and DoD guidance, including Executive Order PDD-63 of May 1998 and the DoD CIP Plan of November 1998, Secretary of the Navy Instruction (SECNAVINST) 3501.1 formally established DON policy, structure, and responsibilities for implementing CIP throughout the Department. The DON CIAO was given responsibilities that ranged from serving as the DON's central point of contact for CIP-related issues to sponsoring and executing a new Naval Integrated Vulnerability Assessment (NIVA) program.

The execution of these responsibilities has resulted in a fully operational, highly regarded CIP program. An independent audit commissioned by the DON CIO to assess the Department's progress concluded that "Both the DON policy and DON CIO implementation of the policy are among the best-founded and complete programs within the federal government."

## The DON CIP Initiative

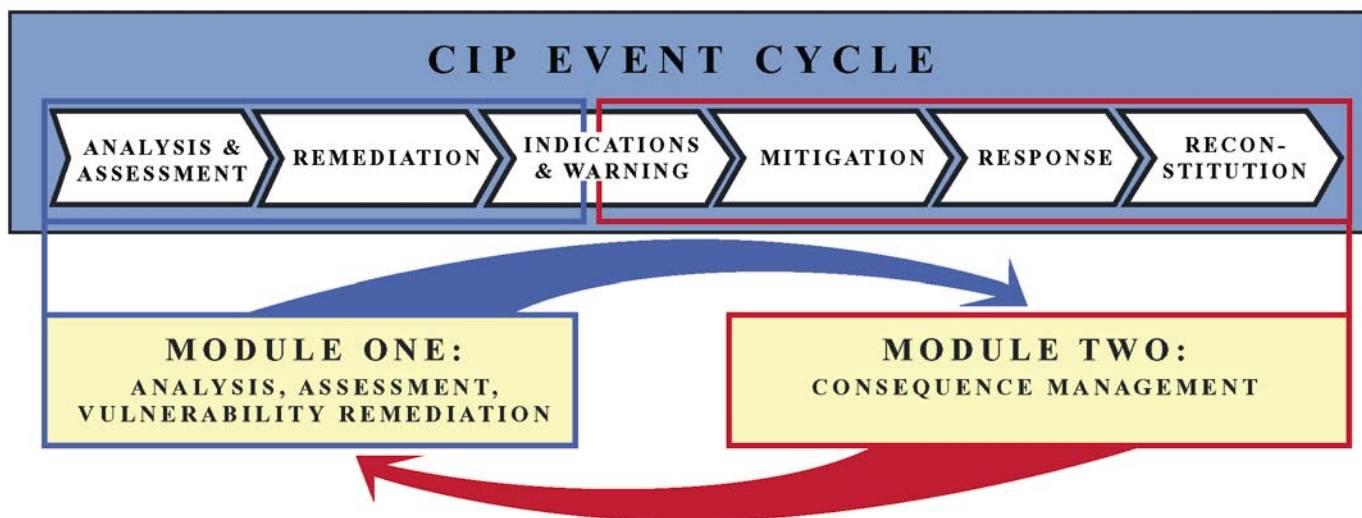
The DON CIAO structured efforts around the government-recognized CIP Event



*The CIP Self-Assessment Tool and Reference Guide enables a four-pillar assessment for those installations not scheduled for a Naval Integrated Vulnerability Assessment.*

Cycle (see Figure 1). This six-phase series of activities identifies actions necessary to: identify and assess critical assets, remediate significant vulnerabilities to such assets before an incident occurs, and pre-plan and maintain actions to ensure continuity of operations during and after an incident. The DON CIP Team has developed or implemented processes and tools that address all of the requirements of this event cycle (see Figure 2). A brief summary of

**Figure 1. The CIP Event Cycle identifies activity phases essential to an effective CIP Program.**



these processes and tools is provided in the following paragraphs.

## DON CIP Processes and Tools

### Analysis & Assessment

Naval Integrated Vulnerability Assessments (NIVA) are multidisciplinary efforts involving four assessment pillars. Each pillar involves a distinct protocol and assessment focus, summarized below.

- **Antiterrorism/Force Protection (AT/FP)** assesses an installation's physical asset vulnerability to compromise; e.g., perimeter controls/protection, building security and guard forces.
- **Computer Network Defense (CND)** identifies vulnerabilities to cyber assets, e.g., computer networks, industrial controls, data retrieval and storage systems.
- **Commercial Dependency (CD)** assesses dependencies on off-base commercial utilities, e.g., water, telecommunications, power and transportation.
- **Consequence Management (CM)** planning evaluates plans and procedures that support continuity of operations throughout a disruptive event.

As illustrated in Figure 3, different organizations may be involved according to pillar and asset owner. NIVAs are conducted on installations containing DON critical assets to determine whether significant

vulnerabilities exist that could jeopardize mission support if compromised. Identifying such vulnerabilities initiates a remediation and consequence management chain of events to protect those assets and assure they remain available to DON warfighters.

The DON CIAO has coordinated NIVAs in the National Capital Region, Mid-Atlantic Region, Naval District Washington, Navy Region Hawaii, Navy Region Northwest, Navy Region Southeast and Navy Region Southwest. The first NIVA outside of the continental United States (OCONUS) was conducted in October 2004 on Navy assets in Naples, Gaeta and Sigonella, Italy.

For those installations not scheduled for a NIVA, the Self-Assessment Tool and Reference Guide compact disc is available to Department personnel to enable a four-pillar self-assessment.

The Critical Asset List (CAL) is a catalog of Navy and Marine Corps assets designated as essential to the National Military Strategy. The CAL, periodically updated by the Office of the Chief of Naval Operations and Headquarters Marine Corps, influences NIVA candidate sites and allows the Department to focus limited assessment and remediation resources on assets deemed most critical.

### Remediation

Remediation corrects vulnerabilities found during assessments to protect them from

compromise and make them a less attractive target. The Remediation Planning Guide, published in summer 2004, provides a methodology and plan of action that assists DON entities in developing vulnerability remediation strategies that balance resources and risk. The goal is to achieve maximum return on investment while focusing limited resources on remediating the most essential assets.

### Indications & Warning

The Critical Asset Management System (CAMS) is an accredited and operational stand-alone system that resides in the Naval Criminal Investigative Service (NCIS) Multi-Threat Alert Center. CAMS is the single DON CIP repository for Critical Asset List and vulnerability assessment information.

### Consequence Management

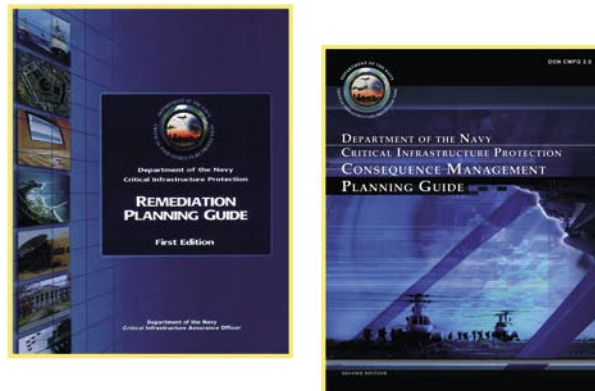
CM Assessments review how an activity's CM planning supports its overall continuity of operations. The DON CIP CM Team has reviewed over 175 CM plans since the CM pillar was added to the NIVA protocol in 2002.

The DON CM Planning Guide (Version 2.0) provides methodology and guidance to assist CM planners with developing strategies and plans that will maintain continuity of operations during or after an event. This second edition, which has just been distributed, incorporates expanded guidance as well as information requested by first edition users.

Figure 2. DON CIP processes and tools have been developed to address the specific needs of the CIP Event Cycle.

CIP EVENT CYCLE	DON PROCESS TOOL
ANALYSIS & ASSESSMENT	<ul style="list-style-type: none"> <li>✓ NAVAL INTEGRATED VULNERABILITY ASSESSMENT</li> <li>✓ CRITICAL ASSET LIST</li> <li>✓ SELF ASSESSMENT TOOL</li> <li>✓ DEFENSE INDUSTRIAL BASE SURVEYS</li> </ul>
REMEDIATION	<ul style="list-style-type: none"> <li>✓ REMEDIATION PLANNING GUIDE</li> </ul>
INDICATIONS & WARNING	<ul style="list-style-type: none"> <li>✓ DON CRITICAL ASSET MANAGEMENT SYSTEM</li> </ul>
MITIGATION	<ul style="list-style-type: none"> <li>✓ CONSEQUENCE MANAGEMENT PLANNING GUIDE</li> <li>✓ CONSEQUENCE MANAGEMENT PLANNING ASSESSMENTS</li> </ul>
RESPONSE	
RECONSTITUTION	

## FOUR-PILLAR NAVAL INTEGRATED VULNERABILITY ASSESSMENT (NIVA)



THE REMEDIATION PLANNING GUIDE AND THE CONSEQUENCE MANAGEMENT PLANNING GUIDE ARE AVAILABLE TO DEPARTMENT PERSONNEL ON THE DON CIAO WEBSITE.

Figure 3. Naval Integrated Vulnerability Assessments look for significant weaknesses that could jeopardize mission support.

### Defense Industrial Base Surveys

Defense Industrial Base (DIB) surveys review the production and delivery systems of DIB entities viewed as critical to sustaining warfighting readiness. Since 1999, 62 surveys have been completed involving DIB production of major Navy or Marine Corps weapons systems.

Based on one survey, the first commercial NIVA was conducted at a manufacturer's site. These surveys find important information and have influenced positive change in the sustainment of DON weapons systems, including establishing second manufacturing sites and moving to domestic versus foreign production.

### Education and Outreach

Institutionalizing CIP throughout the DON is a primary goal implemented by education and outreach efforts. Early accomplishments include the first course on CIP presented at the Naval Postgraduate School. Recent achievements include the following initiatives.

✓ The Web-based DON CIP Course is an interactive multimedia suite of instructional courseware that defines the DON CIP initiative and the roles and responsibilities of DON personnel in an effective CIP program. The four modules are categorized as Navy Courses DONCIAO-5862-1, 2, 3, 4 and Marine Corps Courses DI5500A, B, C, D.

These courses are available to Department personnel worldwide through the Naval Education Training Professional

Development Technology Center (NET-PDTC) e-learning and the MARINET portals at <https://www.nko.navy.mil> and <http://www.marinet.usmc.mil>, respectively. This course is being considered as the model for the development of a Joint Staff sanctioned course on CIP.

✓ Wargame participation involves adding CIP scenarios to wargames and is an effective approach to bringing all facets of CIP to a wide audience. CIP scenarios are based on real NIVA cases in which vulnerabilities were identified.

✓ Efforts to add CIP traditional school-house curricula are receiving more emphasis. The most recent opportunity is the Commanding Officer Anti-Terrorism (COAT) Course given by the Center for Anti-Terrorism and Navy Security Forces at the Naval Amphibious Base, Little Creek, Va.

Also on the drawing board are the Senior Officer CIP Course for CAPSTONE, CIP Executive-Level Seminars and guest lecture briefings to DON students.

### The Way Ahead

With a comprehensive program now in place, future activities will emphasize institutionalizing CIP throughout the Department.

Today's compelling challenges to mission assurance call for a proactive CIP initiative. Continuing to build on the achievements made to date and setting new goals to

### CIP Tools and Guides

The Self-Assessment Tool compact disc, Remediation Planning Guide and Consequence Management Planning Guide are available to Department personnel and are especially valuable for base commanders and installation owners.

Tools and guides are available from the DON CIAO Web site at <http://www.doncio.navy.mil/>, then select the Products tab.

The Web-based DON CIP Courses are available to Department personnel worldwide through the Naval Education Training Professional Development Technology Center (NETPDTC) e-learning and the MARINET portals at <https://www.nko.navy.mil> and <http://www.marinet.usmc.mil>, respectively.

improve upon those measures, the DON CIP Program's focus remains firmly on the warfighters' mission assurance.

For more information, go to the DON CIAO Web site at <http://www.doncio.navy.mil/>, the select the Products tab. CHIPS



# CAN YOU HEAR ME NOW?

## TRANSFORMATIONAL COMMUNICATIONS - THE SPACE SEGMENT

By the DON CIO Telecom/RF Spectrum/Wireless Team

The stated goal of the Transformational Satellite communications system is to provide improved, survivable, jam-resistant, worldwide, secure and general purpose communications ...

### DoD's Future Communication Architecture

In the Jan-Mar 2005 edition of *CHIPS*, multiple aspects of the Department of Defense (DoD) planned Transformational Communications Architecture (TCA) were explored. This follow-on article focuses on the TCA space segment, which is a composite of space-based assets of the National Aeronautics and Space Administration (NASA), DoD and the Intelligence Community (IC). These combined assets will interoperate and they will be supported by the other three TCA segments, which are primarily earth-bound: the terrestrial infrastructure segment, the terminal segment and the network and management segment.

### The TCA Space Segment

The space segment will extend the Global Information Grid (GIG) to users without fiber connections, providing improved connectivity and data transfer capability resulting in a revolutionary change in satellite communications for the warfighter. Figure 1 shows the types of services that currently compete for satellite bandwidth. These services will benefit from the planned improvements in satellite communications.

Role of Satellites in Recent Conflicts
Battle Management
Communication
Surveillance
Space-based radar
Photo-reconnaissance
Weather Monitoring and forecasting

Figure 1.

Transformational Communications System-MILSATCOM (TCM) will enable high data rate connections to space and airborne intelligence, surveillance and reconnaissance platforms. Using the data from these platforms, future networks of advanced battlefield sensors will be able to monitor, discriminate and report

minor changes, such as types of vehicular/pedestrian traffic, environment, etc. The projected growth in TCM capabilities would allow broader distribution of this type of sensor data.

The satellite components of the TCA will incorporate radio frequency (RF) and laser communication links to meet joint agency requirements for high data rate protected communications. Included in the space-based programs are:

Wideband Gapfiller System (WGS), a follow-on generation for wideband communication

Mobile User Objective System (MUOS), a next generation narrowband solution providing critical connectivity for more than 80,000 UHF devices, such as small antenna radios (as small as 1 foot) found in tactical ground vehicles, hand-held man packs, and even airborne systems

Advanced Extremely High Frequency (AEHF) satellites, for updated protected communication to support strategic assets with upgraded EHF protected/survivable features

### Transformational Satellite (TSAT)

As the terrestrial aspects of communication in the TCA evolve, so will DoD satellite resources. The stated goal of the Transformational Satellite communications system is to provide improved, survivable, jam-resistant, worldwide, secure and general purpose communications as part of an independent but interoperable set of space-based systems that will support NASA, DoD and the IC. TSAT will ultimately replace the DoD's current satellite system and supplement AEHF satellites.

The TSAT proposes a radio frequency (RF), i.e., traditional radio-based, crosslink to complete the AEHF group of satellites or constellation. The constellation is called the Advanced Polar System (APS), which supports strategic and national users in the polar region. The APS is designed to withstand nuclear attacks and support the strategic mission with uninterrupted service. These satellites introduce the use of jam-resistant laser crosslinks for connection into the TSAT.

The TSAT includes satellite resources and TCM satellite operation centers, TCM Mission Operations Systems and ground gateways. This creates an Internet-like transport architecture between space, air, ground and sea nodes. This design will culminate in a flexible Enterprise warfighting environment. The full GIG implementation, supported by TSAT, means every asset in the

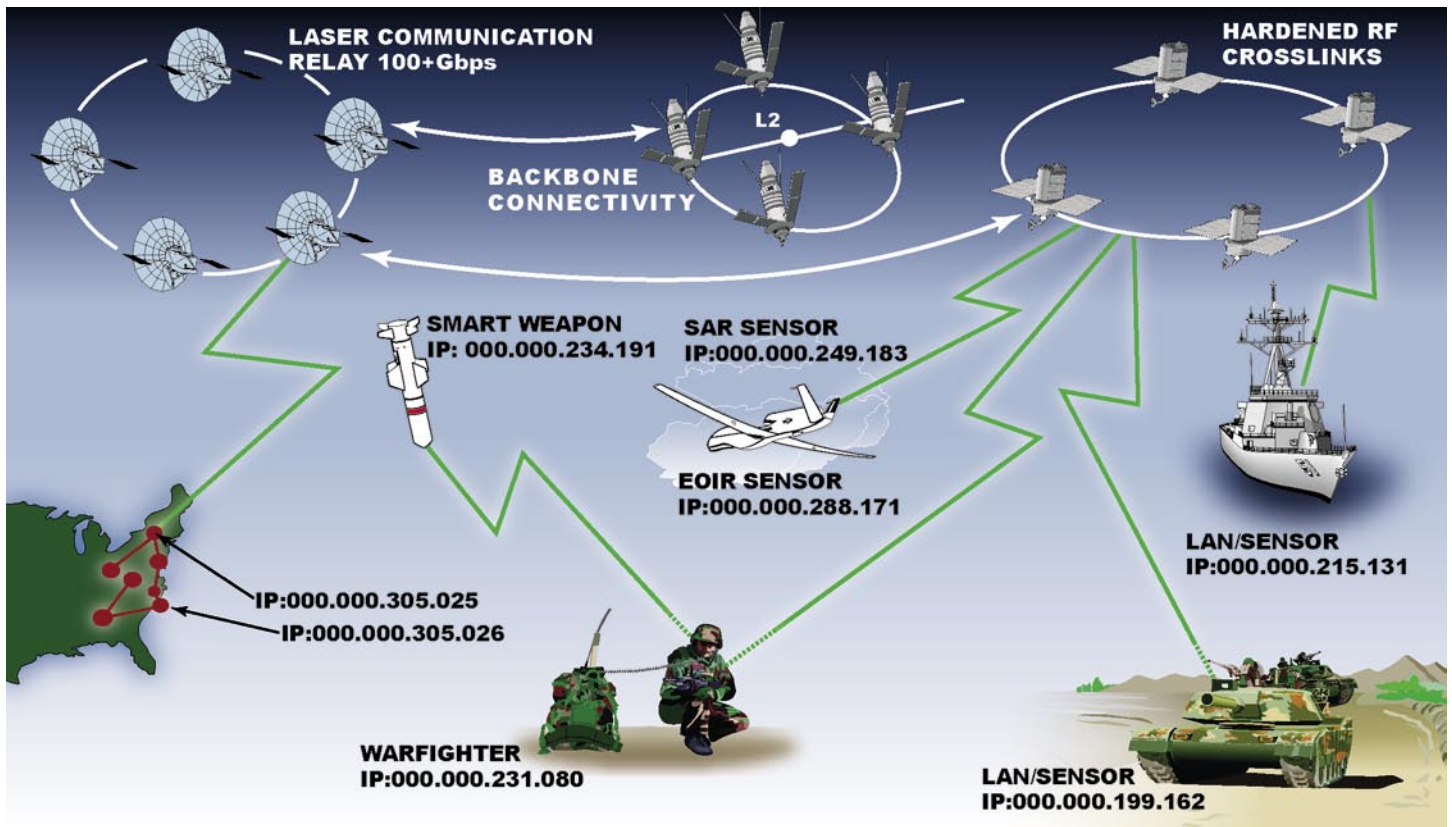


Figure 2. IP-Based and protected by IA initiatives, each platform and each sensor is accessible and integrated with warfighters.

battlespace would be addressable and capable of generating, processing or routing information. Current TCA vision calls for the U.S. Air Force, as program sponsor, to launch a constellation of five transformational satellites or TSAT spacecraft about 2011. This constellation will form the DoD ring. In this scenario, the Department of the Navy will design a service-specific architecture to leverage the spacecraft capabilities.

The TSAT assets of the DoD ring support RF data rates up to 45 Mbps and laser communication user data rates into the 10-100s Gbps range. A design objective of the DoD ring is to provide multiple, simultaneous user access to laser-based communications. This feature creates a virtually jam-proof environment. The TSAT also offers an enormous increase in total bandwidth capacity with loaded capacity of about 2 Gbps of RF per vehicle compared with 250 Mbps for AEHF.

### DoD Initiatives Being Satisfied through TCA

Several Secretary of Defense initiatives are being satisfied through the TCA and its unique implementation of the space segment including: (1) providing protection from attack for our information networks; (2) utilizing information technology to link different organizations so they can fight jointly or provide coordinated homeland security; (3) maintaining protection and unhindered access for our space capabilities.

Figure 2 depicts future satellite networks that provide hardened RF crosslinks. While it is easy to define requirements and presume success, much of the technology needed to succeed will need to be developed by a public-private partnership engaging government and industry. In fact, laser communication technol-

ogy is dependent upon a level of industry investment to produce multi-access laser communication receivers, develop and integrate laser communication terminals to airframes, and further develop communication-on-the-move vehicular antenna technology.

International efforts to identify services for commercial wireless implementation will support some of the same technologies. The Navy Marine Corps Intranet (NMCI) will act as the Department of the Navy's terrestrial component to support, distribute, analyze and respond to the information collected and transmitted by the satellite components of the TCA.

### TSAT Enables our Shifting Naval Strategy

Naval strategy is shifting from threat-based, platform-centric to an effects-based, network-centric force. Our warfighters' information environment has seen exponential growth. The need to execute bold strategies, versus reactionary and temporary responses to situational demands, is critical to creating capable resources for future requirements.

At an interoperability level, the concept of Naval Power 21 poises the Department to embrace the GIG environment, ready to exploit joint capabilities and partner in the distribution of information. The vision for the Transformational Communication Architecture would exploit new technologies to support critical communications capabilities for the warfighter and the commander.

For more information, contact the DON CIO Telecom/RF Spectrum/Wireless Team at [DONSPECTRUMTEAM@navy.mil](mailto:DONSPECTRUMTEAM@navy.mil). CHIPS



In the *CHIPS* Jan-Mar 2005 edition, we discussed the recent advances and evolution of the small computer system interface (SCSI) standard. You can view this article at [http://www.chips.navy.mil/archives/05\\_jan/web\\_pages/scuzzy.htm](http://www.chips.navy.mil/archives/05_jan/web_pages/scuzzy.htm). In Part II, we will look at some of the overarching issues surrounding when and why SCSI may or may not be the preferred solution for you, and we will compare SCSI to some of the other competing standards.

Raw specifications are fine, but to evaluate an entire system you must look at all of its components. So what are some of the criteria that might be a factor in this process? Typically, we would be concerned with the following: (1) Reliability/Maintainability - for example, mean time between failures; (2) Fault Tolerance - what is the impact of a failure on the system as a whole; (3) Speed/Data Throughput - how fast can data pass; (4) Storage capability - disk or array size; (5) Cost - usually expressed as cost per gigabyte; and (6) Scalability/Flexibility - how hard is it to change the configuration or increase storage.

### Comparing Drives

SCSI's performance can be compared with Serial Advanced Technology Attachment (SATA) and Integrated Development Environment (IDE). When evaluating drives alone, the information in Figure 1 summarizes the current state of technology. However, manufacturers are working on larger and faster drives for both SCSI and SATA.

As you can see, SCSI clearly outperforms the other two types of drives, but it should be noted that when implemented in a RAID (Redundant Array of Independent Disks) environment, differences in individual drive parameters become much less pronounced as even lower performance drives can saturate the data bus and other system components. This is because in a multi-drive array each individual drive has to do less work since the workload is shared across all the drives in the array.

### Comparing Bus Types

In addition to evaluating the drives, there are factors regarding the data bus to consider. The SCSI bus is supported via cabling that can handle up to 15 devices per channel in series. It can support both internal (in the case with the central processing unit)

and external devices. While cabling that supports SCSI U160 and U320 standards are more expensive than other storage architectures they can be easier to work with because multiple devices can be connected to a single cable run and each cable run can be several meters in length.

Each channel on a SCSI bus supports up to the maximum data transfer rate supported by the specification (i.e., U160 or U320), but since they are connected in series, bandwidth is shared by all devices on the channel. Currently, the IDE and SATA data buses require a separate cable between each device and the controller. So while the cables are relatively inexpensive you will need significantly more of them, and if they are not properly installed they tend to clutter the inside of the enclosure and can restrict air flow required for cooling.

IDE cables are usually flat ribbon cables, although rounded versions are available and are limited to 36 inches in length. SATA cables are smaller and easier to manage and can be up to 40 inches in length. SATA also implements multi-lane cabling that combines four device connectors into a single cable. In addition to the newly available 300 MBps devices, SATA has a 600 MBps specification in the works. New features will include native command queuing, an external interface (to allow the use of external enclosures), a port multiplier to further decrease cable clutter and hot-swap capability — features that up until now were only available in a SCSI environment.

### Other Factors Affecting Overall Performance

At this point we have examined individual drive issues as well as

Drive Type	SCSI	IDE	SATA
RPM	10,000	7,200	7,200
Avg Seek Time	<4.7ms	<9.5ms	<8.5ms
Data Transfer Rate	320MBps	133MBps	300MBps
Size 1 (GB) <sup>1</sup>	36	120	120
Avg Cost	\$197	\$89	\$95
Avg Cost p/GB	\$5.5	\$0.742	\$0.80
Size 2 (GB) <sup>2</sup>	146	200	200
Avg Cost	\$700	\$89	\$131
Avg Cost p/GB	\$4.794521	\$0.445	\$0.655
Size 3 (GB) <sup>3</sup>	300	500	500
Avg Cost	\$1,590	\$468	\$489
Avg Cost p/GB	\$5.3	\$0.94	\$0.98

<sup>1</sup>Average size of typical entry level drive

<sup>2</sup>Average size of mid-level drive

<sup>3</sup>Largest size currently available

Figure 1.



those associated with each type of data bus. Now we will turn to some of the other factors that can influence overall system performance. This discussion will only address issues involving when the storage subsystem is installed as a direct component of a server versus as a Serial Attached SCSI (SAS) or Internet SCSI (iSCSI) implementation.

The disk controller acts as the interface point between the drives, data bus and system bus. If the controller is functioning only as a basic disk controller then it should perform at the same rate as the data bus. But if it is also performing as a RAID controller then the performance of the RAID function can have a significant impact on the overall storage system performance especially if it is an older or less capable device. But a RAID implementation with low performing hardware would probably still outperform one implemented via software only.

Another system component that can have a significant impact on performance is the system bus. Currently, the most popular bus is the Peripheral Component Interconnect (PCI) 2.0 bus, which replaced the Industry Standard Architecture (ISA) bus several years ago. However, a new bus called PCI-Express is available, which provides significant increases in bandwidth to pass data between the system components and installed interface cards.

PCI-Express will replace both the PCI 2.0 as well as the Accelerated Graphics Port (AGP) bus types on system motherboards. The final hardware and software components that can affect storage performance are: (1) Motherboard and CPU - especially if implementing software; (2) System memory - amount and speed; and (3) Network interface - if providing data or services to other servers or clients.

The last item to consider is the usage profile. This will determine the optimal mix of component types for the desired level of performance. If normal usage will include a small number of users accessing a small number of large files, such as video streaming, then a smaller number of high-capacity drives would be sufficient.

But if normal usage will include a large number of users accessing a large number of smaller files, such as general file services, then a larger number of smaller capacity drives would provide better performance. This is due to contention or competition for resources. Contention occurs when more than one request is pending for data on a single physical drive. The larger each individual drive is in an array, the greater the probability that there will be data requests pending. This and other issues including system storage are important to understand before finalizing a system design.

### Factors Affecting Total Cost per Gigabyte

In addition to the costs associated with the individual drives in a storage system, there are a number of other components that can significantly add to the average cost per gigabyte. These include:

- ✓ Disk Controllers – especially high-end RAID units.
- ✓ Redundant system components to provide higher availability – these could include disk controllers, power supplies and interface components.

✓ Cabling – drive-to-controller cabling as well as chassis-to-chassis cabling.

✓ Additional infrastructure – equipment racks and cases, additional room cooling and power and increased electricity usage.

✓ Backup facilities – most backup systems, especially tape-based systems, may require a significant amount of time to transfer data from the primary system onto the backup system. This could result in the need for a high-end complex backup system.

✓ Management overhead – the larger and more complex a storage system, the more time and labor will be required to design, implement and manage it.

### Alternative Approaches

In the last couple of years a new way of building storage has emerged: combining one type of drive with a different type of data bus. Normally, you will find IDE or SATA drives attached to a U160 or U320 SCSI bus. This provides most of the advantages of the SCSI bus with a relatively lower cost per gigabyte for IDE and SATA drives. There are also fewer tradeoffs in average seek time and reliability in this approach. These hybrid arrays can be purchased as turnkey products. The arrays incorporate a controller that performs the RAID function as well as the conversion function, and they just require connection to a (non-RAID) SCSI controller.

A hybrid array can also be built by combining devices that connect between the individual drives and the SCSI bus to make the IDE or SATA drive appear as a SCSI drive to an existing controller. Total cost per gigabyte for turnkey systems are about \$2 to \$3 and for self-built (including chassis, drives, controller and cables) about \$1 to \$2. This can be a substantial savings over a traditional array where all components are SCSI-based and can cost \$6 to \$9 per gigabyte.

### What does the Future Hold?

In the past 10 years, SCSI-based products have been evolving much more slowly than IDE and SATA-based products. SCSI-based products have, however, been showing an increased rate of improvement in the last two years. It will be interesting to see how SCSI technology evolves, but regardless of the approach used we can expect performance and capability to continue to increase and cost per gigabyte to continue to fall.

*Patrick Koehler is a member of the SPAWAR Systems Center Charleston, FORCEnet Engineering and Technology Support Branch. He has a bachelor's degree in computer information systems and holds certifications in A+, CCNA, CCNP, MCDBA 2000, MCP/MCSA/MCSE Windows 2003, MS Outlook/Powerpoint/Access/Word Expert 2002, Network+, Security+, Server+ and Inet+.*

*Lt. Cmdr. Stan Bush is the Military Faculty and Program Officer for the Information Technology Management curriculum at the Naval Postgraduate School. He holds a bachelor's degree in computer information systems and a master's degree in computer science. He holds certifications in MCP, CISSP and CISM and certificates in the DoD CIO & NSTISSI No. 4011 Programs. Web site: [http://research.nps.navy.mil/cgi-bin/vita.cgi?p=display\\_vita&id=1078774080](http://research.nps.navy.mil/cgi-bin/vita.cgi?p=display_vita&id=1078774080). CHIPS*

By Retired Air Force Major Dale J. Long



## The Lazy Person's Guide to Internet Hoaxes, Myths and Legends

You are traveling through another dimension — a dimension of bits and bytes and information. It is a journey into a wondrous land whose boundaries are that of imagination and there is a signpost up ahead. Your next stop: the Internet Zone. Within the vast, bright realm of cyberspace, however, lurk various tricksters and scam artists ranging from amusing to annoying or downright dangerous.

These miscreants have turned their not inconsiderable talents to creating stories that convince the unwary to spread the seeds of their imaginations around the world. Submitted for your consideration are some of the stories that have become Internet legends and urban myths. All of them are hoaxes, but they cling to their odd half-lives through a combination of cunning, persistence and their ability to draw new believers to their cause.

If an informed electorate is the foundation of democracy, then informed users should be the foundation of the Internet. In this issue, we will dissect a few of these hoaxes with a view to helping prevent their spread in the future. The more people who understand how chain spam really works, that there aren't really people in Nigeria who want you to launder money for them and that apparently friendly warnings usually start out as misanthropic attempts to stir up a cloud of e-mail activity, the better off we will be.

### Forward Me!

What prompted this particular topic was an e-mail mass mailed by someone at one of our field offices. It went something like the message in Figure 1. Some of you may recognize this one. Zippy received it from a well-meaning person and forwarded it to another few hundred people, some of whom managed to forward it to others in the 10 minutes it took me to send a notice telling people to ignore the message because it was a hoax.

How do we know it is a hoax? On the surface, there is a grain of truth in the story. Yes, there is a National Do Not Call Registry where people can register their phone number to avoid telemarketing calls. Yes, there is an industry group trying to establish a 411 directory of cell phone numbers. Add in that many people do not trust telemarketers or telecommunications companies to protect

Urgent! Urgent! All Cell Phone Users!

From: Zippy  
Sent: December 01, 2004 10:08  
To: All of my friends  
Subject: FW: IMPORTANT!

Starting Jan. 1, 2005, all cell phone numbers will be made public to telemarketing firms. So this means as of Jan. 1, your cell phone may start ringing off the hook with telemarketers, but unlike your home phone, most of you pay for your incoming calls. These telemarketers will eat up your free minutes and end up costing you money in the long run.

According to the National Do Not Call List, you have until Dec. 15, 2004, to get on the national "Do not call list" for cell phones. Registering only takes a minute. Make sure you register now!

Figure 1.

their privacy and you have rich fertilizer to sprout a bumper crop of panicky e-mails.

However, it is just fertilizer because the main assertions are simply not true. First, there is no deadline for registering on the Do Not Call Registry. Second, current Federal Communications Commission (FCC) regulations prohibit telemarketers from calling cell phones. Finally, the industry-sponsored wireless 411 directory, as currently proposed, will only include the cell phone numbers of people who voluntarily add their numbers to the listing.

The industry group is also fighting pending legislation that would regulate cell phone directories and make it virtually impossible to create or distribute any list without voluntary participation by cell phone users. Apparently, there is enough valid information in the message to convince many otherwise rational people that this is a real problem, and they should forward the warning on to all their friends and relations as a public service. Unfortunately, all that does is encourage hackers who rely on social engineering to create even more entertaining e-mail fiction.

*Other popular e-mail subjects over the past few years have been:*

- ✓ You can get free cash (or beer) by forwarding an e-mail message
- ✓ The U.S. Postal Service is going to start collecting a 5-cent fee for every e-mail message sent
- ✓ Business travelers are waking up in their hotel rooms in ice-filled bathtubs minus a kidney
- ✓ Gas pump handles trapped with hypodermic needles are ready to prick you when you grab the handle (similar to ATM deposit envelopes laced with cyanide)
- ✓ Nike will give you new shoes if you turn in your old ones
- ✓ Money will be donated to charity (injured child, abandoned puppies, political campaign, etc.) for forwarding an e-mail
- ✓ Pending legislation will require all gun owners to list their guns on their income tax returns
- ✓ Your free e-mail service will cancel your account if you do not forward this e-mail

Frankly, I do not care about the subject of a chain-forwarded e-mail; I delete virtually all of them. I will admit to passing on the one about the soldier in the shack on Christmas Eve, and every once in a while I see something particularly humorous that I just have to share with a few friends. Even some that appear to be *good spam* are self-serving attempts to generate e-mail traffic. And given the proven ability of e-mail to carry malicious viruses, I am not inclined to be forever known among my friends as "Typhoid Dale" because I sent a virus to everyone in my address book.

## Out of Africa

Another persistent e-mail scam that I still see in my inbox, despite a pretty good Bayesian filter, is known as the Nigerian Scam. These types of scams are known as advance fee fraud scams or 4-1-9 fraud. 419 is the number of the section of the Nigerian penal code that addresses fraud schemes.

This scam starts when you receive an e-mail plea from an allegedly wealthy foreigner, who needs your help to move millions of dollars from his homeland to the United States and will reward you with a hefty percentage of the money. Or you have won a foreign lottery you did not know you entered. Or some wealthy repentant sinner wants to leave your church millions of dollars in his will. All you have to do is send several thousand dollars in processing fees to release the money so they can send it to you.

Now you would think that upon reading this particular pitch the frontal lobes of the average cerebellum would be screaming, "WARNING, WARNING! Danger Will Robinson! SCAM, SCAM!" It is so obviously a scam that three blind hedgehogs living inside a padlocked canvas mail sack should be able to see it coming.

However, a 2002 U.S. Secret Service report (<http://www.secretservice.gov/alert419.shtml>) estimates that advance fee schemes still con people out of hundreds of millions of dollars every year. Advance fee scams are not new. They have been around since the Spanish Prisoner letter scam in the 1920s. But for some reason, people really want to believe in free money and, once hooked, will not let go of the illusion until they run out of money. The stories of people duped by these schemes are legion. You can find clues that you may be dealing with a hoax at the Department of Energy's Computer Incident Advisory Capability (CIAC) on its HoaxBusters site at <http://HoaxBusters.ciac.org/>.

## Phishing Phollies

Speaking of fish, no discussion of online scamming would be complete without a description of *phishing*. This occurs when scammers "fish" for information by posing as banks, credit card companies or online businesses and try to obtain account details and pin numbers.

Most phishing today is done via e-mail. You get an official-looking e-mail from companies like Visa, Amazon.com, eBay, Smith Barney, etc., that asks you to click on an embedded link to *their* Web site and confirm your account data. While these links may appear genuine, the underlying URL (Uniform Resource Locator) in the page code takes you to the scammer's site, which is designed to look exactly like the genuine article. Once you enter your account information into the login form, you get a reassuring message that everything

is just fine with your account and the scammer gets your account details.

As with advance fee scams, phishing is not new, it is based on old telephone scams where someone called up claiming to be from the bank or credit card company and asked people to *verify* their card number, expiration date, billing address, Social Security Number, etc.

Phishing has apparently been very profitable for phishers. In the United States alone, banks reportedly paid out more than \$1.2 billion last year due to phishing scams. There have been reports of phishing operations that targeted a favorite phisher target: Microsoft's Internet Explorer browser. Security experts identified vulnerabilities in IE Version 6 (including those on computers updated with Windows Service Pack 2) that allowed phishers to create realistic looking Web sites that fake Secure Socket Layer signature padlock certificates and hijack cookies from other Web sites, including those with login and account information.

While it is likely that these holes will have been patched by the time you read this, browser and e-mail vulnerabilities represent the main chinks in our armor that phishers and other malicious software authors have targeted recently.

The next wave of Internet-related scams, however, may move from phishing to *pharming*. While phishing is a social attack where the scammer throws out bait and hopes someone will nibble, pharming is more like sowing seeds and waiting for them to sprout and bear fruit. Pharming involves spreading a worm or virus to host computers that automatically and invisibly redirects your browser when you try to reach a particular URL.

As users become harder to dupe with phishing schemes, we may see a shift from phishing to pharming. While all alleged reports of this form of exploitation have so far involved redirects to advertising sites, it is theoretically possible that pharming worms could become sophisticated enough to allow scammers to create a look-alike site intended to steal account information and send out instructions to their worms to redirect you from your online banking or shopping site to theirs.

Apparently, it isn't happening yet, but it may only be a matter of time. It was not so long ago that we thought you could not get a computer virus from simply opening e-mail, so I have every expectation that someone will figure out how to make pharming work, too.

Another theoretical variation on pharming is based on Domain Name System poisoning. This occurs when the scammer confuses your DNS server into believing that the site you want is an Internet Protocol (IP) address that belongs to the scammer, not the site's actual numeric address. Most Internet services rely on DNS, which is a distributed Internet directory service that has two primary functions: (1) translate between domain names and IP addresses and (2) control e-mail delivery.

In particular, Web browsers depend on DNS to locate Web sites. While your browser shows you the text-based URL, the site that

actually resolves is based on the numeric IP address, whether or not it is really the correct address. However, DNS servers do not always authenticate the source of the numeric IP address. In many cases, there is no way for a DNS server to be sure that the address actually came from the real site.

Plugging identification and authorization exploits like DNS poisoning can be a never-ending arms race with the DNS server constantly on the defensive. As with any security scheme, proper configuration of your system is crucial. If all DNS servers were configured using something similar to Secure Shell architecture, DNS poisoning or any similar scam that depends on trust-based vulnerabilities would be less of an issue. For more information, see the Internet Engineering Task Force Web site at <http://www.ietf.org/html.charters/secsh-charter.html>.

## **Mom Was Right**

Of course, no amount of armor will protect anyone who insists on repeatedly swimming in shark-infested waters. There are some steps you can take to protect you from online scams, and they sound a lot like advice mom gave us when we were children:

**1. Don't touch that — you don't know where it's been.** Or in the case of embedded links in unsolicited e-mails, where it is going. Never click on an embedded link in spam e-mail. At best, it tells the spammer that your address is "live." At worst, it loads some type of *malware* (malicious software) on your PC that burrows in and does ugly things. If you get a message saying you need to go to your online bank, eBay account or credit card company, type the URL in yourself.

**2. Don't mess around with things you don't know anything about.** This one is good advice for any e-mail attachment, particularly since clever, inventive people have found ways to embed viral code in everything from word processing documents to graphics files.

**3. Lock your doors.** In this case, turn off or restrict anything that could be used to allow unauthorized code into your system. That includes ActiveX controls, the Windows Scripting Host and HTML rendering in e-mail.

If you are really concerned about Web vulnerabilities, you may wish to replace MS Internet Explorer with another browser. In Zippy's case, he is only safe because his wife restricts him to an old Macintosh IIsi running Mac OS version 6.7 and an ancient version of Netscape. Many people would consider that security overkill, but you were not there when Zippy tried to buy into a fake scam for Millennium Bug Insurance a few years ago (see [http://www.chips.navy.mil/archives/99\\_jul/dale.htm](http://www.chips.navy.mil/archives/99_jul/dale.htm) for the details). His wife has not let him play on the Web by himself since.

**4. Don't talk to strangers.** Particularly strangers offering you free candy, money, beer or lunch online. This also applies to chat rooms, as malicious software can apparently be spread via chat software.

I got a first-hand look at this a couple of years ago when my martial arts instructor, a man with eight black belts, who owns more hand-held weapons than he has ball-point pens, got cyber-mugged in a chat room by someone who hacked his computer remotely through the chat software and took control of the PC.

The only sure way to regain control after an attack like that is to physically disconnect the power, unplug the Internet connection, exorcise the offending malware by backing up the data files, reformatting the hard drive, and reloading the operating system and applications from scratch. Chat rooms are the cyberspace equivalent of hanging out in bars. If you want to be safe, go with people you know, and do not play games for money with strangers.

**5. Wear your raincoat.** A properly configured firewall or Web proxy (or both) can save you a lot of grief. In particular, you should have something set up to prevent unwanted intrusion and restrict what your computer might try to send out without your knowledge. Some phishing scammers do not care if you voluntarily provide them with your ID and password as long as they can download, install and activate a keystroke logger on your computer. While it may be useful to set your computer to automatically check for and download updates for your operating system or applications, you should control any activity that transmits data from your computer.

## **Grains of Sand and Salt**

I would like to reiterate that there is a kernel of truth at the core of every successful scam. Without some veneer of credibility, people would be less likely to fall for them. The only way to combat them is with a healthy distrust of anything that shows up uninvited, regardless of how lucrative, alluring or even patriotic it seems.

If you are interested in e-mail hoaxes, scams or urban legends, there are Internet sites that are useful to those of us trying to keep Zippy from increasing the amount of junk e-mail traffic clogging the Internet.

Please e-mail this article to all of your friends. If everyone passes this on to 10 other people, eventually the entire world will read it, and we could eliminate forwarded e-mail spam forever! Then again, maybe you should just tell your friends to read the article in *CHIPS* or on the *CHIPS* Web site!

## **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.*

*Editor's Note: The Department of the Navy Chief Information Officer (DON CIO) offers an Information Literacy Toolkit on compact disc for use by government, industry and academia partners in support of government. The disc provides information on how users can become skilled in recognizing valid information on the Internet and in e-mail. There is also information about hoaxes online in the Exploring Online/Evaluating Information section. Go to <http://www.doncio.navy.mil/iltoolkit/> for assistance. Navy NMCI users who receive unauthorized e-mail should contact the NMCI Help Desk at 1-866-843-6624 for assistance. Other government users should follow your agency's guidance on handling chain and scam e-mail. 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.don-imit.navy.mil/esi>.

### 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

##### Invoke Software (CESM-E)

**Invoke Software** - A collaboration integration platform that provides global awareness and secure instant messaging, integration and interoperability between disparate collaboration applications in support of the DoD's Enterprise Collaboration Initiatives.

**Contractor:** *Structure Wise* (DABL01-03-A-1007)

**Ordering Expires:** 4 Sep 05

**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. Inventory exists for Navy customers, contact Navy Project Managers below 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 May 05

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

www.it-umbrella.navy.mil

**Special Note to Navy Users:** The Department of the Navy (DON) established a Navy Shore-Based Oracle Database Enterprise License Agreement that was implemented Oct. 1, 2004 effective through Sept. 30, 2013, to provide Navy shore-based organizations the right to use the Oracle databases. This agreement is managed by the Space and Naval Warfare Systems Center (SPAWARSYSCEN) San Diego DON Information Technology (IT) Umbrella Program Office. This agreement consolidated existing and new Oracle Database software licenses and maintenance under a single contractual vehicle and procured the rights to use for authorized users. All DON General Fund and Working Capital activities are covered, with an exception of Marine Corps activities. Marine Corps activities are currently covered by a separate Marine Corps-wide Oracle database agreement.

Authorized users at covered activities include all Navy active duty, reserve and civilian shore-based billets not assigned to a ship. On-site and off-site contractors who access Navy systems for the purpose of supporting Navy shore-based operations are also covered. This Navy Shore-Based Oracle Database Enterprise License Agreement provides significant benefits including substantial cost avoidance for the Department. It facilitates the goal of net-centric operations by allowing all shore personnel to access Oracle databases, permitting the sharing of authoritative data across the shore-based enterprise. The agreement has a priced option that, if exercised, will enable the Department to extend these benefits to the afloat Navy. Activities covered by this license agreement shall not enter into separate Oracle database agreements or procure additional Oracle database licenses outside this central agreement whenever Oracle is selected as the database. This prohibition includes software maintenance that is acquired:

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

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

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

## Sybase (DEAL-S)

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

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

**Ordering Expires:** 15 Jan 08

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

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

## Enterprise Architecture Tools

### Rational Software (AVMS-R)

**Rational Software** - Provides IBM Rational software licenses and maintenance support for suites and point products 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:** 25 Aug 05

**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-EMS)

**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 2-5 percent off GSA Schedule pricing plus spot discounts for volume purchases.

**Contractor:** *Citrix Systems, Inc.* (W91QUZ-04-A-0001); (301) 280-0809

**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 10-18 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>

## 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](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); (301) 581-2212

**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 DoD activities. The BPAs offer GSA discounts from 10 to 20 percent. Firm fixed prices and performance-based contracting approaches are provided to facilitate more efficient buying of systems integration services. Five BPAs were competitively established against the GSA Schedule. Task orders must be competed among the five BPA holders in accordance with DFARS 208.404-70 and Section C.1.1 of the BPA. Acquisition strategies at the task order level should consider that Section 803 of the National Defense Authorization Act for 2002 requirements were satisfied by the BPA competition.

### Contractors:

*Accenture LLP* (N00104-04-A-ZF12); (703) 947-2059

*BearingPoint* (N00104-04-A-ZF15); (703) 747-5442

*Computer Sciences Corp.* (N00104-04-A-ZF16); (856) 252-5583

*Deloitte Consulting LLP* (N00104-04-A-ZF17); (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](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.don-imit.navy.mil/esi/>

**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](http://www.cert.mil/antivirus/av_info.htm)

SIPRNET site: [http://www.cert.smil.mil/antivirus/av\\_info.htm](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.don-imit.navy.mil/esi/>

**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](http://www.cert.mil/antivirus/av_info.htm)

SIPRNET site: [http://www.cert.smil.mil/antivirus/av\\_info.htm](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.don-imit.navy.mil/esi/>

**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](http://www.cert.mil/antivirus/av_info.htm)

SIPRNET site: [http://www.cert.smil.mil/antivirus/av\\_info.htm](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 accor-

dance 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

**Hewlett-Packard** (N00104-02-A-ZE80); (800) 535-2563 pin 6246

**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

**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** (N00104-02-A-ZE86); Small Business; (304) 725-6110

**Software Spectrum, Inc.** (N00104-02-A-ZE82); (800) 862-8758 or (509) 742-2308

**Ordering Expires:** 26 Jun 05

**Web Link:** <http://www.it-umbrella.navy.mil/contract/enterprise/microsoft/ms-ela.shtml>



## Netscape Products

**Netscape Products** - Netscape Communicator Client and a number of the Netscape Server products for use across DoD. Available for download at no cost. Customers must choose between the commercial version and the Defense Information Infrastructure Common Operating Environment (DII COE) Segmented Versions.

Licensed software products available from the Defense Information Systems Agency (DISA) are commercial versions of the software, not the segmented versions that are compliant with the DII COE standards. The segmented versions of the software are required for development and operation of applications associated with the DII COE, 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 DII COE, GCCS or GCSS, you must go to one of the Web sites listed below to obtain the DII COE 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.

**DII COE or GCCS users:** Common Operating Environment Home Page

<http://disa.dtic.mil/coe>

**GCSS users:** Global Combat Support System

<http://www.disa.mil/main/prodsol/gcss.html>

**Contractor:** *Netscape*

**Ordering Expires:** Mar 05 – 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 Corporation, for the purchase of WinZip 9.0, a compression utility for Windows. Minimum quantity order via delivery order and via Government Purchase Card to Eyak Technology, LLC is 1,250 WinZip licenses. All customers are entitled to free upgrades and maintenance for a period of two years from original purchase. Discount is 98.4 percent off retail. Price per license is 45 cents.

**Contractor:** *Eyak Technology, LLC* (W91QUZ-04-D-0010)

**Authorized Users:** This has been designated as a DoD ESI and GSA Smart-BUY Contract and is open for ordering by all United States federal agencies, DoD components and authorized contractors.

**Ordering Expires:** 27 Sep 09

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

## Operating Systems

### Novell

**Novell Products** - Provides master license agreement for all Novell products, including NetWare, GroupWise and ZenWorks.

**Contractor:** *ASAP Software* (N00039-98-A-9002); Small business; (800) 883-7413

**Ordering Expires:** 31 Mar 07

**Web Link:** <http://www.it-umbrella.navy.mil/contract/enterprise/novell/novell.shtml>

## Sun (SSTEWS)

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

**Contractor:** *Dynamic Systems* (DCA200-02-A-5011)

**Ordering Expires:** Dependent on GSA Schedule until 2011

**Web Link:** <http://www.ditco.disa.mil/hq/contracts/sstewchar.asp>

## Research and Advisory BPAs Listed Below

Research and Advisory Services BPAs provide unlimited access to telephone inquiry support, access to research via Web sites and analyst support for the number of users registered. In addition, the services provide independent advice on tactical and strategic IT decisions. Advisory services provide expert advice on a broad range of technical topics and specifically focus on industry and market trends. BPA listed below.

**Gartner Group** (N00104-03-A-ZE77); (703) 226-4815; Awarded Nov 02; one-year base period with three one-year options.

**Ordering Expires:** Gartner Group: 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 (FMS).

**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:** [como@mailbuoy.norfolk.navy.mil](mailto: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 05, with two one-year options

**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 05, with two one-year options

**TDS** (Small Business) (N00039-98-A-3008); (619) 224-1100;

Awarded 15 Jul 98; Ordering expires 14 Jul 05, with two one-year options

**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, Segovia

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. But avoid using a myriad of acronyms throughout your article since they can be confusing to the reader.

Articles may contain illustrations. Photos and illustrations are acceptable in .jpeg, .gif, .tif or .eps formats. 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.

*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. (Suggest applying the word count feature in Microsoft Word to check your article length.)

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

The following information is provided to help you understand our production process. We have subject matter experts on staff, who review each article for technical accuracy. 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 equating to a major rewrite, 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.

CHIPS



***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](http://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**