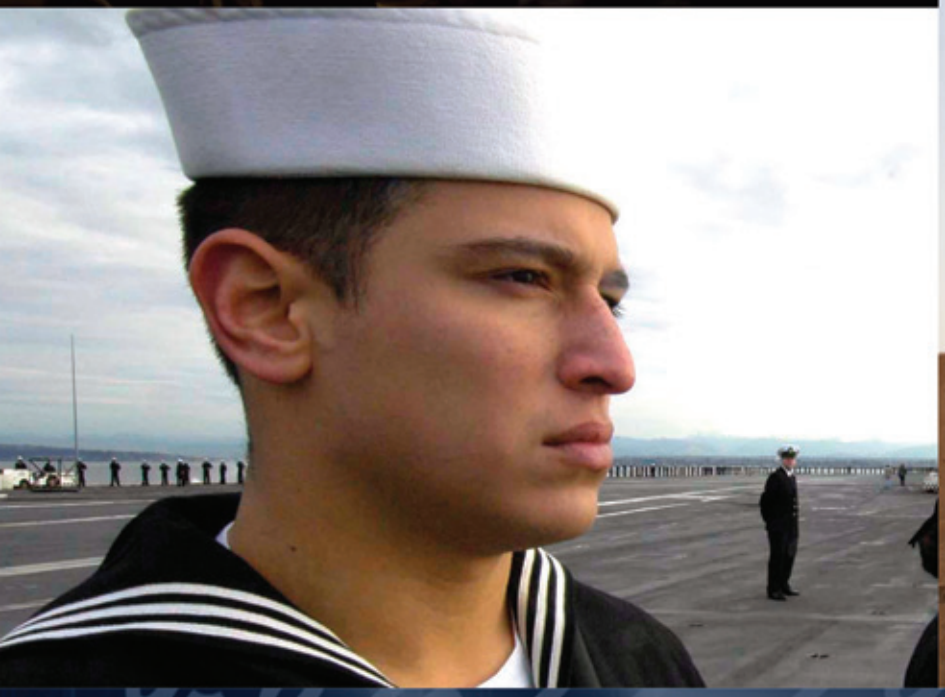
Sharing Information - Technology - Experience

CHIPS

October - December 2010



CYBER/IT WORKFORCE

Information Dominance Corps Update

Policies, certification programs and Scholarships for Cyber/IT professional development and career planning

CHIPS

October – December 2010 | Volume XXVIII Issue IV

Department of the Navy
Chief Information Officer
Ms. Barbara Hoffman (Acting)

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

Space & Naval Warfare Systems Center Atlantic
Commanding Officer Captain Bruce Urbon

Senior Editor
Sharon Anderson

Assistant Editor
Nancy Reasor

Layout and Design
Sharon Anderson

Web Support
Tony Virata – DON IT Umbrella Program

Columnists
Sharon Anderson, Barbara Hoffman
Mike Hernon, Christy Crimmins
Tom Kidd, Mark Rossow, Michelle Schmith

Contributors
Lynda Pierce, DON CIO Communications
Holly Quick, SPAWARSYSCEN Atlantic

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

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

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

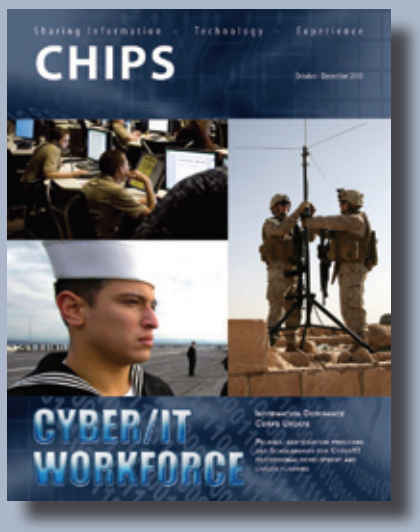
Requests for distribution changes or for other assistance should be directed to Editor, CHIPS, SSC Atlantic, 9456 Fourth Ave., Norfolk, VA 23511-2130, or call (757) 443-1775; DSN 646. E-mail: chips@navy.mil; Web: www.chips.navy.mil.

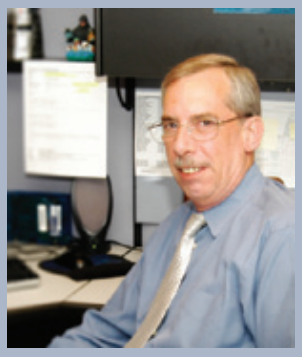
Disclaimer: The views and opinions contained in CHIPS are not necessarily the official views of the Department of Defense or the Department of the Navy. These views do not constitute endorsement or approval by the DON CIO, DON IT Umbrella Program or SPAWAR Systems Center Atlantic. The facts as presented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

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

Cover

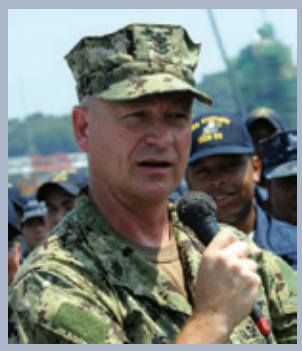
This issue of CHIPS focuses on the Cyber/IT Workforce and Information Dominance Corps development and promotes a Department of the Navy culture of lifelong learning through continuous training and educational programs and courses.





6 DON CIO Director of the Cyber/IT Workforce Chris Kelsall discusses the Cyber/IT Workforce Strategic Plan for Fiscal Years 2010-2013. Kelsall serves as an expert on workforce policy, planning, systems, credentialing and development for the workforce. Kelsall also represents the DON in DoD and federal efforts surrounding cybersecurity workforce development, competency development and in reporting to Congress.

10 The DCNO for Information Dominance, Director of Naval Intelligence and workforce leader for the Information Dominance Corps Vice Adm. Jack Dorsett discusses rapid progress in developing Personnel Qualification Standards, training and career planning for the IDC officer and enlisted communities.



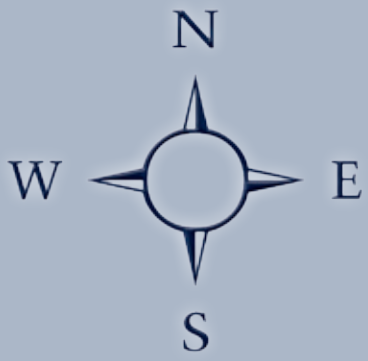
14 YOKOSUKA, Japan (Aug. 31, 2010) Master Chief Petty Officer of the Navy (MCPON) Rick West talks with Sailors aboard the guided-missile destroyer USS Stethem (DDG 63) during his visit to Fleet Activities Yokosuka. MCPON (SS/SW) Rick West talked to CHIPS about enlisted training and education for the Information Dominance Corps workforce. U.S. Navy photo by Mass Communication Specialist 1st Class Jennifer A. Villalovos.

16 NORFOLK (June 30, 2010) Rear Adm. Michelle J. Howard, commander of Expeditionary Strike Group (ESG) 2 gives a tour of the aircraft carrier USS George H.W. Bush's (CVN 77) hangar bay to Deputy Chief of Mission Minh Tien Nguyen of Vietnam during a visit to the ship marking the 15th anniversary of the reestablishment of diplomatic relations between the United States and Vietnam. Just days before Howard's assignment to the Joint Staff, Howard talked to CHIPS assistant editor Nancy Reasor. U.S. Navy photo by Mass Communication Specialist Seaman Leonard Adams.

Navigation

Featured Interviews with

In Every Issue



From the DON CIO

Around the Fleet

From the Department of Defense

Editor's Notebook

In this issue, we are emphasizing the importance the departments of the Navy and Defense place on continuous learning and education, professional and personal development, and career management with focus especially on the Cyber/IT Workforce and Information Dominance Corps (IDC).

Taking charge of your professional development is perhaps more vital than ever before. Consider the maelstrom of cybersecurity threats against defense networks and the increasingly complex systems that the DON and DoD build that are critical to national security.

There is exciting news for the Cyber/IT Workforce and IDC because the DON provides opportunities for professional certifications, courses and career paths for advancement. Newly released guidance from the DON Chief Information Officer, the DON Cyber/IT Workforce Strategic Plan, and DON and DoD programs and scholarships for military and civilian personnel, provide impressive learning opportunities. Best of all, with easy online access and smartphone accessibility to many courses, it is more convenient and beneficial than ever to seek self-improvement from academic institutions, technical schools and DON and DoD-sponsored programs and courses. Further, many naval commands and defense agencies offer guidance and assistance with career development and training plans.

Whether you are in the beginning of your career, the end, or somewhere in the middle, identify your strengths and weaknesses, define and execute a personal development plan, develop your talents — and maybe fulfill a lifelong dream.

And don't underestimate the value of joining professional associations, communities of interest and engaging with colleagues — or time invested in professional reading. Be a mentor and — or get one! Develop a mentoring culture in your command. It has been proven time and again that successful, confident leaders often had mentors along the way who were instrumental in their rapid career progression.

Cyber warriors — the DoD and the DON are urging you to investigate and pursue training and educational opportunities and to institute a habit of lifelong learning.

Welcome new subscribers!

Sharon Anderson

Become a lifelong learner!

VIRGINIA BEACH, Va. (Aug. 4, 2010) Sailors assigned to Navy Cyber Defense Operations Command (NCDOC) monitor, analyze, detect and respond to unauthorized activity within U.S. Navy information systems and computer networks. NCDOC is responsible for around the clock protection of the Navy's computer networks, with more than 700,000 users worldwide. U.S. Navy photo by Mass Communication Specialist 2nd Class Joshua J. Wahl.

Marine Corps Base Hawaii (Sept. 5, 2005) (Clockwise from left) Sgt. Jeremy D. Sadler; Sgt. Alexander Papiernik; Cpl. Andrew P. Parsons and Lance Cpl. Michael D. Hargis are tactical data networking specialists with 2nd Battalion, 3rd Marine Regiment. The self-proclaimed cyber-warriors demonstrate the growing trend in the Marine Corps evolution to a modern battlefield. Photo by Sgt. Robert M. Storm.

VIRGINIA BEACH, Va. (Aug. 12, 2010) Rear Adm. Edward H. Deets III, commander of Naval Network Warfare Command (NETWARCOM), presents a command coin to undergraduate students participating in a Navy Recruiting Command tour at Navy Cyber Forces and NETWARCOM. The students are on a two-day tour aboard afloat and shore commands at Joint Expeditionary Base Little Creek-Fort Story to learn about potential job opportunities in the Navy. U.S. Navy photo by Mass Communication Specialist 2nd Class Joshua J. Wahl.

MESSAGE FROM THE DON CIO

Ms. Barbara Hoffman
Department of the Navy
Chief Information Officer (Acting)

The Department of the Navy Chief Information Officer recently released the DON Cyber/IT Workforce Strategic Plan. This plan establishes the DON's priorities for workforce excellence by identifying the goals and objectives that will allow us to recruit, manage, develop, sustain and retain a talented workforce. The value of the Cyber/IT Workforce to national security is underscored by events such as the appointment of the White House Cybersecurity Coordinator and the stand up of U.S. Cyber Command.

In light of the importance placed on the Cyber/IT Workforce, this issue of "CHIPS," is dedicated to that workforce, and you will see a common thread: To be successful we must enable our people. An important mission of the DON is to secure our networks to the best of our ability. To do this, our workforce must be given the control, guidance, processes, network visibility, tools, education, training and support they need to get the job done. Our people are doing a remarkable job today, but much more can be achieved if we listen to them, identify current and future needs, and implement the processes needed to meet the challenges we face.

TO BE SUCCESSFUL WE MUST ENABLE OUR PEOPLE.

Intuitively, we know that if we accurately communicate the mission to our personnel and give them what they need, we will be successful. If we take care of our people — through recruiting initiatives, retention incentives, and by rewarding performance — then they will be successful. There are a multitude of workforce initiatives underway. They include mandatory certification of the cybersecurity workforce, civilian workforce hiring reform, scholarship and internship programs, and continuous learning, to name a few. We owe it to our people to ensure these initiatives are coordinated and usable.

President Obama released Presidential Memorandum – "Improving the Federal Recruitment and Hiring Process," May 11, 2010, which is about the need to improve the federal recruitment and hiring process. The president is calling on executive departments and agencies to help with the complexity and inefficiency of today's federal hiring process, which deters many highly qualified individuals from seeking and obtaining jobs in the federal government. DON CIO, as the IT Functional Community Manager, is partnering with the DON Office of Civilian Human Resources (OCHR) to assist in streamlining the hiring process. This includes elimination of essay style questions and instead, allowing individuals to apply with resumes and cover letters; use of category rating, which results in an increased number of qualified applicants; and notifying applicants about their status at various stages throughout the process. You may follow the Department of Defense Hiring Reform Initiative at www.cpms.osd.mil/HiringReform/.

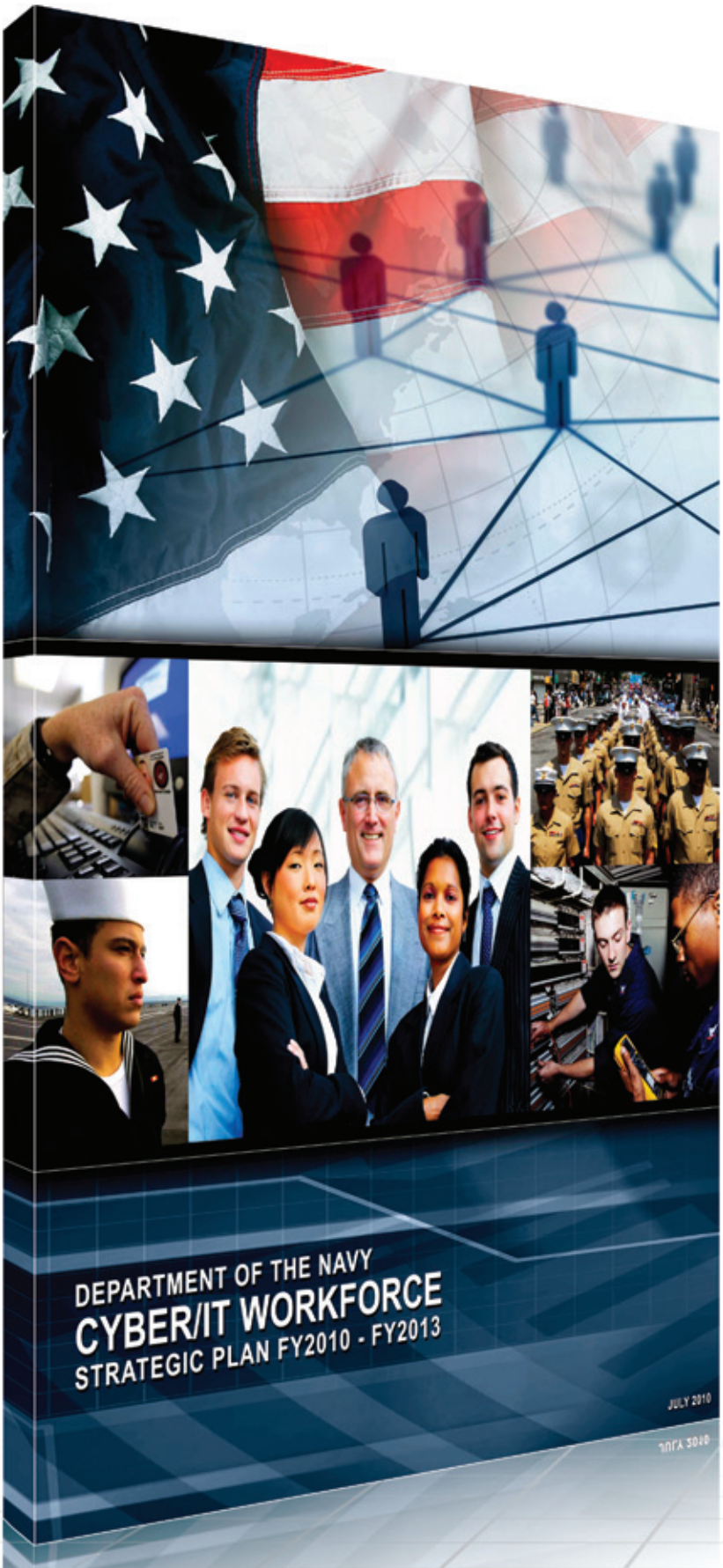
To help us improve our overall cybersecurity capabilities, the DON was recently given authority to hire individuals with cybersecurity skills under Cybersecurity Schedule A hiring authority (available at www.public.navy.mil/donhr/Employment/CivJobOpps/Pages/CyberSecuritySchedA.aspx). Additionally, the DON CIO, working with OCHR and several other DON organizations, developed the selective placement factors for IT Specialist (2210) and Computer Scientist (1550) positions. This effort is in direct support of the emergent needs of the newly created Navy and Marine Corps Cyber Forces Commands and our operational and systems commands.

The Cyber/IT Workforce — a cadre of educated, trained and motivated personnel — is entering a culture where "continuous learning" will be the norm. It is crucial that our personnel develop an Individual Development Plan that addresses individual needs and improves the capabilities of our communities. Our personnel diligently design, operate, maintain and defend the network on a 24/7 basis. Constant attention to detail on the job, supplemented by proficiency through improved skills, will make our workforce world class and second to none.

We are always looking to the future to determine how we need to adapt and improve, and the DON Cyber/IT Workforce Strategic Plan for Fiscal Years 2010-2013 spells this out. I urge you to download it, take a look, and move with us as we bridge to the future. It is available at http://www.doncio.navy.mil/Products.aspx?ID=1839. CHIPS

DEPARTMENT OF THE NAVY - CHIEF INFORMATION OFFICER

WWW.DONCIO.NAVY.MIL


DEPARTMENT OF THE NAVY
CYBER/IT WORKFORCE
STRATEGIC PLAN FY2010 - FY2013
JULY 2010

THE DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER HAS PUBLISHED THE DON CYBER/IT WORKFORCE STRATEGIC PLAN FOR FY 2010-2013. THIS PLAN ESTABLISHES THE DON'S PRIORITIES FOR ENSURING WORKFORCE EXCELLENCE. IT IDENTIFIES THE GOALS AND OBJECTIVES THAT WILL ALLOW THE DON TO RECRUIT, MANAGE, DEVELOP, SUSTAIN AND RETAIN A TALENTED WORKFORCE.

Under the Clinger-Cohen Act and Federal Information Security Management Act, command information officers are responsible for Cyber/IT Workforce planning. The DON Cyber/IT Workforce Strategic Plan details the strategy to develop a highly competent Cyber/IT total force (see Tables 1 and 2) that is capable of implementing, integrating, securing and executing sustained operations across the full cyberspace domain. The DON Cyber/IT Workforce Strategic Plan is the way forward to ensure the department's efforts to provide the best support to commands and to help members of the Cyber/IT Workforce achieve individual career goals.

The strategic plan goals are:

- Provide workforce capabilities that fully support cyberspace operations.
- Develop competency-based planning and management processes.
- Support required capabilities by recruiting a qualified and experienced workforce.
- Develop and manage the DON Cybersecurity/ Information Assurance Workforce.

CHIPS asked the DON CIO Director of the Cyber/IT Workforce Chris Kelsall to discuss the strategy in August.

CHIPS: Could you explain your role in supporting the Department of the Navy CIO Cyber/IT Workforce team? Can you tell us specifically what you do in your role?

KELSALL: As the director of the DON CIO Cyber/IT Workforce Team, I serve as an expert on workforce policy, planning, systems, credentialing and development requirements for the workforce. Additionally, I'm responsible for recommending and integrating new workforce programs and requirements, and developing theories, concepts, principles, standards and methods for workforce development. I also represent the DON in both Defense Department and federal efforts surrounding cybersecurity workforce development, the associated competency development, and in reporting to Congress.

I also serve as the DON lead for the Information Assurance Workforce Improvement Program which includes training and certification efforts. I represent the DON CIO on the Federal CIO Council IT Workforce Committee. All of these activities are accomplished working directly with Navy and Marine Corps Cyber/IT Workforce personnel organizations and folks from our DON Civilian Human Resources Office. Finally, I'm a member of the Executive Board of the Federal Information Systems Security Educators' Association. Their objective is to facilitate information exchange in the area of information systems security awareness, training and education.

CHIPS: What are some of the main takeaways from the DON Cyber/IT Workforce Strategic Plan?

KELSALL: We're doing the work today — and pretty well. We must concentrate

identifying the places we need to focus people and tools to improve, and then we must determine how to train and qualify folks to handle those roles. We have the people; rather than looking to hire 'new skills' we must identify who has those skills today and how to balance the roles and work within the workforce. We must also continue to bring in new talent to build them into the replacements for those who leave the department.

We must work with academia and research and development organizations to know what's changing and what new employees will bring with them so we can integrate them rapidly into our workforce. Knowledge, skills and abilities (KSAs) don't fit the bill in this area; what's being done and what people are actually being equipped with does. We must be able to speak with a common language across DoD, federal agencies, private industry and academia. No longer can we fall into 'DoD speak' in this area. If we're going to be able to work the 'security risk to one in cyberspace is a risk to all' issue we must be able to understand each other.

CHIPS: How are you able to ensure the Department of the Navy has the leadership commitment, the resources and the initiative to develop the Cyber/IT Workforce?

KELSALL: The DON leadership, cyber/IT leaders and human resources leadership are all committed to ensuring the DON has the most capable Cyber/IT Workforce in the world. The policy and strategic planning guidance we are receiving from the top is putting us on the path to realizing that goal. Also, the people within the DON who are working these issues have direct access to leadership — the cyber/IT flag officers and the senior executive service personnel — on a daily basis. These working relationships across the department, including with the Navy and Marine Corps, have allowed us to coordinate across the services and organizations. The workforce itself has really jumped at this opportunity. They are very committed. We've established teams that work together on workforce issues, policies, strategies and the requirements that are needed to move forward. All of these are developed with input from workforce personnel across the department.

Just as importantly, the human resources leadership and key workforce members have been working with us on a daily basis to ensure they provide the knowledge needed to execute strategies and workforce plans and provide the human resources information that is necessary to realize our recruiting and hiring principles. Additionally, the DoD has established teams to specifically address Cyber/IT Workforce requirements and issues. This venue provides us the additional opportunity to share across the DoD components, and where needed, gain visibility at the DoD level for workforce needs.

"As one of the Nation's leading employers, the Federal Government is in need of highly skilled individuals to meet agency staffing needs and to support mission objectives. Our veterans, who have benefited from training and development during their military service, possess a wide variety of skills and experiences, as well as the motivation for public service, that will help fulfill Federal agencies' staffing needs."

~ Mr. Barack Obama
President of the United States

CHIPS: How will the Navy recruit the right people with the right skills?

KELSALL: Our recruiting actions today are getting us the folks we need today, but if we are going to fully understand and attract the future workforce, we're going to need to become even more involved with academic institutions from universities, to vocational schools, to high schools. We need to understand the skills people will be bringing with them. If we're going to appeal to people we need to be able to provide an environment where they can apply what they've learned, and we've got to be able to convey that to them. If we truly understand the people who have an interest in joining our team, we must know what they are looking for and become part of the environment in which they exist — schools, social media, research and development, and anywhere else we can.

"The opening rounds of the next war will be in cyberspace — the Navy must be ready to prevent wars as well as win them; to do that, we must understand how we will live, operate, and win in cyberspace."

~ Adm. Gary Roughead
Chief of Naval Operations

CHIPS: What skills will they have to have already, and what will the Navy train people for?

KELSALL: We look for aptitude and background for our military folks, and education and experience for our civilians. The fundamentals should match across the board; we'll just need to provide the education to our military folks up front if they don't have the background. The key is that we'll need to provide valuable continuing education for everyone on an individual level. Gone are the days where our people 'are hired with everything they need.' It is crucial that we provide the means for our workforce to stay current. Additionally, we must provide training for our teams. People don't work alone anymore; defending our networks is a team effort. We'll have to continually challenge them in simulated environments as a team if we're going to stay ahead of our adversaries.

CHIPS: How do business skills mesh with cybersecurity skills?

KELSALL: As we're now at the point where cybersecurity has become a mission area along with our warfighting

and business mission areas, we must have people who understand the 'business' of the DON in the Cyber/IT Workforce. We can't afford to take hundreds or thousands of requirements identified by functional area managers, translate them into system specifications, and then give our warfighters a tool that we think does what they want. We have to develop our new tools as a team, so our techies must also speak the business language and be part of the business process. We'll need to cover everything; cybersecurity and our IT tools are everywhere and support all of our operations. Plus we'll need to be able to support operations outside of the DON, not only with federal, state, local and private organizations, but also with our international partners.

CHIPS: What are some challenges that you are facing? How are you going to overcome them?

KELSALL: The primary challenge faced by the community is the future requirements that will need to be addressed. We have to constantly look at our needs regarding our current systems, networks and telecommunications, but we also have to look at how we are going to do business in this new world defined by cybersecurity. Right now, there are multiple studies, reports, pending legislation and efforts addressing the nation's cybersecurity workforce. Once the new structure of the Defense Department's cyber domain is fully outlined, we'll need to take a hard look at how we structure our workforce to align with it. We will be doing this while balancing the other workforce requirements of the department. We will have to work directly across multiple occupational areas to ensure that we have the right resources necessary to be that world-class workforce that we talked about.

CHIPS: Is there funding for FY11 to meet the training requirements of the Cyber/IT Workforce? Readers will want to know where the funding in individual commands will come from.

KELSALL: Yes, there is funding for FY11. Every command receives money for civilian training every year. However, command IOs and IT staffs must make sure they are budgeting for civilian cyber/IT training. Military training requirements are being funded through the education and training commands for the most part. Military personnel attending the different military training schoolhouses will receive the appropriate training as part of revised curriculums. Electronic training has been funded by the enterprise, and therefore, is available for no cost to individual commands. This training is readily accessible to the workforce. CHIPS

See the e-Learning article in the July - September 2010 issue of CHIPS for more information: www.chips.navy.mil/archives/10_Jul/web_pages/e-Learning.html.

Table 1: DON Civilian Cyber/IT Community

Series	USN	USMC
2210 – IT Specialist	6,688	1,354
1550 – Computer Scientist	2,734	45
0332 – Computer Operator	50	55
0335 – Computer Clerk and Assistant	207	20
0390 – Telecommunications Processor	54	17
0391 – Telecommunications	586	126
0392 – General Telecommunications	47	9
0394 – Communications Clerical	15	5
1410 – Librarian	94	32
1411 – Library Technician	214	125
1412 – Technical Information Services	62	11
1420 – Archivist	12	N/A
1421 – Archivist Technician	5	N/A

Note: Marine Corps numbers include nonappropriated fund personnel. Series 1420 and 1421 are not considered part of the Marine Corps Cyber/IT community.

Table 2: DON Military Cyber/IT Community

Rank	USN	USMC
Officers	1,842	1,091
Enlisted	12,155	6,607

Talking with Vice Adm. Jack Dorsett DCNO N2/N6

Vice. Adm. Jack Dorsett

Vice Adm. Jack Dorsett, Deputy Chief of Naval Operations for Information Dominance (N2/N6), Director of Naval Intelligence (DNI) and workforce leader for the Information Dominance Corps, talks about training opportunities and career management for IDC officers and enlisted personnel. The IDC is composed of military and civilian cyber warriors who will execute the Navy's strategy to enable information to emerge as a core warfighting capability equivalent to U.S. Navy sea and air power. The admiral responded to CHIPS questions in early October.

CHIPS: The Department of the Navy Chief Information Officer published the DON Cyber/IT Workforce Strategic Plan in July. This plan establishes the DON's priorities for ensuring workforce excellence. It identifies the goals and objectives that will allow the DON to recruit, manage, develop, sustain and retain a talented workforce. Is the Information Dominance Corps included in this strategy, or will you and the Chief of Naval Personnel develop a different strategy for military and civilian personnel in the Information Dominance Corps?

Vice Adm. Dorsett: The Navy faces the challenge of expanding its cyber capabilities while at the same time working within a resource constrained environment with competing programs vying for limited funds. The IDC and DON CIO have been working closely throughout the development of the Navy's cyber capabilities, to include a new manpower and training strategy. This strategy will lead to a solution that is Navy-specific but still compatible with more comprehensive DON CIO strategies.

CHIPS: In our April-June 2010 CHIPS interview, you emphasized how important cross-training would be in the development of the IDC. You indicated that Personnel Qualification Standards were in development across all the disciplines. Have these standards been completed? Have any career paths been formalized?

Vice Adm. Dorsett: Qualification as an Information Dominance Warfare Officer (IDWO) or Enlisted Information Dominance Warfare Specialist (EIDWS) requires completion of cross-IDC core Personnel Qualification Standards. Each community has its own unique PQS required, in addition to the core qualification. All are now available with the exception of the Space Cadre PQS, which remains in development. Distinct community career paths existed previously and these remain largely intact after the formation of the IDC. However, in an effort to offer significant professional development opportunities for senior leaders, and better position IDC senior officers for future leadership, a number of cross-detailing opportunities have been added at the O-5 and O-6 paygrades. These tours are not mandatory for promotion, but they do take officers into billets outside of their normal career paths, broaden their knowledge and enhance their leadership skills, while improving the overall quality of officers across the IDC.

CHIPS: The DoD CIO study "Net Generation: Preparing for Change in the Federal Information Technology Workforce" identified the need for a significant cultural shift to attract and retain younger workers. Within the workplace, the Net Generation wants flexibility in work hours, pay for performance, the ability to have their voices heard, continual performance feedback, and access to advanced technology and social networking applications. Although some changes have been made, many leaders say that military personnel policies and programs need to evolve. You indicated in our previous interview that you and the Chief of Naval Personnel were working on needed changes. Can you talk about the status of changes?

Vice Adm. Dorsett: Navy recognizes that the Net Generation has different needs and expectations as they enter the workforce. We have already embraced many of the changes this new and capable generation of workers sees as important to their job satisfaction, professional development and career success. The Navy work environment now includes options for flex schedules and for telework, and we will continue to explore ways to leverage technology to make the workplace remotely accessible and more dynamic.

The current Defense Civilian Intelligence Personnel System (DCIPS) has helped to institutionalize management by objectives and a process that provides performance feedback. We have also developed advanced education opportunities to include academic fellowships, tuition payment, part-time study, and other mechanisms that appeal to a generation that is committed to lifetime learning. Many of the larger initiatives, to include social networking applications and other new technologies, are part of larger DoD policy efforts. Navy has been an active participant in promoting 'out of the box' approaches as the department seeks to balance innovation with practical security concerns.

The bottom line is that Navy's workplace environment, and the means we will use to attract and retain a world-class workforce, will continue to evolve. This is not an area where we are satisfied with the status quo.

CHIPS: Since the consolidation of various disciplines, an estimated 45,000 positions, come under the Information Dominance Corps, which includes: 1800 – Meteorology/ Oceanography, 1810 – Information War-

The Information Dominance Corps will consist of an estimated 45,000 active and Reserve Navy officers and enlisted and civilian professionals who possess extensive skills in information-intensive fields to develop and deliver dominant information capabilities in support of U.S. Navy, joint and national warfighting requirements.

fare, 1820 – Information Professional, 1830 – Intelligence, 1840 – Cyber Warfare Engineer, 1850 – Any IDC-qualified officer billet, Civilian Intelligence, Network Operations, Space Cadre, Cryptology/Signals Intelligence, Information Operations and Electronic Warfare, have you had any feedback from these communities?

Vice Adm. Dorsett: A series of IDC 'Road Shows' involving experts and senior leaders from all IDC communities was conducted at major commands and fleet concentration areas around the world in the last few months. The Road Shows were intended to inform our personnel about the IDC and give them the opportunity to ask questions directly of their communities' officer and senior enlisted representatives. Road Show feedback indicates that while IDC Sailors and civilians have a number of questions about what the IDC realignment means to them and their careers, the overall feeling is very positive and IDC Sailors are excited about the futures of their communities.

CHIPS: One of the most exciting changes affecting the IDC is that the Navy is prepared to make the investment in personnel and training to create an elite, world-class corps of professionals. Will the current budget climate affect your vision to grow and train the Information Dominance Corps?

Vice Adm. Dorsett: Achieving this level of prominence in the current fiscal environment will be challenging. That said, a trained and focused IDC is actually a force multiplier that will increase the capability of the force without a corresponding growth in capital investment. 'Manpower, Personnel, Training and Education' (MPT&E) initiatives that align IDC management, consolidate staff functions, and innovate training are underway. These are designed to optimize operational effectiveness and ensure the development of a world-class corps of professionals.

CHIPS: Colleges and universities are offering summer cyber boot camps and formal courses to anticipate the growing job market for cyber professionals. Is the Navy in discussion with academia about a standardized curriculum that would offer the most value to students who would like to work for the Navy or Defense Department?

Vice Adm. Dorsett: Navy has initiated a Cyber Option NROTC Scholarship program that is a key part of a comprehensive Navy strategy to attract, recruit and develop the elite cyber professionals needed to operate securely and effectively in cyberspace. The scholarship is specifically for high school and college students who excel at the U.S. Cyber Challenge competitions (see www.uscyberchallenge.org/featured/navy-scholarships.php). The Cyber Challenge is a national talent search and skills development program that identifies young Americans with the interests and technical skills required to fill the ranks of cybersecurity practitioners, researchers and professionals who become the innovative leaders in cybersecurity.

CHIPS: Will training for cyber military and civilian positions be similar so that their job responsibilities could be interchangeable?

Vice Adm. Dorsett: Cyber training will be primarily interchangeable for military and civilian personnel. However, there will be limitations on specific assignments due to operating environments. Some assignments are inherently military due to the likelihood of direct or imminent combat operations or basing on an operational platform (sea or air based).

CHIPS: Under Secretary of the Navy Robert Work said, "Every IT professional in the Navy and Marine Corps has to think of themselves as a warrior. The network is their weapon." How do you convey that sense of responsibility to junior enlisted and young civilian employees who grew up with an ease for using social media, texting and gaming, and who may not recognize the seriousness of Mr. Work's message?

Vice Adm. Dorsett: The Navy continues to educate the entire workforce on threats that pose a danger to its IT infrastructure and the appropriate mitigation strategies. The most recent example of these efforts is the 19 Aug. [issuance of] ALNAVs 056/10 and 057/10 to all Department of the Navy employees providing guidance on official and non-official posts on the Internet, to include social media sites, and the need to be professional and security conscious. It is imperative that we implement and enforce policies to ensure the security of Department of Navy networks. The DoD [Directive] 8570.01 Information Assurance Workforce (IAWF) certification requirements will ensure that our IT professionals are prepared to administer and secure DoD networks. CHIPS

For more information, go to the Navy Personnel Command website at www.npc.navy.mil/.

Taking Stock

By Mary Purdy

The Making of the CIO

"The Power of Team: The Making of a CIO," a seminal book written by the Department of the Navy Chief Information Officer (DON CIO) staff in 2002, is used throughout information technology (IT) classrooms across the services, and still remains relevant to the changing world of the CIO. Some fundamental points of the book are that CIO organizations need to stay on the leading edge of change, manage through change, and innovate so initiatives stay aligned to the changing technical environment. A dynamic staff, flexible and energetic, is best to tackle and accomplish the tasks associated with adapting to the ever evolving information environment.

By organizational standards, it was only a short time ago that the Clinger-Cohen Act of 1996 mandated the establishment of federal CIOs, and thus, the DON CIO. Later, the Secretary of the Navy established the two service-level DON Deputy CIOs, (Navy and Marine Corps). Several other laws (see the CIO responsibilities box) brought about the requirement to establish clear accountability for information resources management, and service subordinate command information officers (IOs) were created. During the last decade, command IO staffs have worked zealously to become established, grow, and finally, thrive.

The Evolving Role of the Command IO

As organizations continue to define and institute the appropriate workforce structure, they improve in mission effectiveness. It is an ongoing process to understand the organization's value and seek improvements. The fourth quarter of the calendar year is always a good time for the CIO organization to pause and "take stock" of its accomplishments. Through review of "The Power of Team" (available via the DON CIO website: www.doncio.navy.mil/Products.aspx?ID=440), the command IO can see how the individual organization compares to those standards set back in 2002. In addition to a thorough retrospect, a healthy organization will also envision the future, review its successes and challenges, define its requirements to grow in the future, and look forward to change.

Command IOs have a responsibility to organize, expand and adjust their workforce to meet today's information environment. Because of the DON's increasing dependence on IT and command, control, communications, computers, combat systems and intelligence (C5I), the command IO position is even more relevant today than it was five or six years ago. In today's environment, command IOs may be involved in everything from information systems policy-making to advising on technical aspects of warfighting and mission planning, providing social networking rules, securing the Global Information Grid, protecting personally identifiable data and preparing IT budgets.

Metrics

The interest in metrics related to the services' ability to provide efficient and cost-effective support to the warfighter has never been greater than it is now. From the Federal Information Security Management Act (FISMA) to the White House's mandate for transparency in government, the services are on the verge of moving from monthly reporting to continuous monitoring.

Vivek Kundra, the first White House appointed CIO, has pledged to increase oversight on all agency IT investments. The Department of Defense (DoD) will not be exempt from this new review process. Service command IOs and their staffs are challenged by the need to adjudicate and balance command funding requirements for information sharing, user friendly tools and information assurance initiatives. Additionally, with the Secretary of Defense's direction to move the DoD toward a more efficient, effective and cost conscious way of doing business, service command IOs may be required to address these topics in a more resource-constrained environment.

CIO RESPONSIBILITIES

The Goldwater-Nichols Act of 1986
Directed the Secretary of the Navy to establish an office to conduct information management. The bill went on to say "no office or other entity may be established or designated within the Office of the Chief of Naval Operations or the Headquarters Marine Corps to conduct information management."

Paperwork Reduction Act of 1995
Instructed agencies to designate a senior official responsible for carrying out the agencies' information resources management activities to improve agency productivity, efficiency and effectiveness.

Clinger-Cohen Act of 1996
Requires processes to be developed for: capital planning, modular contracting, business process reengineering, training and IT workforce competencies, standards and architectures, performance and results-based management and strategic planning. This act establishes chief information officers for executive agencies.

Given the changing funding environment, service command IOs must take stock of their current efforts to manage their mission needs. The DON has established several enterprise electronic tools, such as the Department of the Navy Application and Database Management System (DADMS) and Department of Defense IT Portfolio Repository-Department of the Navy (DITPR)-DON to manage IT projects. However, for individual command initiatives, a clearly defined requirement, cost analysis and measurement toward progress through electronic means will show commanders and commanding officers that the command IO is not only a good steward of the organization, but a skilled IT program and business manager. The functional area managers, teaming with the command IOs, will validate individual program requirements and require extensive documentation to support additional requirements.

Howard Schmidt, the first White House cybersecurity coordinator, has pledged to have greater insight into the cybersecurity architecture of agency systems. Therefore, all CIOs, from the White House and the DoD CIO, to the DON and DON Deputy CIOs, to command IOs, may expect to provide more visibility into the security posture of IT systems. The Office of Management and Budget guidance released in fiscal year 2010 stated that FISMA reporting for agencies will follow a three-tiered approach: (1) Data feeds directly from security management tools; (2) Governmentwide benchmarking on security posture; and (3) Agency-specific interviews. For DoD, this data will be electronically reported through several different service component electronic systems.

The Federal CIO's Core Responsibilities

Regardless of heightened congressional oversight, CIOs need to attend to their core responsibilities which are to ensure information and information systems are designed, managed, disseminated, secured and protected to ensure privacy in a cost effective manner. CIOs are required to oversee the education and training of the Cyber/IT Workforce. This oversight comes with the task of ensuring increased training requirements are funded. One way to reduce expenditures is to leverage strategic partnerships with law enforcement and intelligence communities to combine critical cybersecurity training, and this is being accomplished through an initiative with DON CIO and service staffs. However, command IO staffs will continue to budget for civilian cyber training while military training will be funded by the education and training commands.

Actions to Empower the Command IO

Real world requirements continue to put stress upon our command IOs. As the services continue to focus on cyber and cybersecurity, Congress is also working to determine cyber roles and authorities. The National Defense Authorization Act for FY 2011 includes language that updates FISMA and establishes a National Office for Cyberspace in the Executive Office of the President. Throughout all of this, one thing is clear: Command IOs will be relied upon to have more stringent IT oversight and make "lean and mean" financial decisions so IT acquisition will go further in buying more capability. Some tried and true actions which, if taken, can empower organizational command IOs and staffs are:

- Build a strong CIO organization with strategic planning, IT, cybersecurity, budget and workforce expertise;
- Consolidate and reuse IT infrastructure;
- Make metrics and continuous assessments your friend;
- Communicate and use social media to engage the organization;
- Be a good fiscal steward;
- Attract millennial workers to balance the heavily weighed "boomer" workforce;
- Assign everyone an individual development plan to ensure continuous learning; and
- Develop billet structures so civilian 2210s and military IT/C4 professionals are put in career paths that lead to CIO.

Going forward, command IO staffs should expect to continue to take stock of the evolving cyber landscape, embrace change, focus on providing the best value for the money and listen to customers' needs. It is not enough to expand an organization's IT business portfolio; command IOs must continuously develop both their own personal knowledge portfolio, as well as that of their staff. The future DoD funding environment requires tomorrow's workforce to be well educated, decisive, and ready to work as a team. Metrics collected electronically will tell the story, and CIOs, while in a rapidly evolving environment, will be more accountable than ever before. CHIPS

Government Information Security Reform Act of 2000
Reconfirms the role of the CIO as the provider of the agency's strategic view of architecture and cross-cutting security needs. Among other things, it states that federal agencies must designate a senior information security official.

National Defense Authorization Act for Fiscal Year 2011
Directs updates to the Federal Information Security Management Act (FISMA).

Mary Purdy has a GIAC Security Leadership Certification (GSLC) and is the cybersecurity/IA workforce management, oversight and compliance manager for the DON CIO Cyber/IT Workforce team.

Talking with

MASTER CHIEF PETTY OFFICER OF THE NAVY (SS/SW) RICK D. WEST

West talks about career development and the Information Dominance Corps

MCPON (SS/SW) Rick D. West

Master Chief Petty Officer of the Navy (MCPON) (SS/SW) Rick D. West has served as MCPON since 2008. MCPON serves as the senior enlisted adviser to the Chief of Naval Operations and to the Chief of Naval Personnel in matters dealing with enlisted personnel and their families.

The MCPON is also an adviser to many boards dealing with enlisted personnel issues; is the enlisted representative of the Department of the Navy at special events; may be called upon to testify on enlisted personnel issues before Congress; and maintains a liaison with enlisted spouse organizations.

West fulfills his responsibilities to the Navy's missions and for the well-being of Sailors with tremendous vigor and passion. When MCPON talks, Sailors listen — naval leadership listens as well. CHIPS asked West if he would talk about the significant changes and training opportunities for enlisted personnel who are part of the Information Dominance Corps.

CHIPS: Vice Adm. Jack Dorsett, DCNO for Information Dominance and the Director of Naval Intelligence, designated the Information Dominance Corps as the first line of naval defense in the cyber fight. As the workforce leader for the IDC, the admiral said he will set the training standards high. Are Sailors in the IDC excited about the training, new Personnel Qualification Standards and promotion opportunities that will be available to them?

WEST: Sailors are excited about the opportunities that are available to them, and leaders need to take every opportunity to ensure our Sailors are on the right career path and challenging Sailors to stay on track regarding both in-rate and warfare qualifications, and for advancement.

The rigorous qualification program for the new Information Dominance Corps Warfare insignia is an excellent opportunity to provide IDC Sailors with a solid foundation regarding knowledge of the command/warfare assigned. Sailors should always be looking to increase their level of knowledge and scope of responsibility through a continuum of learning — even after obtaining the warfare qualification.

CHIPS: I understand that you have already visited some of the cyber/network commands where IDC Sailors work. Which commands have you visited?

WEST: I have visited many cyber/network commands and will continue to aggressively visit with these warriors. To name a recent few, I've seen Sailors working hard at Navy Information Operations Command Denver, NIOC Maryland, and in Europe, I visited NIOC Menwith Hill and Navy Information Operations Detachment Molesworth, and I was impressed. Visiting these commands gives me a level of knowledge of what each command and the Sailors assigned are responsible for and what they do for our Navy.

Everywhere I go, I am continually amazed by our Sailors and their performance. They are performing their mission well; I'm very proud of what they do. I routinely speak about issues affecting them and their families, but to do this I need to be well-versed in their mission and interested in what is on their and their families' minds.

CHIPS: In a study by the Department of

SANTA RITA, Guam (Aug. 19, 2010) – Master Chief Petty Officer of the Navy (MCPON) Rick West meets with chief petty officer selectees from the submarine tender USS Frank Cable (AS 40) during his visit to U.S. Naval Base Guam. MCPON is continuously traveling and meeting with Sailors worldwide to answer their questions and address their concerns on a wide range of issues, from career and professional development, warfare qualifications, promotion opportunities, to quality of life, health and work-life balance. MCPON is continuously assessing and reporting on what is foremost on Sailors' minds to naval leadership and Congress. U.S. Navy photo by Mass Communication Specialist 1st Class Jennifer A. Villalovos.

NORFOLK Aug. 5, 2010) – Master Chief Petty Officer of the Navy (MCPON) Rick West holds an all-hands call aboard the amphibious assault ship USS Kearsarge (LHD 3) during his visit to Naval Station Norfolk. West is wearing the Navy Working Uniform (NWU) Type III during the conformance test phase. The NWU Type III will replace the existing tri-colored woodland camouflage utility uniform, will be the standard camouflage uniform worn in CONUS, and can be worn while deployed as prescribed by combatant commanders. Occasion for wear of the NWU Type III will be the same as the current woodland camouflage utility uniform per NAVADMIN 188/09. U.S. Navy photo by Mass Communication Specialist 1st Class Jennifer A. Villalovos.

Labor, it was reported that young people entering the job market want flexible working arrangements and to work with advanced technology. Do you think that the Navy's emerging cyber jobs can attract top performers and meet their expectations?

WEST: Yes, I do. In our great Navy we have the most advanced equipment and technology, our weapons systems are the best money can buy and our platforms are unchallenged worldwide. Simply put — our Navy is the best it's ever been, and many would say it is because of the advanced technology. All of those things are important, but the engine that truly drives our Navy and the reason we are the best is because of our people. Our Sailors are what makes our Navy the best that's ever sailed the world's oceans.

The Navy has been nationally recognized for excellence in workforce planning, training, education, diversity, and life-work integration, and continues to attract, recruit, develop, assign and retain our force. Our Navy is a rewarding place for our nation's best and brightest to serve.

CHIPS: When you visit Sailors is there a common theme in their concerns no matter what rating they are in?

WEST: I don't really see a common theme per se; it's cyclic with what's going on in the nation and the Navy. What I do see is our Sailors like to be informed and, in fact, they are more informed today than they've ever been in the history of the Navy.

On a personal level, I enjoy speaking with and hearing from Sailors. Speaking at command all-hands calls and symposiums and receiving questions on my Facebook page are just a few of the ways that I communicate with Sailors, their families, our Navy civilians and our retired population. I receive a wide variety of questions. Sometimes I get the same questions, but that's why communication is key. It's important for Navy leadership to continually strive to find different methods to communicate.

"There is nothing a Sailor can't accomplish if you provide solid leadership and clearly communicate the expectations that you as a leader have in them … More importantly, they should know what they should expect from you!"

– Master Chief Petty Officer of the Navy (MCPON) Rick West

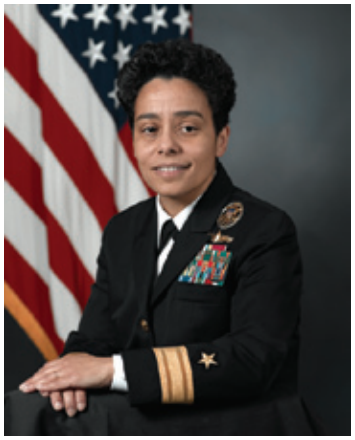
CHIPS: Do you have a vision for what you hope to accomplish while you are MCPON?

WEST: Continue to support our Sailors and their families to both leadership and lawmakers. To provide an atmosphere in which we challenge each of our Sailors to live up to and achieve their true potential, but, more importantly, providing them [with] both the opportunities and the resources to do so. Additionally, I hope to continue fostering an atmosphere that capitalizes on the diversity, ingenuity and passion that our Sailors have for our Navy and our great nation by continually seeking out new opportunities to communicate with our Sailors and their families.

I'm proud of our Navy and what our Sailors accomplish daily, there is nothing a Sailor can't accomplish if you provide solid leadership and clearly communicate the expectations that you as a leader have in them … More importantly, they should know what they should expect from you! Our cyber forces are on the cutting edge of technology — simply put: They are on the front lines everyday! CHIPS

Follow MCPON on Facebook at www.facebook.com/MCPON. For more Navy news, go to www.facebook.com/USNavy or www.navy.mil.

A Few Minutes with Rear Admiral Michelle Howard
Commander, Expeditionary Strike Group 2


Rear Adm. Michelle Howard

Rear Adm. Michelle Howard, as the commander for Expeditionary Strike Group Two, has oversight of 15 amphibious ships and Naval Beach Group Two with its four tenant commands. Expeditionary Strike Group Two includes: four landing helicopter dock (LHD) ships, one landing helicopter assault (LHA) ship, four landing platform dock (LPD) ships and six dock landing (LSD) ships. Howard took command of the USS Rushmore (LSD 57) on March 12, 1999, becoming the first African American woman to command a ship in the U.S. Navy. In 2006 she was also the first woman graduate of the U.S. Naval Academy to be selected for the rank of admiral. Rear Adm. Howard was the commander of Combined Task Force 151, which rescued the ship's master when pirates captured the Maersk Alabama in 2009.

Howard has been selected for promotion to rear admiral and will be assigned as Chief of Staff, J5, Joint Staff, Washington, D.C. CHIPS spoke with the admiral July 8 — just days before she was due to report to her new assignment to the Joint Staff.

CHIPS: As a surface warfare officer and commander of Expeditionary Strike Group 2, what are your technology needs, and what capabilities do you wish you had?

Rear Adm. Howard: The question about capabilities you wish you had is always a dangerous question because that means you want transporters like in 'Star Trek' vice the capabilities that are [realistic] requirements.

When you use the 'wish' word it gets dangerous; it means going down the path of what people desire and going past what they need — the request. In terms of needs, like most operational strike groups, we need reliable long-haul communications, we need bandwidth, and we need it across the force. One of the challenges we deal with [is that] operationally capabilities are not evenly distributed in terms of capacity, so life on a smaller ship is always more challenging than life on a big deck amphib in terms of communications capacity.

The other piece is interoperability as we move around the theater, not just within Navy forces, but with other services, joint, coalition partners and non-governmental organizations, [and] having common gear so that we can not only communicate, but also share a common operating picture. That is really [important], particularly when we get in missions like humanitarian assistance/disaster relief (HA/DR) and counterpiracy which are fundamentally unclassified missions in terms of information sharing.

Having an operating picture on the unclass side that we can use with coalition partners, as well as NGOs, and as real time as possible, that's what I would wish for.

CHIPS: What are the essentials that expeditionary forces depend on?

Rear Adm. Howard: If you look at expeditionary writ large, it is not just the amphibious forces under ESG 2, but it is also the expeditionary forces that come under NECC (Navy Expeditionary Combat Command). We do work with explosive ordnance demolition folks, and we do work with divers. One of the pieces we have to get at is commonality of equipment. It's a piece we work at all the time with the Marine Corps. You can't have different radio sets and different receiver groups. You have to be able to talk … 'Blue' has to be able to talk 'green.' We have to get that sort of commonality thought process working across all the different forces that make up expeditionary forces.

CHIPS: The ESG 2 mission mentions the Navy/Marine Corps team that provides robust "blue/green" capability unrivaled by any other combined force. What characteristics of the team make this combined force so strong?

Rear Adm. Howard: The first thing that comes to mind is flexibility, a very professional, well-trained force. When you look at the blue/green team and you look at the maritime strategy, the major pillars — power projection, sea control, humanitarian assistance/disaster relief — those tasks skill sets are core to the Navy and Marine Corps.

The characteristics associated with a traditional blue/green team, ARG/MEU (Amphibious Ready Group/Marine Expeditionary Unit) from other order of ships and a special MAGTF (Marine Air Ground Task Force), is one of the flexibilities.

The forces have trained across the range of missions for the last two decades, illustrated by the Nassau ARG with the 24th MEU deployment that started in January when the ship and the Marines went out. As they went to U.S. Central Command they diverted south, went to Haiti, did humanitarian assistance/disaster relief, and then two weeks after that went back to their original mission and became the Theater Reserves — 5th Fleet's Theater Reserve — relieving the USS Bonhomme Richard ARG and 11th MEU in Central Command.

You have almost the span of the range of military missions within one deployment, and the execution by the blue/green team [is] just perfect in terms of supporting those missions and getting the job done. It's that flexibility that is probably the greatest characteristic of the Navy/Marine Corps team.

CHIPS: The ESG 2 mission statement mentions that ESG 2 provides the bridge between the Navy and Marine Corps planning efforts. How is team planning executed?

Rear Adm. Howard: We have natural counterparts with several Marine organizations. We are working with a MEF (Marine Expeditionary Force) for a Bold Alligator exercise coming up this winter to exercise how the Navy and Marine

Corps operate together. Bold Alligator is an exercise geared to the ESG/MEB (Marine Expeditionary Brigade) level to revitalize amphibious planning and execution skills. The training audiences are ESG 2 and 2nd MEB. We will work within a scenario using the current force structure. The effort should integrate and operationalize emergent operational concepts, doctrine, policies and technologies.

We have integrated relationships with the Marines' concept development group, MCCDC (Marine Corps Combat Development Command). We also have natural relationships with expeditionary warfare on the Chief of Naval Operations staff, which is the part of the CNO's staff where there are Marines embedded, and I have Marines on my staff.

The Expeditionary Strike Groups 2, 3, 7 and 5 in Bahrain are Navy and Marine personnel making up a staff with a commander that is a one-star rear admiral. We have organic expertise from the Marine Corps and then that makes us the advocates and the subject matter experts for amphibious missions and expeditionary missions that fall into our domain.

My time spent with the amphibious forces is incredibly educational; it is not just the perspective of the mission set, learning how to plan the mission set and then executing it. You are working with a separate service, you are still one department, but there are language and culture [differences] because each military [service] has its own set of acronyms and language. But it is also educational to learn about the entire Department of the Navy beyond the 'Corps Blue' that most of us grow up in.

CHIPS: You were the head of the Combined Task Force 151 when the Maersk Alabama was captured by pirates in April 2009. What are the lessons learned from the successful rescue of the ship's master, and what were your thoughts during operations?

Rear Adm. Howard: One of the major lessons was a lesson relearned, which is that we have terrific Sailors and Marines, particularly the USS Bainbridge (DDG 96), which was the lead ship in that operation, and the special forces that boarded [the pirate vessel]. There were several ships out there, different associated assets were [involved], and every person did their job. The quality of people that we have, the care that they have, and the passion was probably the primary ingredient in that mission being successful.

From a tactical perspective, I could not have done that mission if we did not have reliable long distance communications. Look at Central Command, from the Somali Basin all the way to the Gulf of Aden, and the ships distributed through there with the fleet commander being homeported out of Bahrain, [it is] thousands of miles, and you are trying to coordinate with our headquarters, as well as coordinate with tactical units as the mission unfolds, so long distance communications were an essential mission set.

Another tactical piece that was a new lesson learned for me in terms of intelligence is that there are limitations to reachback. When you look at intelligence, and you go from the gathering phase to the analytical phase, there are advantages and benefits derived from having that core competency across the entire process chain, collocated with the commander.

If you are using reachback for the analysis phase, for example, the time and delay in pushing information back, having it analyzed and pushing it forward may not be timely for you to incorporate the knowledge that comes out [of reachback] as the mission moves forward.

The support overall was just tremendous, whether it was from civilian organizations or the fleet commanders. There was a huge on-scene team; there was a much larger remote team from Central Command going all the way back to the United States.

CHIPS: Navy leadership is promoting diversity in leadership positions throughout the Navy. What advice do you have for rising officers and enlisted?

Rear Adm. Howard: Officers and enlisted [personnel] at some point have to make that journey to where they don't consider themselves part of the team — but they consider themselves the leaders of the team. My advice on diversity is that people as leaders get to an understanding of what diversity means for themselves and what diversity means for their organization.

CHIPS: In listening to your remarks at the Women in Defense breakfast April 8, in Virginia Beach, Va., I think anyone would be lucky to have you as a mentor. Do you have advice for the first women on submarines?

Rear Adm. Howard: Within the framework of integrating new units, one of the factors you have to look at is that the numbers of people who are integrating are generally very small. At some point in an organization when you go through the integration process, you hit this critical mass, where the new units are no longer obvious because they are part of the team.

At the breakfast, I think I mentioned that the Department of Labor considers work as nontraditional when women make up 25 percent of the organization or community. When you are starting off, and you are in the bow wave of small numbers, there is a need for that initial group of people to stay connected to each other to have sounding boards and someone to share thoughts with and walk through sessions on this happened, how should I react, and what should I be doing — or here are some challenges that I am dealing with.

There are very few people that they are going to be able to go talk to and are going to have a shared experience with. It is important that they find out who the other women are and, in some cases, it will be the women they are serving with on the submarine. They should stay connected to each other and create a self-support system.

CHIPS: Would you like to talk about your next assignment on the Joint Staff?

Rear Adm. Howard: I am sorry to be leaving the waterfront; this is where the Sailors and Marines are. I think anyone who has had the privilege of leading Sailors and Marines knows this is why we stay in. They are just a group of people who perform miracles all the time.

The next job is J5, chief of staff. For me, Joint Staff is always an exciting place to serve. Last time I was there, it was maybe too exciting because that was when 9/11 occurred. It probably won't be that exciting this time, but it is professionally educational observing the leadership and then contributing to policy that has impact on the armed forces. It has always been professionally challenging but professionally rewarding as well. CHIPS

GOING MOBILE

Trends in Workforce Mobility

By Mike Hernon

While it is axiomatic to say that the speed of technological change is breathtaking, the past year in particular has witnessed a spate of announcements in the mobility world that is truly unprecedented. New operating systems, smarter smartphones, and new device types seem to appear on a weekly basis. For the technically inclined, this represents a smorgasbord of delights. What is more important, however, is the impact these advances are having in enhancing the capabilities and productivity of the mobile worker. At the same time, these changes also represent challenges for the enterprise to effectively leverage these new capabilities while also protecting the information they store, process and transmit.

This article takes a look at some of the most prominent mobility trends, how they are impacting various workforces, and the manner in which they may be implemented within the departments of Defense (DoD) or Navy (DON) network environments.

Smarter Smartphones

Does anybody remember when a mobile phone was just a phone? As each new product release tries to outdo the previous ones, smartphones are literally getting smarter and smarter every day. While the Apple iPhone and Android-based devices have gotten most of the recent attention, BlackBerrys, Palm devices and others have all joined in the race to provide the coolest, most capable devices. These devices sport enhanced multimedia support, document handling capabilities and even video conferencing. In addition to the mind-boggling number of consumer applications available for these devices, and many are free, corporations are also developing their own custom apps to support their mobile workforce. With the promised roll out of dual-core processors for smartphones similar to PC processors, mobile devices will be even more capable of handling multimedia, and interactive and processing-intensive applications. With the exception of screen and keyboard size, the distinction between a smartphone and a full-size computer will soon be irrelevant from a technical standpoint.

Tablets

While tablet PCs have been around for a while, they have typically been designed around a laptop platform with a pen or touch-based interface added on. They tended to be heavy and difficult to use, and as a result, have not been very popular. The newly released iPad, or rumored to be soon released tablets (Research in Motion or RIM and Hewlett-Packard) represent devices designed from the ground up to be sleek, easy to use and capable. With larger screens and keyboards than smartphones, tablets are seen to be much more user-friendly for a number of uses including: document creation and editing; accessing and manipulating back-office corporate applications and data; graphics-intensive work; and multimedia applications. Using Voice over Internet Protocol (VoIP), tablets could also support voice communications, although that has not been a primary application offered to date.

BYOM

The numerous device and service options available today are obviously difficult to manage from an enterprise standpoint — so some corporations have decided not to even try. A growing trend is: bring your own mobility (BYOM), where employees can buy whatever personal device they like and are allowed to attach it to the corporate network, under certain conditions. Mr. Robert Carey, the former DON Chief Information Officer, spoke of this trend in an April 2010 interview with CIO Talk Radio, an Internet-based talk radio show aired globally through VoiceAmerica Business Radio. Most organizations realize that their employees often conduct business on their personal devices anyway, so BYOM is a formal acknowledgement of that and allows corporations to better manage that activity.

BYOM has some significant advantages. Employees will be happier using the device of their choice, and those who carry a business and a personal device can just carry one, making life a little easier. For the enterprise, the prospect of happier employees has obvious value, but the money saved by not buying devices has a monetary value more easily calculated.

Third Party Management Platforms

The majority of the new mobile devices were initially, and sometimes exclusively, designed for the consumer marketplace. This makes integrating them into an enterprise network problematic because the necessary control and management of the device required to enforce corporate policy and protect sensitive information are lacking. However, a number of software providers, independent from the device

manufacturer or service provider, have developed management platforms that provide the necessary management controls that enterprises rely on to protect their information, such as password enforcement, remotely wiping data from a lost or stolen device, and encrypting data. Some applications also permit devices to have two distinct profiles, so that corporate and personal data are never intermingled.

4G Networks

No matter how fast your sports car may be, it won't take you anywhere quickly if the roads you are driving on can't handle the speed. The same is true with your mobile device. Services, such as on-demand multimedia, video conferencing, wireless VoIP and real-time navigation, require a high degree of bandwidth availability, as well as low latency, in the round trip between end points. To support these devices and apps, all the major commercial cellular providers have established schedules for the roll out of their fourth-generation mobile or 4G services. In some areas, 4G service is available today. Whether based on the WiMax or Long Term Evolution (LTE) standards, these networks will provide throughput capabilities for smartphones of up to 100 megabits per second (Mbps), dramatically faster than the 3 Mbps speed of a 3G connection.

Enhanced Voice Encryption

Because smartphones are used to conduct an increasing amount of business by the mobile workforce, concern over securing voice conversations has risen. This concern has recently been highlighted by the breaking, and public posting of the encryption algorithm utilized by many providers that use the Global System for Mobile Communications (GSM), which is the most popular mobile telephony standard used by carriers in more than 200 countries, including the United States.

A number of solutions are currently on the marketplace to provide enhanced encryption for voice calls between similarly configured devices. Unfortunately, at this time, none of these solutions are interoperable with each other. A standards-based, interoperable solution, however, could be available in the future.

One Person, One Phone

Many consumers today eschew having a traditional, copper phone line installed at their residence and instead use their mobile phone for all voice needs regardless of their location. Due to advances in integrating cellular networks with traditional phone systems, such as Private Branch Exchanges (PBX) popular in the corporate setting, this trend is also now beginning to make advances with larger enterprises as well.

With only one voice mail application to tend to, using a mobile phone as your primary, or only, phone cuts down on phone tag and multiple, redundant messages. The enterprise can also save by not paying for redundant voice services and equipment.

DoD Implications

Taking advantage of these advances can empower the mobile workforce to a degree that was considered visionary only a year or two ago. Today, unfortunately, the stringent information assurance requirements of the DoD prevent their full adoption on military networks. However, as the corporate world focuses more on the security of mobile platforms, many of the concerns of those of us in the DoD environment are also being addressed by commercial providers. While some DoD requirements, such as Common Access Card support, may continue to call for unique, custom solutions, in general, the DON will increasingly be able to take advantage of these advancements. This will empower our Sailors, Marines, and those who support them, to better accomplish their missions. CHIPS

Mike Hernon is the former chief information officer for the city of Boston. He currently supports the DON CIO in telecommunications and wireless strategy and policy.

Changes and Challenges in Delivering Navy Total Force IT

Capt. Michael S. Murphy

A conversation with Sea Warrior Program Manager Capt. Michael Murphy

Navy Total Force strategy is reshaping how information technology is attained in the Navy… The Sea Warrior program (PMW 240) within the Program Executive Office for Enterprise Information Systems, Total Force's IT agent, provides structure, process, resource and acquisition support for key Chief of Naval Operations (OPNAV) manpower, personnel, training and education (MPTE) applications. In an interview, Sea Warrior's Program Manager Capt. Mike Murphy discussed lessons learned in the enterprise approach to Total Force IT solutions. Murphy was interviewed by the Sea Warrior public affairs staff in August.

Q: When was Sea Warrior established and how does the Navy benefit?

A: In 2006 the Chief of Naval Personnel requested that the Assistant Secretary of the Navy (Research, Development and Acquisition) appoint PEO EIS to lead affordable business IT delivery and incremental capabilities.

In September 2007 Sea Warrior began operating within PEO EIS with the mission to coordinate MPTE IT development, acquisition and life cycle maintenance under a single systems command and program office. This is important because MPTE businesses were merged to form the Navy's single manpower resource sponsor, called Navy Total Force.

The term 'Total Force' had long been used to describe the coordination of active and Reserve components and government service civilians. For MPTE to achieve the Total Force vision, multiple IT service providers needed to be better aligned. The resulting benefits are numerous.

First, the functional community no longer has to communicate requirements to multiple IT program offices. Prior to the enterprise model, IT service providers reacted to uncoordinated command requests for system changes. Today, a proactive governance model is evolving that prioritizes and approves changes, which we then bundle into a release. As a result, technology refresh is more systematic and predictable, which particularly benefits the fleet.

Second, software changes and engineering proposals are managed via systems engineering standards from the Department of Defense and Space and Naval Warfare Systems Command (SPAWAR), and changes are adjudicated via Functional Review Boards and Configuration Control Boards. We follow a standardized, rigorous systems engineering process for MPTE applications in which our stakeholders and the fleet actively participate.

Third, this process yielded a documented acquisition baseline of technical solutions, which anchors the process of budget planning and execution. It also fosters a single engineering focus to technical solutions.

Finally, organizing MPTE IT under an enterprise-level program office increased the visibility of duplicative system functions, data, interfaces, users supported, financials and other attributes. We completed a portfolio analysis of 66 MPTE systems which informs IT consolidation decisions.

Q: Would you explain some key aspects of your systems engineering approach?

A: Solid systems engineering employs rigorous, repeatable technical processes and testing. I can't emphasize enough the importance of thorough and progressive testing at all levels, afloat and ashore, and most importantly with end users at the operational level. It's been proven time and again — take testing shortcuts — and you'll face serious adverse consequences later.

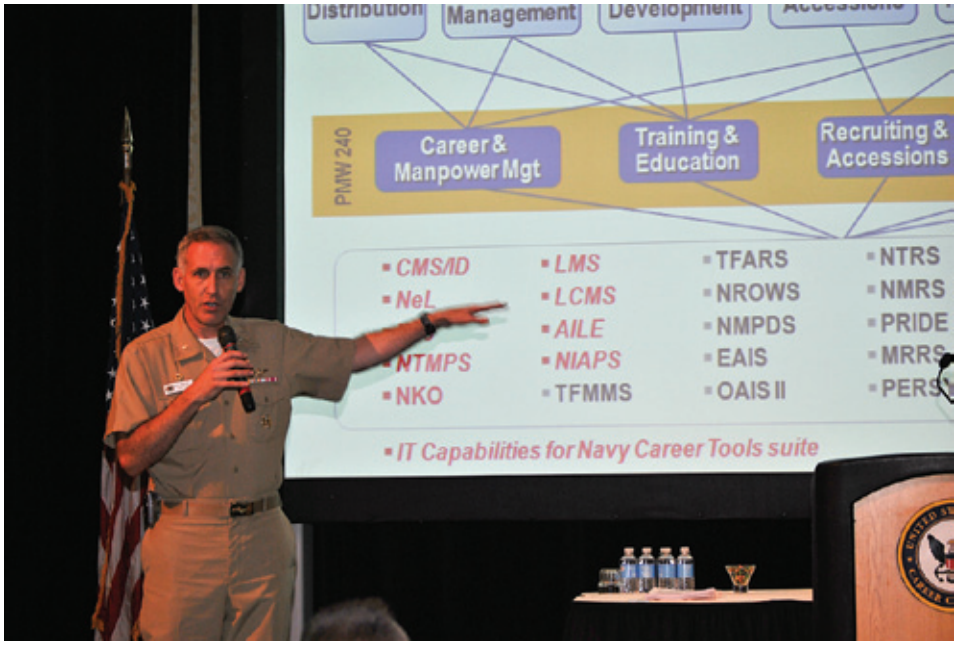
Many organizations have reported that rework costs range anywhere from 10 to 100 times [more than] the cost of doing it right the first time. Let me give you an example from my experience. Last June we delivered the IT capability for enlisted Sailors to negotiate their orders online using Career Management System/Interactive Detailing (CMS/ID). Testing confirmed this capability as operationally effective in the Internet environment, but revealed numerous technical and user interdependencies in the disconnected environment while ships are underway.

We learned the shipboard Navy Information Application Product Suite (NIAPS) environment wasn't designed to support the high data interchange rates needed by CMS/ID to perform a critical business process such as detailing. CMS/ID itself was proven effective; however, it needed the Internet to ensure full mission capability — so the decision was made not to deploy CMS/ID in the NIAPS suite.

Another key aspect of our systems engineering approach was to instantiate systematic application releases and technical reviews. The target is to release enhancements every six months. We are working to ensure every major release

"I can't emphasize enough the importance of thorough and progressive testing at all levels, afloat and ashore, and most importantly with end users at the operational level. It's been proven time and again — take testing shortcuts — and you'll face serious adverse consequences later."

– Sea Warrior Program Manager Capt. Mike Murphy



NORFOLK (June 28, 2010) Capt. Michael S. Murphy, program manager for Sea Warrior (PEO-EIS PMW 240), describes the Sea Warrior portfolio of Navy Career Tools to Navy counselors during the 22nd Navy Counselor Association symposium. U.S. Navy photo by Senior Chief Mass Communication Specialist Maria R. Escamilla.

has a system release plan based on the SPAWAR model that covers all impacted software components, constraints, risks, process steps, schedules, testing, logistics and other aspects. Regular technical reviews provide PEO EIS, as the Milestone Decision Authority, a documented and integrated baseline with respect to proceeding to the next phase of the IT project.

One more outcome worth mentioning — the standardized engineering process and six-month release target have a major impact, fiscally and operationally, but IT project directors are constantly balancing the right tension between maintaining a sense of urgency and allowing experts to follow the proven process. The technical team must allow sufficient time for operational testing and incorporating fleet feedback without slowing the next development cycle. That's no small task.

Q: One of the most pressing enterprise issues is getting decades-old systems to "talk to one another." Is there progress toward more integrated Navy human resources systems?

A: This is a very difficult problem to solve because systems were 'silo-architected' over the past several decades. The average age of our systems is 26 years. Reengineering these systems is a significant task mainly because data elements are embedded in the application code. This in turn spawned over 2,000 different crosswalks between systems, often with conflicting or latent data.

Let me illustrate the point using the DoD language code mandate. Defense human resources systems needed an expanded language field to accommodate service members' abilities to speak two to five different languages, including dialects, which affects member compensation. This seemingly simple code change to legacy systems involved 70 point-to-point interfaces, 100 different file transfers and 5,500 total hours of development effort. We must get to the place where applications and trusted data are maintained separately. That's when there will be true interoperability.

Enterprise data management is a strategic MPTE imperative, but a long-term undertaking when you consider that MPTE has hundreds of systems. The effort is progressing incrementally and involves data definition, consolidation, cleansing and standardization.

We're continuing to deliver near-term solutions as the enterprise data strategy evolves. For example, the Navy standardized the orders negotiation process on a single system. Sailors use CMS/ID to search and apply for jobs and manage their career progression. Detailers, com-

mands and career counselors use CMS/ID to understand Sailors' duty preferences, rank applicants, advise Sailors on choices and process orders.

A longer-term example is the Navy's Personalized Recruiting for Immediate and Delayed Enlistment (PRIDE) modernization. PRIDE uses a Web application to provide accessions information and processing through a service oriented architecture (SOA) environment. The application will become the Navy's only interface with the U.S. Military Entrance Processing Command's enterprise SOA, linking to the command's Integrated Resource System. USMEPCOM's Integrated Resource System is a joint service component system supporting the peacetime and mobilization mission of qualifying and enlisting applicants into the U.S. Armed Forces.

Part of this work involves prototyping an authoritative data environment that uses an operational data store approach. The PRIDE effort will replace legacy batch file transfers with interactive, Web service-based data exchanges — an important step toward interoperability.

Q: As you explained, supporting business IT in afloat and remote environments is an ongoing challenge. How is your program addressing this?

A: We oversee two business IT environments for units underway, NIAPS and Navy Standard Integrated Personnel System (NSIPS). Both allow use of various MPTE applications in a disconnected operational environment regardless of geographic location, thereby reducing reliance on the Internet. Delivering business IT afloat is a very complex undertaking involving over 45 hosted applications, hardware suites, integration, data replication, global fleet support, security, installation and other factors.

That's why one of the biggest benefits is a series of operational assessments of MPTE applications — systems deployed and used by fleet Sailors. These assessments are key to the testing I mentioned earlier, and they are very rigorous. Each assessment has an established purpose, objectives, data collection method and test criteria. Assessments typically take months to complete because they involve actual operational units and type commanders. We learn a lot from these assessments, which are summarized using COMOPTEVFOR reporting standards so everyone has a common context. Operational Test and Evaluation Force provides an independent, objective evaluation of operational effectiveness and suitability of naval systems in support of DoD and Navy acquisition and fleet introduction decisions. The assessments continue to guide how we address reliability and suitability gaps of MPTE applications afloat.

In a related area, we've more closely aligned the technical upgrades of afloat business IT systems with the Navy Modernization Process (NMP), formerly known as SHIPMAIN (Ship Maintenance). This is the enterprise-level process for surface ships, instituted by the Surface Warfare Enterprise and Naval Sea Systems Command, which helps identify the right maintenance and modernization effort and the right level of performance. We work within the NMP process, yet focus on accelerating software pushes to the fleet. We track the required documentation through the ship's technical assessments and NMP boards until the software update is authorized for shipboard installation.

Q: PMW 240 installed NIAPS on the first two Consolidated Afloat Networks and Enterprise Services early adopter ships. What were your findings?

A: CANES is part of the Navy's network convergence providing a single, highly scalable network infrastructure afloat. There are currently 10 early adopter CANES ships and all have NIAPS integrated into their environment. An important point, however, is that the same NIAPS version is used for both the early adopters and legacy ships. We do this by virtualizing NIAPS for the CANES blade server environment. This allows us to use a 'build it once, deploy it twice' approach, which reduces cost and maintains commonality across the fleet.

The early adopter program is a phased subsystem and integration testing process that's part of the complex transition from [the] Integrated Shipboard Network System (ISNS) to CANES. Testing allows us to identify and correct NIAPS integration issues in concert with software updates in the ISNS Increment 1 package. Plus, we're working out NIAPS CANES installation issues including prerequisites, computing resources, technical training, documentation and inevitable ship schedule conflicts.

"Buying business IT is significantly more complex for a global, networked Navy. Success depends on organizational collaboration. We're committed to improving integration and synchronization within PEO EIS, the SPAWAR team, the OPNAV codes and subordinate commands in advancing the MPTE shared accountability acquisition model."

Q: What are your top priorities over the next year and what results are you aiming for?

A: Buying business IT is significantly more complex for a global, networked Navy. Success depends on organizational collaboration. We're committed to improving integration and synchronization within PEO EIS, the SPAWAR team, the OPNAV codes and subordinate commands in advancing the MPTE shared accountability acquisition model. We need to implement enterprise IT governance and transition planning.

Second, as I mentioned earlier, moving from a systems-centric model to a data-centric model is paramount. The problem isn't simply technology, but the need for overarching data governance. To that end, we anticipate completion of a near-term goal to establish the authoritative data environment prototype as a test bed for automated data store processes and tool-

sets for the MPTE enterprise. The prototype will model the ability to share common information among users of Web Standardized Territory Evaluation and Analysis for Management (WebSTEAM), PRIDE and NSIPS.

In addition, the prototype results will guide future IT modernization efforts on the core data required by the DoD enterprise architecture supporting defense business enterprise priorities.

On a related front, we have an IT compliance and portfolio manager in place to help ensure the MPTE IT investment is managed collectively as capabilities rather than individual systems. The compliance effort lets us look across the various DON databases that contain system attribute and funding information to identify redundancies and opportunities for consolidation.

We continue to press forward with improvements to IT delivery afloat. Back in April, the OPNAV N16 Fleet Introduction Team hosted a pierside event for us to engage directly with the fleet, called 'A Day in the Life of Sailors.' It was both eye-opening and energizing. Thirty-one technical team members from Sea Warrior met with representatives from afloat units, Naval Surface Forces, Naval Air Forces, Personnel Support Detachment Afloat, Regional Medical Center and the Career Information Center. We came away with a renewed awareness of the challenges Sailors face using MPTE applications in the operational environment and recommitted ourselves to making their lives better. We'll be doing more end-user engagements going forward.

Finally, we now have a limited investment opportunity in the transformational efforts of a Future Personnel and Pay Solution, Enterprise Training Management and Delivery System and PRIDE modernization. These three major acquisitions are truly transformational because they will help consolidate functionality, establish authoritative data and lessen the administrative burden so Navy Total Force people can focus on their mission. And frankly, that change can't come soon enough. CHIPS

Follow PEO EIS on Facebook and Twitter.

The Consolidated Afloat Networks and Enterprise Services program is part of a larger effort by the Department of the Navy to establish the Naval Networking Environment 2016. CANES is the afloat piece of four components comprising this effort, along with the Next Generation Enterprise Network (NGEN), Base Level Information Infrastructure (BLII ONE-NET) and excepted networks not included in the NGEN enclave. CANES will deliver C4ISR capability as applications rather than complete systems, harvesting significant savings for the Navy while accelerating delivery of warfighting capability to the fleet.

SAN DIEGO (April 13, 2010) – Capt. Hank R. Reeves (center), Sea Warrior program (PEO EIS PMW 240) Integrated Learning Environment project director, meets with crew members aboard USS Stockdale (DDG 106) during a discussion led by Chief Navy Counselor (SW/AW) Beverly Smith (standing left), Stockdale's Command Career Counselor. The group is participating in "A Day in the Life of Sailors," an unprecedented event organized by Sea Warrior and the Chief of Naval Operations Fleet Introduction Team. The purpose of the event is for key Sea Warrior personnel to meet face-to-face with their fleet customers to better understand the challenges Sailors face when using Sea Warrior applications in the operational environment. Sailors voice their opinions on Navy Career Tools, such as the Career Management System/Interactive Detailing, Electronic Service Record, Navy e-Learning and others, to system developers and policy makers, who in turn ask Sailors for recommendations for improvement. The team recognizes that Sailor input is a highly valued and essential contribution to the overall design of the Navy's manpower, personnel, training and education information systems. U.S. Navy photo by Senior Chief Mass Communication Specialist Maria R. Escamilla.

About Capt. Mike Murphy

Capt. Michael S. Murphy is the program manager for Sea Warrior program (PMW 240), which is responsible for non-tactical IT operations and solutions that address MPTE capability gaps and legacy system sustainment. Sea Warrior is part of the Navy's Program Executive Office for Enterprise Information Systems (PEO EIS), which develops, acquires, and deploys seamless enterprise-wide IT systems with full life cycle support for the warfighter and business enterprise.

BUILDING THE USMC IT COMMUNITY THROUGH COMMUNITY WORKFORCE LEADERS

By Pete Gillis

Since its inception in 2001, the Marine Corps Information Technology Management (ITM) Community of Interest (COI) has been focused on the professional development of the Marine Corps IT workforce. As one of 20 functional civilian communities in the Marine Corps, the ITM COI's mission is to create a working environment to attract, retain and empower the best and brightest talent to support and develop a sustainable ITM civilian Marine workforce.

Early on, community leadership recognized that to achieve a consistent, motivated and highly skilled ITM workforce, there must be a support structure established across the Marine Corps. This support structure would be local, would understand local issues, and serve as a conduit for information within the community. Thus was born the ITM community representative system. Community representatives were established at a number of bases, posts and stations and these volunteers were active, engaged members of the community.

In 2008, we recognized that our community representative system needed a jump-start. Having no representation at several installations was detrimental to the community leadership's situational awareness. To revitalize the system, two key steps needed to occur. First, we communicated the value of having a community representative to local commanders. Second, at the recommendation of the existing representatives, we changed the "community representative" title to "community workforce leader" (CWL). Collectively, we felt this title better described the role we wanted these people to play.

In June of this year, the ITM COI held its annual CWL summit. In attendance were 21 of the 26 CWLs, and as part of a complete strategic planning workshop, we established a community steering committee made up of six CWLs. The community manager established short and long-term goals for the community and had discussions that formed the basis for a strategic plan. Additionally, the work conducted at the summit resulted in an amended community charter. Most importantly, the attendees discussed the philosophy of CWL characteristics. Significantly, they agreed that seniority isn't always a requirement. CWLs below the GS-13 level provide a unique perspective. The spirit of volunteerism was judged to be paramount since the community only advances at the will of its members. Many of our CWLs have been volunteers for more than five years. This provides a continuity of message that could not be duplicated with a rapid turnover of personnel.

As part of the goals identified at the summit, enhancing our CWL network by encouraging the use of both the community's SharePoint site and Jabber, the Defense Connect Online (DCO) chat client, was critical. The SharePoint site allows the CWLs to visit a single location and find documents, get information updates and collaborate on COI-wide issues. Further, a dedicated section of the steering committee facilitates the operations of that body. Jabber enables real-time, short-duration communications and is invaluable for getting answers to those "pop-up" questions that invariably occur. Almost half of our CWLs have Jabber accounts and have already conducted numerous ad hoc conferences.

In the future, our CWL infrastructure will mature and evolve. The strength of the community lies in its ability to advance IT-specific workforce issues, and CWLs will play a significant role in this regard. Information transparency will help our CWLs provide a wide range of resources to their constituents. Ad-hoc CWL working groups that volunteer to tackle community issues will draw on the expertise of the local IT workforce, thereby increasing involvement at the grass roots level. Barriers to information sharing will be eliminated as a problem at one installation finds its solution at another.

"Throughout the Marine Corps, the spirit we wish to foster in our CWLs is that of empowering and growing each and every community member," said Deputy Director, Command, Control, Communications and Computers (C4) Directorate, Headquarters Marine Corps and the Marine Corps ITM COI Community Leader Mr. Jim Craft. CWLs will be at the heart of this spirit.

At the end of the day, the whole purpose of the community is to support our ITM workforce and facilitate professional development opportunities. CWLs are critical to this effort, communicating key messages and advancing ideas. The community leadership recognizes that initiatives designed to move the community forward would be untenable without the valuable contributions these individuals provide. With this support, the Marine Corps ITM COI continues to evolve into an entity whose contributions are acknowledged Corps-wide. CHIPS

Pete Gillis is the community manager for the U.S. Marine Corps Information Technology Management Community of Interest. For more information, contact usmc_information_technology_community@usmc.mil.

Charting a Course for Information Assurance Policy

A one-stop shop website for all DoD IA policies and regulations

For the latest version and to gain the full features of the DoD IA Policy Chart, it is best viewed online with easy access via hyperlinks to essential information: http://iac.dtic.mil/iatac/ia_policychart.html

By John Dittmer

For years, one of the primary challenges for Information Assurance (IA) personnel in the Navy, as well as the rest of the Department of Defense, has been finding and determining which policies apply for building and maintaining their information systems. In building, operating and securing the DoD's Global Information Grid (GIG), a wide range of directives, instructions, manuals and other policies has been published. Unfortunately, the breadth and scope of these policies make locating the appropriate policy and obtaining the latest version of that policy difficult — until now.

One-stop Shop

To simplify the process for IA professionals, the Deputy Assistant Secretary of Defense (DASD) for Cyber, Identity and Information Assurance (CIIA) requested that the Defense-Wide Information Assurance Program (DIAP) develop a chart that pulls together all of the essential IA policies into a single document, known as the DoD IA Policy Chart, which is shown on the next two pages.

The chart is designed around the following four goals as described in the CIIA Strategy which can be found at: http://cio-nii.defense.gov/docs/DoD_IA_Strategic_Plan.pdf.

Goals include:

1. Organize for unity of purpose and speed of action (shortened to "Organize" in the chart);
2. Enable secure mission-driven access to information and services (shortened to "Enable" in the chart);
3. Anticipate and prevent successful attacks on data and networks (shortened to "Anticipate" in the chart); and
4. Prepare for and operate through cyber degradation or attack (shortened to "Prepare" in the chart).

These four goal areas are divided into activities that support each goal. In the lower half of the chart is a legend that identifies the originator of each policy by a color-coding scheme. There are boxes that provide the legal authority for the policies, the federal/national level of IA policies, as well as operational level documents that provide details on securing the GIG and its assets, that can be found on the left side of the IA Policy Chart. Embedded hyperlinks to all of the publicly accessible documents mean all of the policies are just a click away.

Most of the policies listed on the DoD IA Policy Chart are Defense Department policies, although some have federal government origins. The managers of the IA Policy Chart at the DIAP, and several other individuals involved in various aspects of IA policy in government, receive regular updates on all changes for DoD-level IA policies. The chart's policies and links are regularly updated to ensure the chart's currency.

Automatic Alerts

Users who want to ensure they keep up with these changes can take advantage of the chart's automatic alert feature. This allows a user to be alerted automatically whenever the chart changes. Additionally, red borders are used to highlight those policies that have changed most recently.

Reaction to the DoD IA Policy Chart has been quite favorable.

"The IA policy chart is a one-stop shop for high-level policy," said Andrew Shaw, IT policy lead in the Naval Surface Warfare Center, Corona Division, command information office. "It gives the average IA person a great tool to see how certain policy documents interact and support one another and makes it that much easier for our community to provide information assurance".

In addition, the links to the chart have been featured on many IT-related websites such as the Department of the Navy Chief Information Officer Policy and Guidance website: www.doncio.navy.mil/Policy.aspx.

Future Development

For the chart's future development, planners at the DIAP are considering several ideas. One near-term approach would be to link to other related policy charts as they are being developed, particularly at the service level. For example, a graduate student at the Naval Postgraduate School is developing a proposal for a similar policy chart for the Navy's IA policies. Other Defense Department components have also made inquiries about developing their own charts, and some international partners have discussed the possibility of charting their own IA policies.

Some are also looking at creating software applications so that these policies can be accessed by iPhones, BlackBerrys and other smart mobile devices. The smaller screen size would require the information to be presented in a modified mobile version.

The chart and background information can be accessed at: http://iac.dtic.mil/iatac/ia_policychart.html.

The page has a feedback feature for your comments or suggestions, which are always welcome. CHIPS

John Dittmer is a Certified Information Systems Security Professional (CISSP), Information Systems Security Management Professional (ISSMP) and Project Management Professional (PMP). He is an associate consultant for Booz Allen Hamilton and supports the Defense-Wide Information Assurance Program (DIAP). Dittmer is a retired Navy Reserve lieutenant commander who has worked on a variety of Navy and DoD IT projects.

BUILD AND OPERATE A TRUSTED GIG

CYBER, IDENTITY & INFORMATION ASSURANCE (CIIA) RELATED POLICIES & ISSUANCES

Developed by DASD (CIIA) | As of: 30 July 2010
Send Questions/Suggestions to *iatac@dtic.mil*

AUTHORITIES

- Clinger-Cohen Act, Pub. L. 104-106
- Federal Information Security Management Act 44 U.S.C. §3541 et seq
- Title 10 Armed Forces §§2224, 3013(b), 5013(b), 8013(b)
- Title 14 Cooperation with Other Agencies Ch 7:§§141, 144, 145, 148, 149, 150
- Title 32 National Guard §102
- Title 40 Public Buildings, Property, & Works Ch. 113: §§11302, 11315, 11331
- Title 44 Public Printing & Documents CH. 35: §§3541, 3504
- Title 50 War & National Defense §§401, 1801
- Unified Command Plan (UCP) US Constitution Art. II, Title 10 & 50

NATIONAL / FEDERAL

- A-130, Mgmt of Fed Info Resources, Appendix III, Security of Fed Automated Info Systems
- Computer Fraud & Abuse Act Title 18 (§1030)
- Federal Wiretap Act Title 18 (§2510 et seq)
- Foreign Intelligence Surveillance Act Title 50 (§1801 et seq)
- Pen Registers and Trap & Trace Devices Title 18 (§2701 et seq)
- Presidential Memo "Classified Information & Controlled Unclassified Information," 27 May 09
- Executive Order 13526 Classified National Security Info
- Executive Order 13231 Critical Infrastructure Protection in the Information Age
- NSPD 54 / HSPD 23 Computer Security & Monitoring
- NSD 42 Nat'l Policy for the Security of Nat'l Security Telecom & Info Systems
- National Security Strategy
- Federal Acquisition Regulation (FAR)
- Stored Communications Act Title 18 (§2701 et seq)
- National Strategy to Secure Cyberspace
- NSTISSI-4002 Classification Guide for COMSEC Info
- CNSSD-502 National Directive on Security of National Security Systems
- CNSSD-900 Governing Procedures of the Committee on National Security Systems
- CNSSD-901 Nat'l Security Telecom's & Info Sys Security (CNSS) Issuance System
- CNSSI-4009 National Information Assurance Glossary

OPERATIONAL

- Computer Network Directives (CTO, FRAGO, WARNORD)
- SD 527-01 DoD INFOCOM Systems Procedures
- SI 504-04 Readiness Reporting
- SI 507-01 NetOps Community of Interest (NCOI) Charter
- SI 701-01 NetOps Reporting
- STRATCOM CONPLAN 8039-08
- STRATCOM OPLANs

SUBORDINATE POLICY

- Component-level Policy (Directives, Instructions, Publications, Memoranda)
- DISA FSO Whitepapers
- Security Checklists
- Security Readiness Review Scripts (SRRs)
- Security Technical Implementation Guides (STIGs)
- Security Configuration Guidelines (SCGs)

CIIA GOAL 1: ORGANIZE

1.1 LEAD & GOVERN

- DoDD 8000.01 Management of DoD Information Enterprise
- DoDD 8500.01E Information Assurance (IA)
- National Defense Strategy (NDS)
- Guidance for Development of the Force (GDF) for 2010-2015
- DoDD 8500.2 Information Assurance Implementation
- DoD Cyber, Identity & Information Assurance Strategic Plan
- National Military Strategic Plan for the War on Terrorism
- National Military Strategy (NMS)
- ASD(NII) / DoD CIO G&PM 11-8450 / DoD GIG Computing
- Quadrennial Defense Review (QDR) Report
- National Military Strategy for Cyberspace Operations (NMS-CO)

1.2 DESIGN FOR THE FIGHT

- Common Criteria Evaluation & Validation Scheme (CCEVS)
- NSTISSP-11 National Information Assurance Acquisition Policy
- DFARS Subpart 208.74, Enterprise Software Agreements
- DoDD 4630.05 Interoperability & Support of IT & National Security Systems (NSS)
- DoDD 8115.01 IT Portfolio Management
- DoDI 8115.02 IT Portfolio Management Implementation
- DoDI 8115.01 DoD IA Certification & Accreditation Process (DIACAP)
- DIACAP Knowledge Service
- DoDI 8115.01 Information Assurance (IA) in the Defense Acquisition System
- Alignment Framework for the GIG IA Architecture (AFG) v1.1
- IA Component of the GIG Integrated Architecture v1.1
- DNI CIO Memo Intelligence Community (IC) Enterprise Software Licensing
- DoDD 5000.01 The Defense Acquisition System
- DoDI 5000.02 Operation of the Defense Acquisition System
- DoDI 7000.14 Financial Management Policy & Procedures (PPBE)
- DoDD 7045.20 Capacity Portfolio Management
- ASD(NII) / DoD CIO Memo DoD Support for the SmartBUY Initiative
- DoD CIO G&PM 12-8430 Acquiring Commercial Software
- CJCSI 317.01G Joint Capabilities Integration & Development System (JCIDS)
- CJCSI 6212.01E Interoperability & Supportability of IT & National Security Systems

1.3 DEVELOP THE WORKFORCE

- NSTISSD-501 National Training Program for INFOSEC Professionals
- NSTISSI-4000 COMSEC Equipment Maintenance & Maintenance Training
- NSTISSI-4011 National Training Standard for INFOSEC Professionals
- NSTISSI-4015 National Training Standard for System Certifiers
- CNSSD-500 Information Assurance (IA) Education, Training & Awareness
- CNSSI-4012 National IA Training Standard for Senior Systems Managers
- CNSSI-4013 National IA Training Standard for System Administrators (SA)
- CNSSI-4014 National IA Training Standard for Information Systems Security Officers
- CNSSI-4016 National IA Training Standard for Risk Analysts
- DoDD 8570.01 IA Training, Certification & Workforce Management
- DoD 8570.01-M Information Assurance Workforce Improvement Program
- DTM-09-026 Responsible & Effective Use of Internet-based Capabilities

1.4 PARTNER FOR STRENGTH

- SP 800-37 R1 Guide for Applying the Risk Mgmt Framework to Fed. Info. Systems
- SP 800-53 R3 Recommended Security Controls for Federal Information Systems
- SP 800-53A Guide for Assessing the Security Controls in Fed. Info. Systems
- NSTISSI-1000 National Information Assurance C&A Process (NIACAP)
- CNSSI-1253 Security Categorization & Control Selection for Na'l Security Systems
- CNSSI-4007 Communications Security (COMSEC) Utility Program
- CNSSI-4008 Program for the Mgt & Use of Nat'l Reserve IA Security Equipment
- CNSSP-14 National Policy Governing the Release of IA Products / Services....
- DoDI 5205.13 Defense Industrial Base Cyber Security/IA Activities
- ICD 503 IT Systems Security Risk Management and C&A

CIIA GOAL 2: ENAB

2.1 SECURE DATA IN TRAN

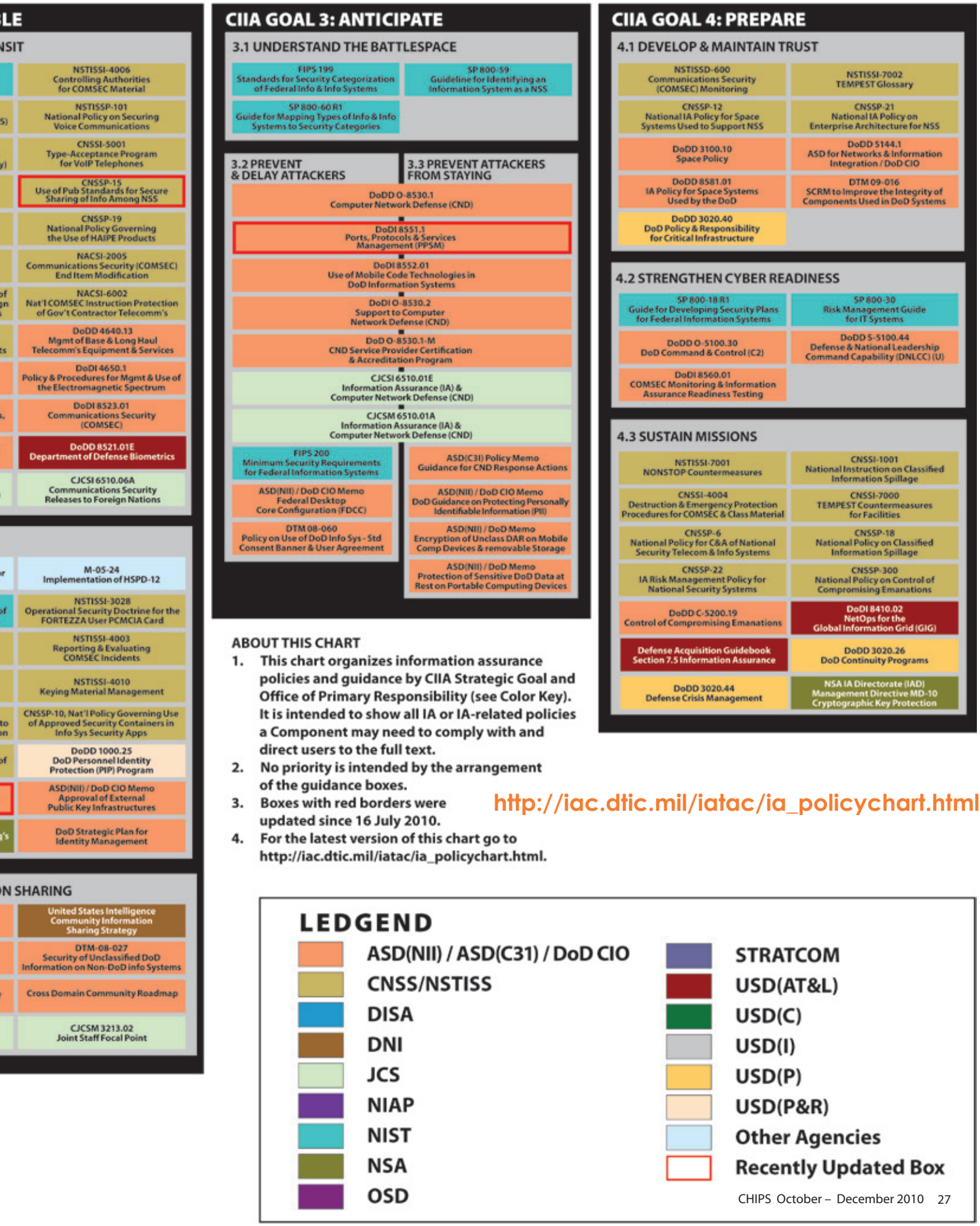
- FIPS 140-2 Security Requirements for Cryptographic Modules
- NSTISSI-7003 Protective Distribution Systems (PD
- CNSSI-5000 Guidelines for Voice Over Internet Protocol (VoIP Computer Technolog
- CNSSP-1 National policy for Safeguarding & Control of COMSEC Materials
- CNSSP-17 National Information Assurance Policy on Wireless Capabilities
- CNSSP-25 National Policy for PKI in National Security Systems
- NACSI-2006, Foreign Military Sales COMSEC Articles & Services to Foreig Governments & International Orgs
- NCSC-5, Nat'l policy on Use of Cryptomaterial by Activities Operating in High Risk Environmen
- DoDD 8100.02 Commercial WLAN Devices, Systems & Technologies
- DoDI 8420.01 Use of Commercial Wireless Device Services & tech in the DoD GIG
- DoDI S-5200.16 Objectives & MinStds for COMSEC Measures Used in NC2 Comms
- CJCSI 6510.02C Cryptographic Modernization Plan

2.2 MANAGE ACCESS

- HSPD-12 Policy for a Common ID Standard fo Federal Employees & Contractors
- FIPS 201-1 Personal Identity Verification (PIV) Federal Employees & Contractors
- NSTISSI-4001 Controlled Cryptographic Items
- NSTISSI-4005 Safeguarding COMSEC Facilities & Materials
- CNSSP-3 National Policy for Granting Access Classified Cryptographic Informatio
- CNSSP-16 National Policy for the Destruction COMSEC Paper Materials
- DODI 8520.2 Public Key Infrastructure (PKI) & Public Key (PK) Enabling
- NSA/CSS Policy 3-9 Crypto Modernization Initiative Re for Type 1 Classified Products

2.3 ASSURE INFORMATIO

- DoDD 8320.2 Data-Sharing in a Net-Centric Department of Defense
- ASD(NII) / DoD CIO Memo Use of Peer-to-Peer File Sharing Applications Across the DoD
- DoD Information Sharing Strategy
- CJCSI 6211.02C Defense Information System Network Policy & Responsibility



ABOUT THIS CHART

1. This chart organizes information assurance policies and guidance by CIIA Strategic Goal and Office of Primary Responsibility (see Color Key). It is intended to show all IA or IA-related policies a Component may need to comply with and direct users to the full text.
2. No priority is intended by the arrangement of the guidance boxes.
3. Boxes with red borders were updated since 16 July 2010.
4. For the latest version of this chart go to http://iac.dtic.mil/iatac/ia_policychart.html.

http://iac.dtic.mil/iatac/ia_policychart.html

LEDGEND

- ASD(NII) / ASD(C31) / DoD CIO
- CNSS/NSTISS
- DISA
- DNI
- JCS
- NIAP
- NIST
- NSA
- OSD
- STRATCOM
- USD(AT&L)
- USD(C)
- USD(I)
- USD(P)
- USD(P&R)
- Other Agencies
- Recently Updated Box

Tracking the Marine Corps Information Assurance Military Workforce

The Marine Corps Information Assurance Workforce (IAWF) is critical to providing the operating forces and supporting establishment with secure, reliable networks that enable command and control. To do this, the IAWF must be identified, properly trained and appropriately certified. The Headquarters Marine Corps Command, Control, Communications, and Computers (C4) Information Assurance (IA) Division, in compliance with federal law and the Department of Defense (DoD) IA Workforce Improvement Program, instituted an electronic tracking program (https://hqdod.hqmc.usmc.mil/IAWF.asp) to ensure the Marine Corps can identify IA professionals, provide training venues and meet mandated certification requirements.

The Marine Corps IAWF currently consists of more than 5,000 personnel who must be trained and certified according to the work tasks and functions they execute. Information assurance managers (IAM) and information assurance officers (IAO) have documented personnel that have "significant" IA responsibilities as part of the IAWF. IAWF personnel hold positions on IA or certification and accreditation (C&A) teams, and network operations, computer network defense, engineering or other positions requiring privileged access to Marine Corps networks. The HQMC C4 IA Division released an August 2010 HQMC C4 IAWF Review analyzing the IAWF posture of the total force and accentuating compliance with DoD Manual 8570.01-M, Information Assurance Workforce Improvement Program, and Secretary of the Navy Manual 5239.2-M, IA Workforce Management.

IAWF IDENTIFICATION

One of the significant challenges in identifying the IAWF is affiliating IA competencies to military billets or positions without tying them to a particular military occupational specialty (MOS). While most of the military population in the IAWF consists of the 06XX (Communications) community, several other military occupational specialties were reviewed as the IAWF was identified (Figure 1). With the proliferation of networks and computer systems and the increasing reliance on Internet-based applications, the IAWF and MOSs will need to be continually reassessed to ensure those Marines with privileged or administrative responsibilities are identified. This identification will allow the Marine Corps to design training curriculums specifically designed to meet the IAWF's requirements.

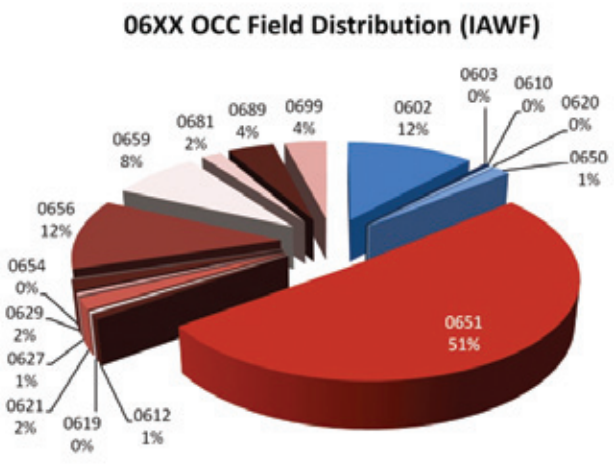


Figure 1.

The majority of the IAWF consists of MOSs in the 06XX occupational field; however, not all personnel with a 06XX designation will be identified as part of the IAWF. This is due to the level of designated privileged or administrative responsibilities which is evident with the Field Radio Operator MOS (0621) with 6.15 percent identified as part of the IAWF, whereas 61.12 percent of the total force Data Network Specialist, MOS (0651), have been identified. The graphs below show the distribution of the 06XX occupational field for the total force (Figure 2) and reported as the IAWF (Figure 3). Shades of red show the enlisted MOSs while shades of blue show officer MOSs.

Other MOSs, in addition to the 0600 community, recognize the integral piece the IAWF plays in their operational success. The Marine Air Command and Control Operational Advisory Group released a message discussing recommendations for the establishment of the IAWF in the 59XX MOS (Command and Control Elec-

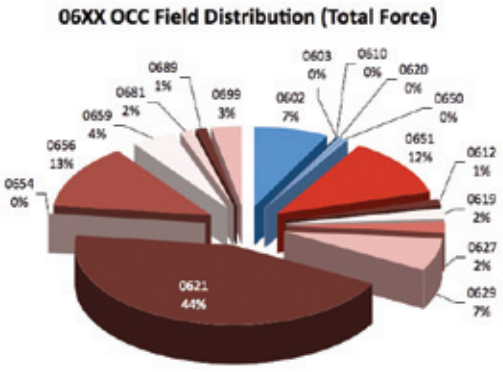


Figure 2.

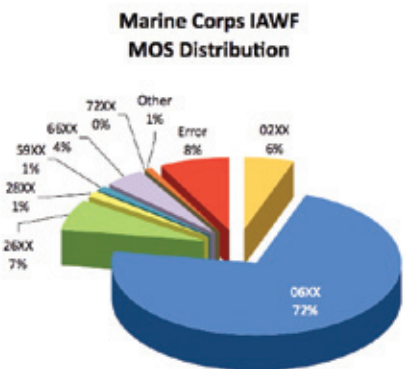


Figure 3.

*0%>1%

The Marine Corps Information Assurance Workforce currently consists of more than 5,000 personnel who must be trained and certified according to the work tasks and functions they execute.

tronics Maintenance). The executive steering committee's decision concurs with the addition of 59XX MOS codes to the IAWF using the top-down approach and tasks wing commanders to identify all 59XX billets with the Marine Air Control Group for proper training and certification. The 6694 occupation field sponsor had also ensured the Aviation Logistics Information Management and Support (ALIMS) MOS for inclusion, which currently makes up 4 percent of the total reported IAWF.

IAWF TRAINING AND CERTIFICATION

For the military IAWF population, the strain of demanding deployment schedules and maintaining operational tempo, coupled with a young workforce and personnel turnover, impacts IAWF training efforts. Additionally, newly trained personnel may not qualify for certification status (normally a minimum of two years experience is required), making it difficult to satisfy DoD Directive 8570.01 requirements.

The Department of the Navy Cybersecurity/Information Assurance Workforce Management, Oversight, and Compliance Council reviews these issues and considers unique operational requirements that may prevent commercial certification compliance. Local commanders have the responsibility to meet training mandates for this population. Training opportunities are widely available for the IAWF.

The HQMC C4 IA Training website (https://hqdod.hqmc.usmc.mil/IA/Pages/Training.asp) contains information on courses pertaining to IA baseline certifications, operating system/computing environment (OS/CE) certifications and additional IA-related training requirements. Marine Corps Communication Training Centers provide classroom and on-site instructor-led training requirements and certification vouchers for military personnel throughout various combatant commands worldwide. Self-paced distance education opportunities include immersive learning technologies at Carnegie Mellon University's Software Engineering Institute in coordination with the Defense Information Systems Agency and Department of Homeland Security (https://www.vte.cert.org/vteweb), with 450 training demonstrations, a resource library, more than 600 IA training videos, approximately 100 hands-on virtual IA training labs, and SkillSoft e-Learning classes available through MarineNet (https://www.marinenet.usmc.mil).

The Marine Corps official distance learning environment provides more than 3,000 courses and content covering CompTIA's A+, Network+ and Security+, International Information Systems Security Certification Consortium, Inc.'s (ISC)2 Certified Information Systems Security Professional (CISSP), EC Council's Certified Ethical Hacker, Information Systems Audit and Control Association's (ISACA) Certified Information Security Manager, and many other OS/CE vendor certifications through Microsoft, Cisco, Oracle, Sun and Linux.

The HQMC C4 IA Division serves as the functional area manager under the Information Systems Management category for the Inspector General of the Marine Corps. IAWF management and compliance is inspected based on the Automated Inspection Reporting System Checklist 405, Information Systems Management, and is conducted by command inspection programs and unit inspection programs, supporting Secretary of the Navy Instruction 5239.20, Enclosure 2, paragraph 2.e. Additional references and supplemental information supporting inspections and assessment programs can be found on the HQMC C4 IA Inspections and Assessments page at https://hqdod.hqmc.usmc.mil/IA/Pages/Inspections.asp.

CONCLUSION

Overall, the Marine Corps approach to identifying, training and certifying its IAWF has generated positive responses from IA personnel throughout the Marine Corps. As the IA Workforce Improvement Program matures, the Marine Corps' IAWF will enter a lifelong learning path focused on securing and maintaining the security of IT assets, and we can also look forward to additional, enhanced cybersecurity training.

The Marine Corps recognizes the critical role of our Information Assurance Workforce in supporting the warfighter and is investing in the IAWF to make it capable of meeting the Corps' needs. CHIPS

Gunnery Sgt. John Paramadilok is the HQMC C4 IA Division information assurance manager. He holds the following certifications: Cisco Certified Network Professional (CCNP), Certified Information System Security Professional (CISSP), Cisco Certified Security Professional (CCSP) and Information Technology Infrastructure Library (ITIL). He can be contacted at iawf@usmc.mil.

Navy Plans Ahead for New Internet Protocol Version

As the pioneering organization under the DoD, SPAWAR Pacific has tested and deployed IPv6 in parallel compatibility with IPv4 for nearly 10 years without sacrificing the old for the new protocol

By Mass Communication Specialist 1st Class (SW/AW) Derrick M. Ingle

Space and Naval Warfare Systems Center (SPAWAR) Pacific's gradual implementation of a new and larger Internet Protocol Version 6 (IPv6) is already well underway for the future of the fleet as explained during a media roundtable at the Pentagon in Washington, D.C., Aug. 4.

The Internet is running out of IP addresses, and the current IP Version 4 (IPv4), which has served as the underlying communication foundation for the Internet for more than 30 years, is now on the brink of foreseeable address exhaustion as early as in the next two years.

"IPv6 was standardized in the 1990s after the realization that we were going to run out of addresses using the old protocol format," said Ronald L. Broersma, SPAWAR network security manager and chief engineer for the Defense Research and Engineering Network. "The Internet will run out of IPv4 addresses by 2012. The massive transition to this new protocol requires changes to the entire global Internet and everything that uses it from the underlying infrastructure right down to your home computer and router.

"At SPAWAR, we're qualified to do this because we directly support the warfighter and understand the priorities of the Chief of Naval Operations for the fleet of the future which will require advanced communications. We're proactive and recognize that need early by having the experience and technology ready," Broersma said.

As the pioneering organization under the Defense Department, SPAWAR Pacific has tested and deployed IPv6 in parallel compatibility with IPv4 for nearly 10 years without sacrificing the old for the new protocol.

"We were a part of [the] DoD IPv6 pilot effort, which started back in 2003, yet we've been using the new protocol well before then," Broersma said. "We've gained valuable operational experience and have shared our lessons learned with DoD, especially the Navy as they [Sailors] go to more advanced networks in the fleet. The experience we've gained and the problems we've already solved are going to save us years down the road as the rest of DoD starts deploying this [IPv6]. Our focus is also [on] coalition partners since Europe and other parts of the world are switching to the new protocol."

SAN DIEGO (June 24, 2010) An aerial view of the Space and Naval Warfare Systems Command (SPAWAR) Headquarters in San Diego. SPAWAR is responsible for serving as the Navy's technical lead for command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR), providing hardware and software to connect Sailors at sea, on land and in the air.

From better security to increased address availability, the Navy's proactive implementation of IPv6 promises to be a wise payoff despite those still awaiting a crisis or incentive to make the switch.

"The transition to IPv6 is a massive complex effort requiring everyone's participation and cooperation with no true near-term incentive. You aren't going to suddenly be able to access new websites you couldn't access before, yet in terms of security, you can now make your IPv6 address private so that it changes daily making it harder for people to track you, which adds to the inability to map the network," Broersma said.

"Although this is a massive effort, this hasn't required any additional funding or any additional personnel. This is a model for how others can succeed as well, if they plan and start early," Broersma added.

SPAWAR is a trusted leader in this forthcoming conversion as the San Diego-based command was recently recognized as the first to reach 100 percent success in an international IPv6 survey.

Broersma has been an engineer for the Navy since 1976 receiving the Meritorious Civilian Service and Superior Civilian Service Awards. In 2010, Broersma was awarded the San Diego Business Journal's Lifetime Achievement Award for his contribution to information systems for more than 30 years. CHIPS

Edited and reprinted from Navy News Service. For more news from the Space and Naval Warfare Systems Command, visit www.navy.mil/local/spawar/.

"THE FUTURE IS NOW" NAVY REVAMPS IT TRAINING PIPELINE

By Chris Kelsall

While a large amount of money is being spent on new technologies to operate and secure the Department of the Navy's (DON) networks, it is the people with the right knowledge, skills and abilities to implement those technologies who will determine success. Enormous challenges confront the DON Cyber/Information Technology (IT) Workforce. Moreover, those who train Sailors and prepare them to meet their operational commitments must work diligently to keep training content cutting-edge and relevant.

After thorough review of the Navy's rapidly changing cybersecurity and network operations role, a new program called "IT of the Future" (IToF) was developed. This program revamps the Information Systems Technician (IT) rating to be an advanced technical field (ATF). The ATF allows the Navy to recruit initial accession Sailors to both four-year and six-year obligations. Forty-nine percent of the new Sailors will be recruited for a four-year obligation, get their basic training in "A" School (basic skills training), and then go to their first permanent change of station (PCS). Fifty-one percent will be recruited for a six-year obligation and receive advanced training in a "C" School (advanced skills training) before transferring to their first PCS. The separate curriculums, supporting IToF, have been approved and are currently in pilot at the Navy's Center for Information Dominance (CID) from July 2010 through April 2011.

The Information Systems Technician "A" School is in the middle of the first pilot program which will change "A" School from an 11-week course to a 19-week course, and in January 2011, the updated curriculum will be presented. Recently, senior workforce managers from the Department of Defense, Department of the Navy and Navy Cyber Forces Command (NAVCYBERFOR) visited the CID to assess the pilot and the progress of the course. There are 20 Sailors participating in the CID "A" curriculum pilot, and it is meeting all expectations. Sailors enrolled in "A" School will graduate with CompTIA A+ and Microsoft Certified Professional XP certifications. All 20 Sailors are maintaining more than an 80 percent average and all have passed the A+ exam on the first try. Sailors who finish the new "A" School will receive Navy Enlisted Classification (NEC) 2790.

Thirty-five percent of the new accession Sailors will go right into "C" School and receive the new System Administration (SYSADMIN) NEC 2791. This training path includes additional certifications for Security + and additional Microsoft training. The new "C" School training will begin its pilot in January 2011. The remaining 16 percent will receive additional training from the new Journeyman Communications Course, which will come into effect at CID in 2012.

Fleet IT Sailors will have the opportunity to gain these new NECs with additional training which will be announced once the new training is fully in place. The Information System Administrator NECs 0000 and 2735 will be phased out in March and June 2011 respectively. Sailors will be required to hold NEC 2790 before acquiring the NEC 2791. Advanced IT training will be presented in courses that support improving the skills of Sailors in NECs 2710, 2720, 2730, 2779, 2780 and 2781.

All NEC 27xx series Sailors who hold privileged access to servers, routers and switches are required to have appropriate IA and operating system certifications in accordance with DoD 8570.01-M, IA Workforce Improvement Program. Therefore, current fleet and shore IT Sailors must attain commercial certifications as part of their daily training regimen and Personnel Qualification Standards. Once the certifications are gained, Sailors will apply to change their NEC. The Sailors can complete the required courses via immersive learning technologies at Carnegie Mellon University's Software Engineering Institute in coordination with Defense Information Systems Agency and the Department of Homeland Security (https://www.vte.cert.org/vteweb), and SkillSoft e-learning classes available through https://navy-iacertprep.skillport.com, or via classroom courses sponsored by NAVCYBERFOR in fleet concentration areas. Certification exams for all IT Sailors will be paid for via the Credentials Program Office supported by Navy Credentialing Opportunities OnLine (COOL) at https://www.cool.navy.mil.

Information regarding transition to the new NEC structure is updated on the NAVCYBERFOR IAWF website at: https://www.portal.navy.mil/cyberfor/IAWF/default.aspx. CHIPS

NAVY ENLISTED CLASSIFICATION (NECS) 27XX SERIES

2710:	Global & Command Control System–Maritime 4.X (GCCS-M 4.X) System Administrator
2720:	GSSC-M System Administrator
2730:	Naval Tactical Command Support System (NTCSS) II Manager
2779:	Information Systems Security Manager
2780:	Network Security Vulnerability Technician
2781:	Advanced Network Analyst
2790:	Information Systems Technician (IAT I)
2791:	Information Systems Administrator (IAT II)

By Stephen Ward and Thomas Kidd

International SPECTRUM Engagement

The Department of the Navy's (DON) engagement in the United States spectrum regulatory environment has been discussed in previous articles. However, the DON has many facilities and operations that are not under the umbrella of domestic regulation. The complexity of acquiring spectrum access for these situations increases and is often multiplied when Navy and Marine Corps operations are located within, or even transiting, foreign nations. As a result, the DON is globally engaged with various multinational organizations to accommodate the international presence of our naval forces and to nurture the availability of spectrum resources.

Internationally, many organizations impact spectrum availability. Some are obvious, such as the United Nations International Telecommunications Union (ITU) Radiocommunications Sector (ITU-R), while others may not be as apparent, but they are still critical to DON spectrum access. To better acquaint CHIPS readers with the DON Chief Information Officer's (CIO) sphere of engagement, a list of several of the organizations in which the DON actively participates and contributes to enhance access to spectrum follows.

Combatant Commands

A July 2008 CHIPS article titled "Military Coalition Frequency Management" (available at www.chips.navy.mil/archives/08_jul/web_pages/coalition_frequency.html) offered some background on the environment in U.S. European Command and the DON's coordination with the North Atlantic Treaty Organization (NATO) members. While the combatant commands have similarities, their policies, guidance and procedures for spectrum usage vary significantly due to differences in area of responsibility. Each combatant command has a structure to act as an emissary to sovereign nations in its area of responsibility to synchronize spectrum access.

Spectrum planning for naval operations in multiple geographic areas in a single deployment is a challenge. Operational engagement with the geographic combatant commanders is invaluable in managing these challenges.

Multinational Military Organizations

North Atlantic Treaty Organization

Perhaps the most recognized multinational body in the Western world is NATO. North Atlantic Treaty Organization nations and partner countries cooperate through NATO's Frequency Management SubCommittee (FMSC) to establish overarching policy for parts of the radio frequency spectrum used by the military.

One particular responsibility of the NATO Frequency Management SubCommittee is establishing policy for the military management of the ultra high frequency band between 225 and 400 megahertz, widely used for military aircraft, naval and satellite communications.

Combined Communications -Electronics Board

The Combined Communications-Electronics Board (CCEB) is a five-nation (Australia, Canada, New Zealand, the United Kingdom and the United States) joint military communications-electronics organization whose mission is the coordination of military communications-electronics matters among its member nations.

Thomas Kidd
Mr. Kidd is the director of strategic spectrum policy for the Department of the Navy. For more information contact Mr. Kidd at DONSpectrumTeam@navy.mil.

Stephen Ward
Mr. Ward supports the Department of the Navy as a senior adviser at various international regulatory and standards organizations.

The CCEB routinely develops strategic plans that provide the roadmap to achieve future interoperability. Following the establishment of the CCEB, discussion and a vision to deliver battle-winning maritime command, control, communications and computer (C4) interoperability led to an effort to align naval communications policies and prevent any barriers to interoperability with the imminent introduction of sophisticated new communications equipment. The DON is involved in the CCEB to support continued coalition interoperability at sea.

Regional Bodies

Gulf Cooperation Council

The Gulf Cooperation Council (GCC) was established in 1981 between Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the United Arab Emirates as a regional common market and defense planning council. The geographic proximity of these countries and their adoption of free trade economic policies are factors that encouraged them to establish the GCC.

In 1991, multilateral security commitments between the United Kingdom, the United States and Kuwait created a liaison relationship to the GCC. The extensive presence of United States Navy resources in the Persian Gulf necessitates that the DON support careful and continual coordination.

European Conference of Postal and Telecommunications Administrations (CEPT)

CEPT is acknowledged by the ITU-R as a composite representative of many European administrations. Bodies like CEPT are given special recognition and negotiation status during major ITU radio regulation conferences. While there is some CEPT membership overlap with NATO, not all CEPT members are NATO partners. The DON works as an adviser to many of the CEPT groups, developing regulatory proposals. Such proactive efforts attempt to mitigate serious disagreement at the final stages of radio regulation modification.

Organization of American States (OAS)

Similar to CEPT, the Organization of American States is a regional body with members from North, Central and South America. The OAS is represented at the ITU-R by its Inter-American Telecommunication Commission Permanent Consultative Committee for Radiocommunications and Broadcasting. The DON works closely with the OAS Inter-American Telecommunication Commission during preparatory meetings to resolve spectrum issues and to develop strategies and Inter-American proposals to formally liaise with other regions and introduce issues or proposals at ITU radio regulations conferences.

Technical and Standards Bodies

Spectrum-dependent technology can be leveraged for DON requirements or become a strident competitor for spectrum resources. The standards by which the systems operate are as critical to the DON as the international rules and regulations governing their use. The DON CIO maintains an active engagement in international standards bodies to manage the creation of specification standards that set the foundation for global technological evolution.

Institute of Electrical and Electronics Engineers (IEEE)

Long recognized as an active body that introduces various communication and computer-related concepts, the Institute of Electrical and Electronics Engineers is an avenue for the DON to influence early decisions on technology trends. A familiar wireless networking standard, 802.11, is an example of an IEEE standard. Areas such as the implementation of software defined radio and cognitive radio systems are immediate examples of recent DON influence and success.

International Organization for Standardization (ISO)

The ISO is an independent group that encourages harmonization of best practice concepts from all regions and nations. Specifically, the global intermodal (ship, rail, truck and air) transfer of goods, which impacts the safety of U.S. harbors and airports, is a high priority interest. The DON CIO serves as an advocate for the adoption of standards that the ITU-R can support with spectrum allocations, and the International Maritime Organization can merge into its policies and procedures.

This is just a few of the international governance bodies in which the DON CIO engages to assure international treaties, standards, processes and regulations are favorable to naval operations while supporting the global electromagnetic environment. The DON CIO is a dynamic leader and trusted partner in various spectrum-related policy and strategy groups. The ability to deliver U.S. naval forces spectrum today and in the future is critically dependent upon these ongoing engagement efforts. CHIPS

For more information about where the DON is engaged in support of Navy and Marine Corps operations, contact the DON Electromagnetic Spectrum Team at DONSpectrumTeam@navy.mil.

Spectrum Isn't Like "Other Natural Resources"

By Thomas Kidd and Mark Rossow

For the past 30 years the use of radio frequencies has dramatically increased. Radio has enabled the unprecedented growth of technology from cellular telephone to high speed wireless Internet. These and other capabilities we take for granted can only exist with the use of radio frequencies from the electromagnetic spectrum. However, a direct consequence from three decades of increased spectrum use is that spectrum availability, in many areas of the world, has declined to the point that spectrum is considered to be in short supply. The electromagnetic spectrum is generally regarded as a natural resource of the nation where it is used.

Spectrum has often been referred to as the "fuel" for wireless technology and the "oxygen" of the Internet. Spectrum differs greatly from natural resources, such as coal, land, water and air, because these resources are finite commodities; there is a limited amount of water, air, coal and land. Because they are finite resources, renewing them is either impossible or incredibly difficult. But the electromagnetic spectrum is not a finite commodity; it cannot be exhausted, and most importantly, the electromagnetic spectrum is instantly renewable. The moment that a radio, radar or some other spectrum-enabled device stops using a radio frequency, that radio frequency becomes instantly reusable by some other device. This simple, yet remarkable, difference means that efforts to manage and conserve the electromagnetic spectrum as if it were a natural resource, like water and land, are often misguided or ill-conceived. A resource that is instantly renewable cannot really be in short supply. As such, spectrum conservation is a misnomer.

The radio frequency spectrum includes all frequencies between 3 kilohertz (kHz) and 300 gigahertz (GHz). Except for the radio frequencies someone else is operating on at that precise moment, the entire electromagnetic spectrum is available for use 24/7. Curtailing or minimizing the use of spectrum to conserve it for future use may make conservation-minded people feel better, but it provides no preservation benefits whatsoever. Unlike natural resources that cannot be instantaneously recycled, spectrum is not physical; it cannot be saved for later use. The electromagnetic spectrum should be considered as an abstract resource.

Time is another abstract resource which cannot be stored and conserved. If time is not put to good use every moment, time is wasted. The same is true of the electromagnetic spectrum. Whenever spectrum is not used, it is a lost opportunity.

The U.S. radio frequency spectrum is allocated among federal and non-federal services, and use is governed by different organizations. The International Telecommunication Union, an agency of the United Nations, regulates information and communication technology issues. For nearly 145 years, the ITU has coordinated the shared global use of the radio spectrum, promoted international cooperation in assigning satellite orbits, worked to improve telecommunication infrastructure in the developing world and established worldwide standards. International spectrum governance involves the allocation of radio frequency bands for specific purposes and assigns radio frequencies for individual, commercial and government use.

This allocation and assignment strategy was conceived a century ago. Regrettably, this allocation and assignment policy restricts the efficient use of spectrum by limiting the use of a given radio frequency to a specific person, organization and/or purpose. Because the use is restricted, most radio frequencies are not used anywhere close to their full operational potential. Policy can be changed and with a new understanding of spectrum as an abstract resource, there is hope for future governance that permits the use of unused radio frequencies.

Understanding that spectrum is instantly renewable, that it can't be stored, and is being wasted every moment it is not used, the Department of the Navy is supporting emerging technology capable of using all available spectrum all the time. Technology under development known as cognitive radio systems will provide a dynamic spectrum access ability to identify and use unused radio frequencies. Cognitive radio systems capabilities will dramatically increase the effective and efficient use of radio frequencies by using more spectrum than is used today and simultaneously minimize the possibility of radio frequency interference.

As long as spectrum is defined as fuel for wireless technology, the oxygen of the Internet or prime real estate, it will likely be mismanaged as a finite resource. We are not running out of spectrum but, like time, spectrum that goes unused is wasted. CHIPS

Mr. Kidd is the director, strategic spectrum policy for the DON. For more information contact Mr. Kidd at DONSpectrumTeam@navy.mil.

Mr. Rossow is a senior spectrum analyst supporting the DON Spectrum Team.

Enterprise Architecture v2.0.000

By Kimberly Brooks and Victor Ecarma

The Department of the Navy Chief Information Officer (DON CIO) released the DON Enterprise Architecture (EA) v2.0.000, July 31, 2010. The DON EA v2.0.000 refines and expands on the content which was released as DON EA v1.1.000 and continues to focus on two overarching objectives:

- Guiding the DON's information technology, including National Security Systems (IT/NSS) investments toward achieving stated departmental goals and objectives.
- Assisting DON program managers in the development of "solution architectures" as mandated by the Joint Capabilities Integration and Development System (JCIDS) and Defense Acquisition System (DAS) processes.

New DON EA v2.0.000 content includes rules regarding open architecture, conditioned-based maintenance and the emerging country code standard. Architecture common element lists were added as part of the DON EA Business and Systems Reference Models. New Enterprise Reference Architecture (ERA) artifacts were also added, including: integrated data dictionary (AV-2), organizational structures (OV4-s), technical view standards (TV-1) and emerging standards (TV-2).

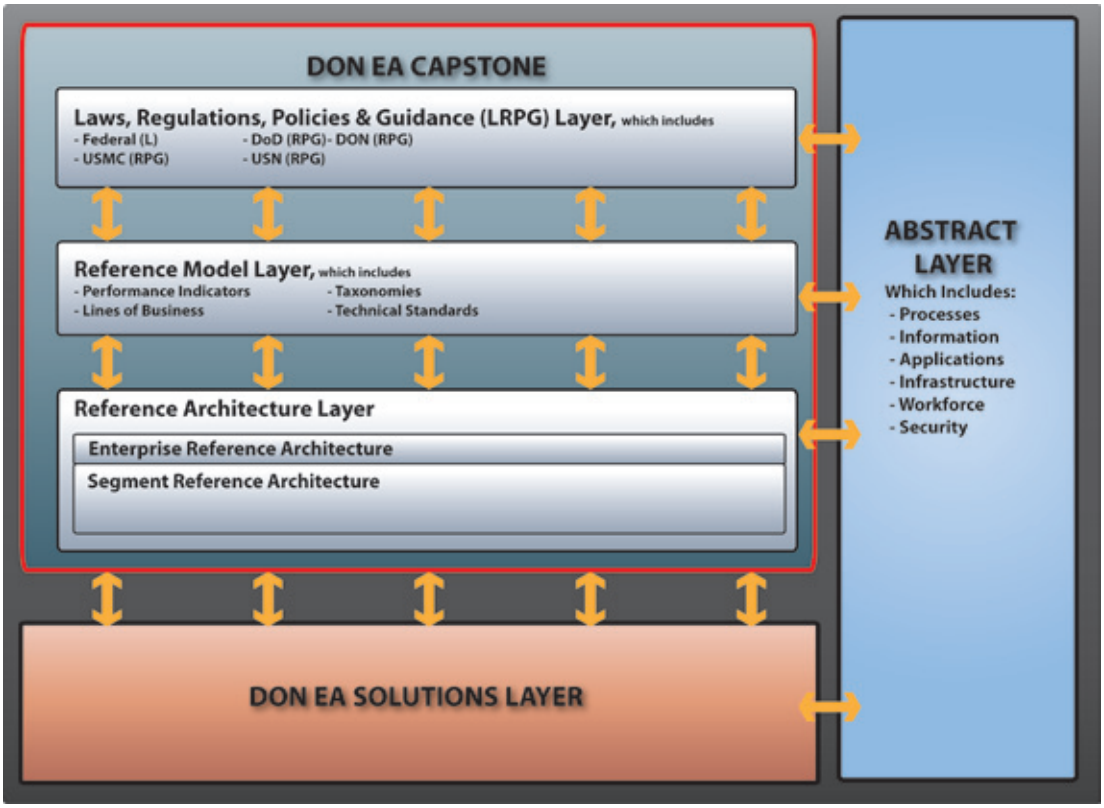
DON EA compliance shall continue to be assessed as part of the following processes:

- The DON Information Management/Information Technology (IM/IT) Investment Review Process. (As of Oct. 1, 2010, the IM/IT Investment Review Process was expanded to include all four mission areas);
- Business Mission Area (BMA), Enterprise Information Environment Mission Area (EIEMA), Warfighting Mission Area (WMA) and Defense Intelligence Mission Area (DIMA);
- The Title 40/Clinger-Cohen Act (Title 40/CCA) Confirmation process; and
- The DON NIPRNET Public Key Enablement (PKE) Waiver Request Process.

During fiscal year 2010, the DON EA assertion of compliance and review process was largely manual in nature and therefore included significant inefficiencies. To address these inefficiencies, this process was automated in the DON variant of the Department of Defense Information Technology Portfolio Repository (DITPR)-DON. This newly automated process will be aligned with functionality that already exists within DITPR-DON for requesting, reviewing and granting DON EA Compliance Waivers. Enforcement of compliance with DON EA v2.0.000 began on Oct. 1, 2010.

A listing of the content contained in DON EA v2.0.000, as well as other current and authoritative information about DON EA policy and procedures, can be viewed at https://www.intelink.gov/wiki/DONEA. In addition, announcements about DON EA status and updates can be tracked at: https://www.intelink.gov/chirp/group/donea.

The DON CIO; Assistant Secretary of the Navy for Research, Development and Acquisition (ASN RDA) Chief Systems Engineer (CHSENG); Navy and Marine Corps systems commands; and associated warfare centers are working toward integrating DON EA alignment and compliance reviews as part of the Systems Engineering Technical Review process. This will allow for programs to ensure alignment with the requirements and content of the DON EA early in the program's life cycle. CHIPS



The DON EA point of contact is the Director of Enterprise Architecture & Emerging Technology, Mr. Michael Jacobs. Ms. Brooks and Mr. Ecarma support the DON EA team.

News and Tips for Social Media

By Christy Crimmins

In this installment of the CHIPS Web 2.0 column we are bringing you a selection of news and tips about collaborative media from around the departments of the Navy and Defense.

SECNAV Signs Internet-based Capability ALNAVs

On Aug. 19, 2010, the Secretary of the Navy released two All Navy Messages (ALNAVs) addressing the use of social media in the DON. These messages provide guidance to DON personnel on the responsible use of Internet-based capabilities (IbC) in both their professional and personal capacities.

The first ALNAV, Internet-based Capabilities Guidance – Official Internet Posts, addresses the use of social media and collaborative tools as a means to disseminate and share official information. The ALNAV outlines some of the policies and procedures for communication in an official capacity via IbC.

The second ALNAV addresses the unofficial use of IbC and states that in addition to ensuring that official DON-related content posted to the Internet is within guidelines, it is recommended that DON personnel be mindful of all content posted to these sites, especially since the lines between personal and professional lives often blur in the online space. The message outlines policy and best practices to ensure that DON personnel are using these tools safely and effectively. Both ALNAVs addressing Internet-Based Capabilities Guidance can be found on the DON CIO website:

- Official Internet Posts
  www.doncio.navy.mil/PolicyView.aspx?ID=1899.
- Unofficial Internet Posts
  www.doncio.navy.mil/PolicyView.aspx?ID=1901.

Recommended Facebook Privacy Settings

As social networking continues to grow and evolve, users may find that more of their information is being shared publicly — sometimes without their knowledge. Much of this information can be safeguarded through the implementation of existing privacy settings.

Facebook recently rolled out a new location-based application that allows users to "check-in" at various locations, permitting friends to see where they are at that exact moment. Additionally, the feature allows other users to check in friends that are at the same location. While there are benefits to using this new feature, there is a trade-off of inadvertently sharing more personal information than some users may wish.

In an effort to help DON personnel safeguard their personal information while enjoying the benefits of social networking, the Navy Chief of Information (CHINFO) has provided a step-by-step guide to privacy settings on Facebook. While personnel and their families may choose to share more or less information, the guide walks users through CHINFO's "minimum recommended privacy settings." To view the presentation, please visit: *www.slideshare.net/navyffsc/recommended-facebook-privacy-settings.*

DoD Unveils New Social Media Hub

On July 22, 2010, the DoD launched an updated "Social Media Hub." The Web page is designed to be a resource for the responsible and effective use of social media and other Internet-based capabilities, and provides information and tips for both official and unofficial use. The site provides information for all levels of users, including training and education for those just beginning to use social media, and tips for any user to improve online safety. The policies and procedures section provides current policy documents as well as a link to register official social media presences. For more information on the DoD Social Media Hub, visit *http://socialmedia.defense.gov.*

FedSpace

FedSpace, hosted by the General Services Administration, is a secure intranet and collaboration workspace for federal employees and contractors. The site, funded through an e-Government project and developed in response to President Obama's 2009 Open Government Directive, is a collaborative space for federal employees and contractors.

Many agencies across the federal government have developed collaborative tools for use within their organizations. Unlike these tools, FedSpace aims to provide capabilities such as file sharing, wikis, a governmentwide employee directory, shared workspaces and blogs across agencies. FedSpace is currently in its "alpha" or initial test phase, so users might notice that some functionality is under development and contains some test content. Users are encouraged to provide feedback on the site to make it a valuable resource for all government employees. To get started, visit *http://fedspace.gov/connect.* CHIPS

Christy Crimmins provides support to the Department of the Navy Chief Information Officer communications and emerging technology teams.

Ready Rooms "Ready" for High-Tech Mission Planning

Antiquated communications systems and gear replaced with 21st century technologies aboard USS George H.W. Bush (CVN 77)

By Frank Kara

Since the earliest days of aircraft carrier-based flight, naval aviators have conducted pre-flight mission planning, briefing and post-flight debriefing in '"Ready Rooms" that were outfitted with the most basic accommodations: paper charts were taped to bulkheads; a few chalkboards were used for drawing; a battered desk housed a couple of drawers from which the squadron duty officer (SDO) attempted to control the daily chaos of endlessly changing operational priorities and flight schedules; and, of course, there was the infamous Ready Room chair.

Surprisingly, when the Navy took delivery of the final Nimitz-class aircraft carrier May 11, 2009, it was outfitted with outdated office equipment supporting sparse and antiquated Ready Room gear for use by embarked aviators who employ the newest generation of fighter and support aircraft. Fortunately, the shortcomings of Ready Room gear had been identified earlier, and in 2003, Congress funded a multi-year effort to research, identify, procure and install "transformational technology" into each of the Ready Rooms aboard USS George H.W. Bush (CVN 77).

USS Intrepid (CV 11) Ready Room circa 1944. Photo courtesy of National Naval Air Museum.

Today, the Navy's newest aircraft carrier is equipped with the latest Ready Room technologies which maximize information flow and leverage the capabilities of modern carrier-based aircraft.

In fall 2005, the Strike Planning and Execution Systems Program (PMA 281), under the cognizance of the Program Executive Office for Unmanned Aviation and Strike Weapons (PEO(U&W)), located at Naval Air Systems Command in Patuxent River, Md., assembled a team of functional experts, including naval aviation subject matter experts and ship design professionals, to determine the best approach to enhance CVN 77 Ready Room equipment and processes.

Team members interviewed aviators from various fleet squadrons, staffs of air and functional wings, and aviation training centers to identify the capabilities and equipment most urgently needing correction. The findings of this group were then validated by the commander of Naval Air Forces and action was taken to equip the Navy's newest aircraft carrier with modern transformational technologies.

Five Ready Room improvements were identified and funded, including increased local area network (LAN) access to support ever-increasing electronic flight mission planning activities, and to more fully exploit the capabilities of the Joint Mission Planning System (JMPS). The upgrade plan provides connectivity for both classified and unclassified computers in each Ready Room. Updated electronic displays to support aircrew flight briefing, debriefing and squadron training replaced obsolete overhead projectors with high-definition 57-inch LCDs, each equipped with an interactive SMART Board overlay connected through its own dedicated solid state computer.

At the front of the Ready Room is a 40-inch LCD to display air wing and ship operational information. There is a second 40-inch LCD near the squadron duty officer's desk for flight schedule and aircraft information. The SDO has a variety of smaller LCDs to view selected information and control the video feeds of both the 40-inch and 57-inch LCDs. Two 21-inch displays are installed on bulkheads in the rear of the Ready Room to support JMPS or other embarked air wing computers used during mission planning, rehearsal, debriefing or training events. Finally, modified sliding dry erase whiteboards (smaller than those previously installed) were retained to ensure no loss of capability in case of power loss or electronic failure.

USS GEORGE H.W. BUSH (CVN 77) Ready Room January 2010 with "transformational technology" including updated computer equipment and more robust LAN access. Chalkboards have been replaced by dry erase whiteboards, and paper charts taped to walls have been replaced with LCDs. Photo courtesy of U.S. Navy Strike Planning and Execution Systems Program (PMA 281).

Dedicated secure mission planning areas were installed in many larger Ready Rooms. The evolution of current and future aircraft capabilities produced the need to conduct mission planning, briefing and debriefing in a secure classified environment. The

upgrade provides a secure space capability while also allowing routine squadron business to be conducted.

A collaborative flight brief and debrief capability was installed to support electronic, secure activities between user selected Ready Rooms and the aircraft Carrier Intelligence Center (CVIC). This system includes an integrated microphone and sound system to allow interaction among all conference members from participating Ready Rooms, regardless of physical location.

The SDO's desk technologies were modernized to support improved coordination and execution of squadron flight operations. The new SDO desk has multiple computers and allows pairing of desired video feeds to any Ready Room display within the integrated video system. Video sources range from secure video information channel footage to presentations and files stored on a local computer.

USS Carl Vinson (CVN 70) received a partial installation of this upgrade. The remainder of Nimitz-class ships will receive the Ready Room modification as ship availabilities permit. The Ready Room upgrade will be installed aboard the Navy's newest aircraft carrier class, Gerald R. Ford. Thus, the modernization of Ready Rooms aboard all U.S. carriers is underway.

U.S. Navy carrier aviation has evolved with the growth and explosion of advanced technology. New aircraft, weapons, information systems and other technological developments have prompted the need to change and modernize aircraft carrier Ready Rooms, supporting operational missions in both peacetime and war. Though the Ready Room function of providing squadrons a place to plan, brief, debrief and congregate largely remains the same, the method and technologies supporting them have evolved. Carrier Ready Rooms now keep pace with technology — one look aboard the USS George H. W. Bush — and you'll be convinced. CHIPS

Frank Kara is a retired U.S. Navy commander and former F-14A/B/D radar intercept officer with operational deployments in VF-31 aboard USS Forrestal (CV 59), VF-102 aboard USS America (CV 66) and VF-11 aboard USS Carl Vinson (CVN 70). He currently provides systems engineering support for PMA 281. For more information, contact the PMA 281 public affairs office at (301) 757-9703.

Outreach Programs Provide Focus for Preparing the Cyber/IT Workforce

By the DON CIO Cyber/IT Workforce Team

To improve the knowledge base and skill level of the future Cyber/Information Technology (IT) Workforce, the Department of the Navy (DON) has numerous educational and outreach activities with academic institutions, other civilian agencies and industrial partners. These outreach programs are important not only to our cyber warfighting commands, but also to DON large acquisition commands, which employ hundreds of scientists and engineers who must be attuned to design, development and fielding of secure IT systems and applications.

In the DON's recent report to Congress, in response to the National Defense Authorization Act 2010, many "best practices" were highlighted. Of note, the Naval Sea Systems Command (NAVSEA) reported a diverse school outreach program which includes programs with elementary, middle and high schools in Philadelphia, Washington, D.C., and the Maryland area. The programs include the Mathematics, Engineering, Science Achievement (MESA) program (120 students), Office of Naval Research (ONR) Science and Engineering Apprenticeship Program (SEAP) (33 students), For Inspiration and Recognition of Science and Technology (FIRST) Robotics Team (90 students), FIRST LEGO (30 students) and SeaPerch (600 students). In addition, the organization sponsors Take Your Child to Work Day each year with more than 400 children of NAVSEA employees touring and participating in various science and technology workshops.

In the cyber/IT arena NAVSEA currently has partnerships with the following.

Organizations/Institutions/Associations:

- SeaPerch;
- For Inspiration and Recognition of Science and Technology (FIRST);
  - FIRST LEGO League;
  - FIRST Robotics;
- George Washington Carver City-Wide Science Fair (Philadelphia);
- Hispanic Association of Colleges and Universities (HACU);
- Hispanics in Science, Technology, Engineering and Mathematics (STEM);
- Advancing Minorities' Interests in Engineering (AMIE);
- American Indian Science and Engineering Society (AISES);
- National Society of Black Engineers (NSBE);
- Society of Hispanic Professional Engineers (SHPE);
- Society of Women Engineers (SWE); and
- Historically Black Colleges and Universities (HBCUs).

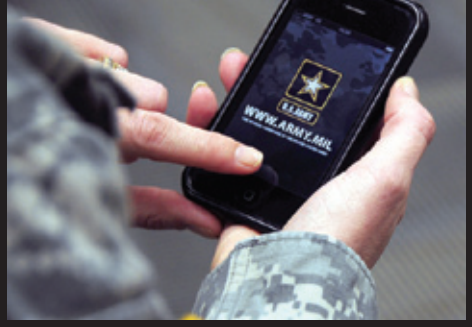
Government Partnerships:

- National Defense Education Program (NDEP);
  - Scientist and Engineers in the Classroom;
  - Engineering curriculum development in school districts;
- ONR Science and Engineering Apprenticeship Program (SEAP); and
- DoD Workforce Recruitment Program for College Students with Disabilities (WRP).

These programs help U.S. educational institutions focus on providing the best cyber curriculums and encourage students to pursue scientific and cyber courses of study. NAVSEA is to be commended for actively engaging in outreach programs so vital to accomplishing the DON's cyber mission. CHIPS

Apps for the Army Challenge

Army Soldiers and civilians respond with ingenuity and speed



By Holly Quick

This summer the Army turned the normal software development cycle on its ear by issuing "Apps for the Army," the Army's first internal application development challenge. Launched March 1, in just 75 days, 141 Soldiers and Army civilians registered in teams or as individuals to participate in the A4A challenge. By the May 15 deadline, 53 Web and mobile applications were developed and submitted.

The Apps for the Army challenge was the drumbeat at this year's LandWarNet, held in Tampa, Fla., Aug. 3-5. The theme of the conference was "Providing Global Cyber Dominance to Joint/Combined Commanders." The Army Chief Information Officer/G-6 is the sponsor for A4A, and the apps were a popular topic of discussion at the sessions and among conference attendees.

"We have a lot of capability within our Soldiers and our civilians that support this Army," said Lt. Gen. Jeff Sorenson, the Army CIO/G-6. "Given the opportunity to expose them to ways to either innovate or create different improvements in the way we operate as an Army or the way they have to live — if we just give them that opportunity to do such, the result normally is magic."

The Army provided the challenge participants with key resources, such as the Rapid Access Computing Environment (RACE), a multi-platform, cloud-based, secure development environment, hosted by the Defense Information Systems Agency. "You now have a computing environment that you can surge, you can expand, you can reduce," Sorenson said.

RACE offered access to on-demand virtual Windows and Red Hat Linux development environments for Android, BlackBerry, SharePoint, LAMP and ASP.net platforms.

Forge.mil, a family of services provided to support the Defense Department's technology development community, was also provided to participants. It served as the collaborative software repository for competitors. To facilitate the cross-pollination of ideas, problems and solutions relevant to the A4A initiative, milBook, the Army's internal Facebook solution, with more than 76,000 users, was used rather than e-mail.

After passing security certification, the apps were judged in five categories by a panel from across the Army. The categories include: Information Access, Location Aware, Training, Warfighting/Mission Specific and MWR/other.

Each of the five categories had first, second and third place winners who received $3,000, $1,500 and $1,000 respectively; there were also categories for honorable mention. Entries were judged on six criteria that assessed each application's usefulness, usability, appeal, inventiveness, effectiveness and viability.

"Usability seemed to be the No. 1 criterion with most of the judges," said Marvin Wages, A4A program manager. "Most of the judges say, well, I would really use this."

The top five A4A winners were recognized at LandWarNet.

New Recruit, an Android application, took first place in the Information Access category. It provides information for potential recruits that includes: military rank and insignia, Army news feeds, an Army physical fitness test calculator and a body mass index calculator.

First place in the Location Aware category was presented to the Movement Projection application, a map-routing Android app for road navigation that allows Soldiers to input obstacles and threats, in addition to stops, start and end points, and calculates the best and fastest route.

Physical Readiness Trainer, the first place winner in the Training category, is an iPhone app that helps Soldiers develop their own physical training program based on the Army's new Physical Readiness Training program. It provides training plans and videos of exercises. "We saw this as a new way that maybe training manuals in the future could be shown, something that is searchable and is fairly easy to navigate but also adds that media component," said Maj. Greg Motes, one of the app developers.

Disaster Relief Operations, an Android application that assists Army personnel working in humanitarian relief and civilian affairs, received first place in the Warfighting/Mission Specific category. It is a data survey, dissemination and analysis tool for accessing and creating maps viewable on Google Earth and Google Maps.

First place in the MWR/other category was awarded to the Telehealth Mood Tracker. This self-monitoring Android application allows users to track their psychological health over a period of days, weeks and months using a visual analogue rating scale. Users can track experiences associated with deployment-related behavioral health issues.

Winning apps are available at the Army Application Marketplace: https://storefront.mil/army/. For desktop access, a DoD CAC is needed. Users browsing from an iPhone and Android-based smartphones do not need a CAC. For more information about the Army CIO/G-6, go to http://ciog6.army.mil/. CHIPS

Holly Quick is a contributor to CHIPS and an operations research analyst with Space and Naval Warfare Systems Center Atlantic.

The DON's New Electronic Signature Policy

By Russell Pitcher

It has been 10 years since President Clinton signed the E-Sign Act ("Electronic Signatures in Global and National Commerce Act" (ESIGN)) granting electronic or digital signatures the same legal status as pen and ink signatures. Since that time, many civilian organizations have adopted electronic signatures as the preferred way for signing legal documents and records. Though there are a few instances in the Department of the Navy where electronic signatures have been used, in general, the DON has been slower to implement electronic signature solutions. There are several reasons for this, but the most often mentioned is that there is no clear guidance from the DON on the requirements for implementing an electronic signature solution.

Before we go further, it is important to understand the term "electronic signature." Electronic signature is sometimes confused with the term "digital signature" and it is important to understand the difference. Public Law 106-229, Electronic Signatures in Global and National Commerce Act, of June 30, 2000, defines an electronic signature as "an electronic sound, symbol, or process attached to, or logically associated with, a contract or other record and executed or adopted by a person with the intent to sign a record." This differs from a digital signature, which is an asymmetric key operation where a private key is used to digitally sign an electronic document, and the public key is used to verify the signature. The easy way to remember this is that electronic signatures serve the same purpose as a handwritten signature and show the person adopts the contents of an electronic document or record, while digital signatures are a subgroup of electronic signatures that provides authentication and integrity protection and are used to implement electronic signatures.

The lack of widespread use of electronic signatures and customer feedback identified the need for a DON electronic signature policy. To address this need, the DON Chief Information Officer signed the Secretary of the Navy Instruction 5239.21: "Department of the Navy Electronic Signature Policy," making electronic signatures the preferred means of signing documents and records within the department. By establishing this policy, the DON hopes to provide a catalyst for organizations to start to identify processes requiring handwritten signatures that can be more effectively accomplished electronically by converting them to electronic processes. This policy is not a mandate to replace handwritten signatures, but rather a policy to adopt electronic signatures as the preferred means of signing legal documents and records within the DON. This policy will ensure the DON complies with statutory and Defense Department mandates for paperless processing. It will also help to reduce the DON's reliance on paper transactions, improve information security and sharing, allow quicker access to documents, and reduce costs and environmental impact.

There are a few highlights in the policy that are important to remember when developing an electronic signature solution. Organizations with applications, systems and business processes that use electronic signatures shall comply with the following.

1. Electronic signatures are to be accomplished using a DoD-approved process that utilizes Public Key Infrastructure (PKI) certificates issued by DoD or a DoD-approved external PKI.
2. All electronic signature solutions must be certified and accredited, and tested and approved for conformance by the Joint Interoperability Test Command.
3. Conduct a legal review of the adopted application or process to ensure legal sufficiency, reliability and compliance with existing laws and regulations.
4. Ensure the integrity of electronically signed documents so that each record can be authenticated, attributed to the signer, and verified to be a full and accurate representation of the transaction to which it attests, to reflect the intent of the signer, and to be complete and unaltered.
5. Ensure all of the information required to validate a digital signature remains available for the life of the document.
6. Ensure the integrity of an electronically signed document in such a manner that records can be determined to be authentic and reliable by tracking the chain of custody and any changes that may occur (authorized or unauthorized).

Implementing electronic signatures is a key tool in the transformation of the department's virtual environments and business processes. The implementation of electronic signatures is essential to the DON's compliance with legislative and DoD mandates for paperless processing while maintaining information security and information sharing capabilities. CHIPS

Russell Pitcher supports the DON CIO Cybersecurity and Critical Infrastructure Team.

Rein In and Rethink the Use of Recall Rosters

By Michelle Schmith

The following is a recently reported data breach involving the disclosure of personally identifiable information contained in an alpha roster sent as an attachment in an unencrypted e-mail. Names have been changed or omitted but details are factual and based on reports sent to the Department of the Navy Chief Information Officer Privacy Office.

Background

Identity theft affected almost 10 million Americans last year. It is more important than ever that we protect the privacy information of DON personnel. Several recent breaches of personally identifiable information (PII) have involved the mishandling of recall rosters. Examples include rosters posted in: publicly accessible areas; rosters transmitted as e-mail attachments without proper encryption and marking; inclusion of the full or truncated Social Security number (SSN) on rosters; rosters stored on a shared drive/Web portal without the appropriate access controls/permissions in place; and failure to protect hard copy rosters outside the workplace. Data elements have included various combinations of names, SSNs, dates of birth, family members' names, home addresses, telephone numbers, and security clearances. Reasons given for dissemination included: all-hands meetings, training, social functions and access requests. Note: Alpha rosters (used to identify essential personnel who must report to duty despite adverse weather conditions or other unusual conditions) and flight rosters are considered recall rosters.

The Incident

In July 2010, a DON command received notification that a breach had occurred. An individual had sent an unencrypted e-mail with an attached alpha roster to several training representatives. The alpha roster contained PII for more than 1,000 personnel. The alpha roster contained SSNs, names, date of birth, health information and other PII. While the recipients had a "need to know" some of the PII elements for the purpose of personnel recall, some of the information (i.e., SSNs and health information) should not have been disclosed. All of the training representatives were notified to delete the unencrypted e-mail immediately.

Lessons Learned

The most valuable lesson learned from this incident is that before sending an e-mail that contains PII, ask: Do the recipient(s) have a need to know? Is the information appropriately marked as "FOUO – Privacy Sensitive"? Are the means of transmission secured? Should the information be displayed in this location? Are only essential PII elements listed? In this instance, if in fact the alpha roster had been properly marked, contained only essential PII elements (SSNs should NEVER be included), and the recipients had a "need to know" all of the information, then it could have been sent within the Defense Department firewall as an attachment to an encrypted e-mail.

Other preventive actions include:

- Establish procedures for proper maintenance, storage and dissemination of recall rosters;
- Provide PII training to ensure DON personnel follow established procedures;
- Ensure that compliance spot checks include recall rosters;
- Ensure that the sole purpose of the recall roster is to recall personnel and/or notify them of building, base or office closings;
- Limit PII elements to only the minimum required to recall an individual, e.g., names, addresses and telephone numbers (home, work, cell);
- Post recall rosters to intranet sites only when proper access controls/permissions are in place; and
- Include a Privacy Act Statement on every document containing PII.

See the Chief of Naval Operations (CNO) Memorandum, Recall Rosters, dated Sept. 7, 2006, at www.doncio.navy.mil/PolicyView.aspx?ID=1891 for additional information. CHIPS

Michelle Schmith is a member of the DON CIO Privacy Team.
Additional privacy information can be found on the DON CIO website: www.doncio.navy.mil.

Learning, Development Roadmap Available for All Enlisted Sailors

By Ed Barker

Culminating three years of intense work by the staffs at Naval Education and Training Command (NETC) learning centers, learning and development roadmaps (LaDRs) are available for every rating as of Aug. 6. Announced in NAVADMIN 258/10, the completed LaDRs are fleet-focused products that provide guidance to Sailors along a learning and development continuum that is specific to each rating.

"Completion of all learning and development roadmaps is a significant milestone for helping Sailors to be successful in their ratings," said Master Chief Petty Officer of the Navy (SS/SW) Rick D. West. "Having a written guide that explains in detail what each Sailor needs at specific points in their career is an invaluable tool for service members and their mentors."

All rating-specific LaDRs were developed by subject matter experts at the NETC learning centers and include input from the enlisted community managers at the Bureau of Naval Personnel and have been validated by the fleet.

"The LaDR for each rating is organized around significant career phases and enables targeted learning opportunities," said Tom Smith, NETC enlisted learning and development coordinator. "Each LaDR is also sequenced to meet growing and changing roles throughout a career. Sailors new to the Navy and early in their careers will find that LaDRs provide a solid technical and analytical foundation that will support tactical and operational competencies."

As a Sailor becomes more senior, learning and development provides an increased strategic perspective and more effective management and business practices. Sailors using LaDRs can properly chart out Navy-valued professional career goals.

"For a supervisor, LaDRs provide a navigable, rate-specific guide to assist in the effective mentorship of Sailors," Smith said. "Command indoctrination is the perfect opportunity for leadership to introduce the LaDRs to their new Sailors. Introducing the LaDRs early-on will result in every service member gaining baseline knowledge of his or her career progression and assist them in setting realistic goals toward upward career mobility."

ATLANTIC OCEAN (July 21, 2010) – Operations Specialist 3rd Class LaShawn E. Sloan, the tactical information coordinator, monitors a radar system aboard the aircraft carrier USS Enterprise (CVN 65). Enterprise is on a scheduled underway for fleet replacement squadron carrier qualifications and is making preparations for its 21st deployment. U.S. Navy photo by Mass Communication Specialist Seaman Apprentice Jared M. King.

"Completion of all learning and development roadmaps is a significant milestone for helping Sailors to be successful in their ratings."

– Master Chief Petty Officer of the Navy (SS/SW) Rick D. West

"LaDRs can also serve as an important guidance tool to use during a Sailor's career development board," said Master Chief Navy Career Counselor (SW/SCW/AW) Tod Shuls, NETC force retention program manager. "Review of LaDRs by leaders helps them recognize and reinforce a Sailor's forward progress and positive job and character traits."

Commanders are required to ensure distribution of LaDRs to every enlisted paygrade at all commands. This can be accomplished through Navy Knowledge Online: https://www.nko.navy.mil/portal/home/. After accessing the NKO home page, a Sailor selects the "Career Management" tab and navigates along the blue side banner and selects the Enlisted LaDR hyperlink.

According to OPNAV Instruction 1500.77, the LaDRs are required to be used during career development boards.

Additional information about learning and development roadmaps is detailed in NAVADMIN 258/10, available from the Reference Library on the Navy Personnel Command website: www.npc.navy.mil/ReferenceLibrary/Messages/. CHIPS

Ed Barker works for the Naval Education and Training Command public affairs office. For more information, visit www.navy.mil/local/cnet/ .

Navy COOL: Helping Sailors Today and Tomorrow

By Gary Nichols

With the current economic situation, the Navy's jobs, benefits and career opportunities are becoming even more attractive for those eligible for military service.

The Navy may have a real edge over the other services when it comes to signing on new recruits thanks to a well-established and growing program, the Navy Credentialing Opportunities OnLine or Navy COOL program, which was established at the Center for Information Dominance (CID) Corry Station in Pensacola, Fla., in 2006.

This program provides funding for Navy enlisted personnel to obtain civilian licenses and certifications that complement (and in many ways support) their Navy jobs or ratings. This is significant because Sailors now have a definite advantage in the civilian job market when they retire or when their enlistment ends.

The Navy COOL program also helps make the Navy a smart choice for young men and women who are considering serving their country, but are unsure which job they want or which branch of the U.S. Armed Forces they wish to serve in.

Navy COOL is a centralized, Web-based hub that consolidates information from numerous sources at the federal, state and local levels on certifications, licenses, apprenticeships and growth opportunities that correspond with each Navy rating, job and occupation.

Originally modeled on a program by the Army, the Navy COOL program has taken on a life of its own and grown exponentially in the scope of certifications it offers to Sailors in the four years the program has been in existence.

Navy COOL program supervisor Sam Kelley said this program has become more comprehensive than the Army's program because his team cross-linked every Navy specialty or rating with the Department of Labor to ensure the Navy offered at least one civilian certification that matched every job in the Navy.

Navy COOL provides funding for Navy enlisted personnel (both active duty and Reserve) to obtain civilian licenses and certifications that are closely aligned to Navy jobs or ratings.

While it's true the Navy does need a large pool of applicants, it places an even higher priority on recruiting the best applicants possible. Kelley said someone who is interested in self-improvement is likely to be a go-getter and someone who would take advantage of all that Navy COOL offers. That's the kind of person the Navy is interested in recruiting and retaining.

"Credentialing within the Department of Navy is a relatively new concept but is paying huge dividends for our Sailors who have used the program," Kelley said.

In fact, the Navy COOL program has helped CID win a number of awards. These include the Naval Education and Training Command Excellence Award for 2010, the Navy Meritorious Unit Citation in 2009, American Society for Training and Development Award for 2008, Workforce Magazine's Top 125 for 2010, and Workforce Management Magazine's Optimas Award for 2009.

"I am extremely proud of the outstanding work performed by our Navy COOL team," CID Corry Station Commanding Officer Capt. Gary Edwards said. "They have done an absolutely great job of ensuring that each and every Sailor in the Navy can improve personally and professionally by having an opportunity to earn certifications."

The end result of the pursuit of a civilian certification is that the Sailor's individual professional knowledge and skill set usually increases due to the extra preparation time required for certification examinations and ongoing maintenance of that certification.

"These additional skills may not necessarily be performed or taught in the Navy's formal training pipeline," Kelley said, "but are skills performed by the Sailors' civilian counterparts. The real benefit to the Navy is having a Sailor with increased individual proficiency as a result of gaining and maintaining additional industry-recognized skills."

Undoubtedly some Sailors are leaving the Navy with newly minted credentials in tow, but Navy COOL program manager Keith Boring is not overly concerned by these occasional losses.

A trained and certified worker, Boring said, is surely contributing to society in a positive way, too, and that is not a bad thing because it is helping to keep the country strong. Plus, he said, someone who is successful in the civilian sector after receiving Navy training and having the Navy pay for his or her civilian certifications is a living, breathing recruitment poster for the Navy.

All Sailors can benefit from Navy COOL, even those potential Sailors who have yet to raise their hand and take the oath to serve their country. Navy COOL can help make active-duty Sailors better at their present job, too.

At some point in their careers, whether they serve for three years or 30, Sailors must eventually take off their uniform and rejoin the civilian sector. Navy COOL will help make that transition easier and provide the necessary tools for that Sailor-turned-civilian to not only survive but thrive in what may be an unfamiliar civilian life.

"This program is a win for the Sailor, the Navy and the civilian Department of Labor workforce," Kelley said.

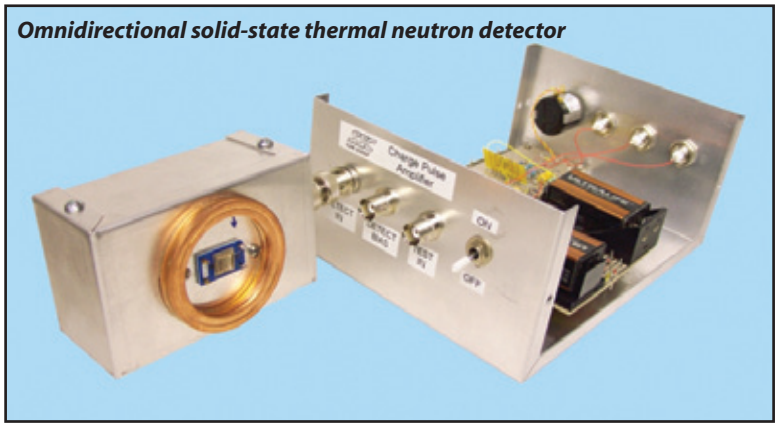
With a staff of more than 1,050 military, civilian and contracted staff members, CID Corry Station oversees the development and administration of more than 168 courses at 16 learning sites throughout the United States and in Japan. CID Corry Station provides training for more than 19,000 members of the U.S. Armed Services and allied forces each year.

For more information visit the official Navy COOL website at https://www.cool.navy.mil. CHIPS

Gary Nichols works for the Center for Information Dominance Corry Station public affairs office.

SSC Pacific scientist awarded patent for nuclear detection device

By Ann Dakis



A new invention by a Space and Naval Warfare Systems Center (SSC) Pacific scientist, Dr. Wayne McGinnis, may enable U.S. Navy and Department of Homeland Security personnel to more effectively detect radioactive materials, such as plutonium, that are being transported illegally on ships, through ports of entry, or by other means.

Such materials present a critical threat to the United States because they can be used in manufacturing nuclear weapons.

A patent for the invention, titled "Omnidirectional solid-state thermal neutron detector," was awarded on June 29 of this year under U.S. Patent 7745800.

"This device furthers the work that a number of us at SSC Pacific began about a decade ago to find an efficient and convenient means to detect concealed radioactive materials," McGinnis said. "We developed a solid-state thermal neutron detector that was patented in 2008 and provides the basis for the new invention."

The detector consists of a semiconducting or insulating sheet of neutron-reactive material, such as boron nitride, sandwiched between two parallel conducting electrodes formed of a metal, such as titanium or zirconium. The total thickness of the boron nitride detector element is typically less than one millimeter. A small voltage applied between the two electrodes produces a continuous electric field within the neutron-reactive material. Because the boron nitride is highly resistive (not electrically conductive), only an extremely small background current will flow between the two electrodes when no neutrons are present.

Thermal neutrons emitted from a radioactive substance interact with the nuclei of boron atoms within boron nitride. Energetic alpha particles (helium nuclei) are one product of this nuclear reaction. The alpha particles then collide with other boron and nitrogen atoms within the boron nitride, knocking electrons from their atomic orbit. These newly freed charge carriers are swept toward the positive electrode, producing a current pulse (larger than the background current), thus indicating the presence of the neutron-emitting nuclear material.

"The solid-state thermal neutron detector provides improvements in sensitivity, size, weight, power consumption, operator safety, transportability and cost compared to other available detectors such as gas proportional counters and scintillation counters," McGinnis said. "It is more compact and therefore more portable. Operation at low voltage also means that the electronics used to apply the electrode voltage and to measure the detector current can be simpler, more compact, safer to the user, and much less power consuming."

However, like the helium-based counters, this device was unable to determine neutron flux direction, so McGinnis went back to work to find a solution to this remaining deficiency. He found that by arranging multiple planar neutron detector elements orthogonally, i.e., at right angles with respect to each other, omnidirectional detection could be attained. Each element will absorb a fraction of the incident neutrons. By comparing the detection (or current pulse) count rate for each detector element, the direction of the neutron flux can be determined.

"This arrangement can take many forms. One example is a configuration wherein six planar solid-state neutron elements are arranged to form the faces of a cube," McGinnis said. "Each pair of opposing sides of the cube forms a directional neutron detecting apparatus, in this instance one of three orthogonally arranged pairs of elements. For a given detector element pair, the neutron source will be on the cube side with the highest count rate." (See Figure 1.)

The new omnidirectional detector has potential use in locating hidden nuclear radiation sources, monitoring nuclear worker safety, hazardous materials assessment, and nuclear weapons surveying.

With support from the Defense Threat Reduction Agency (DTRA) and the Department of Homeland Security, McGinnis has been working with the University of Michigan to develop prototype individual detector elements for evaluation. Future efforts will focus on optimization of boron nitride as a neutron detection material, and demonstration of its use in a solid-state detector that includes directional capability. CHIPS

Ann Dakis works in the SSC Pacific public affairs office.

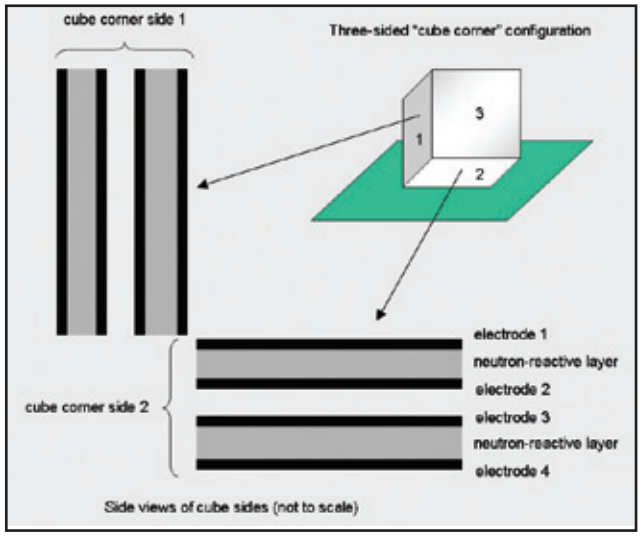


Figure 1.

Enterprise Software Agreements

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

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

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

For more information on the ESI or to obtain product information, visit the ESI website at www.esi.mil/.

Software Categories for ESI:

Asset Discovery Tools

Belarc

BelManage Asset Management – Provides software, maintenance and services.

Contractor: ***Belarc Inc.*** (W91QUZ-07-A-0005)

Authorized Users: This BPA is open for ordering by all Department of Defense (DoD) components and authorized contractors.

Ordering Expires: 30 Sep 11

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

BMC

Remedy Asset Management – Provides software, maintenance and services.

Contractor: ***BMC Software Inc.*** (W91QUZ-07-A-0006)

Authorized Users: This BPA is open for ordering by all Department of Defense (DoD) components and authorized contractors.

Ordering Expires: 23 Mar 15

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

Carahsoft

Opsware Asset Management – Provides software, maintenance and services.

Contractor: ***Carahsoft Inc.*** (W91QUZ-07-A-0004)

Authorized Users: This BPA is open for ordering by all Department of Defense (DoD) components and authorized contractors.

Ordering Expires: 14 Nov 10 (Please call for extension information.)

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

DLT

BDNA Asset Management – Provides asset management software, maintenance and services.

Contractor: ***DLT Solutions Inc.*** (W91QUZ-07-A-0002)

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

Ordering Expires: 01 Apr 13

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

Business and Modeling Tools

BPWin/ERWin

BPWin/ERWin – Provides products, upgrades and warranty for ERWin, a data modeling solution that creates and maintains databases, data warehouses and enterprise data resource models. It also provides BPWin, a modeling tool used to analyze, document and improve complex business processes.

The BPWin/ERWin products are now available from the C-EMS2 contract on page 54. The C-EMS2 contract number is listed below.

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

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

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

Database Management Tools

Microsoft Products

Microsoft Database Products – See information under Office Systems on page 49.

Oracle (DEAL-O)

Oracle Products – Provides Oracle database and application software licenses, support, training and consulting services. The Navy Enterprise License Agreement is for database licenses for Navy customers. Contact the Navy project manager.

Contractors:

Oracle Corp. (W91QUZ-07-A-0001); (703) 364-3351

DLT Solutions (W91QUZ-06-A-0002); (703) 708-9107

immixTechnology, Inc. (W91QUZ-08-A-0001); Small Business; (703) 752-0632

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

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

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

Authorized Users: This has been designated as a DoD ESI and GSA SmartBUY contract and is open for ordering by all U.S. federal agencies, DoD components and authorized contractors.

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

Special Note to Navy Users: See the information provided on page 50 concerning the Navy Oracle Database Enterprise License under Department of the Navy Agreements.

Sybase (DEAL-S)

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

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

Ordering Expires: 15 Jan 13

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

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

Enterprise Application Integration

Sun Software

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

Contractors:

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

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

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

Ordering Expires: 24 Sep 12

Web Link:
http://www.public.navy.mil/usff/itumbrella/Pages/AllDocuments.aspx

Enterprise Architecture Tools

IBM Software Products

IBM Software Products – Provides IBM product licenses and maintenance with discounts from 1 to 19 percent off GSA pricing. On June 28, 2006, the IBM Rational Blanket Purchase Agreement (BPA) with immixTechnology was modified to include licenses and Passport Advantage maintenance for IBM products, including: IBM Rational, IBM Database 2 (DB2), IBM Informix, IBM Trivoli, IBM Websphere and Lotus software products.

Contractor: ***immixTechnology, Inc.*** (DABL01-03-A-1006); Small Business; (800) 433-5444

Ordering Expires: 02 Dec 10

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

Enterprise Management

CA Enterprise Management Software (C-EMS2)

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

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

Ordering Expires: 22 Sep 12

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

Microsoft Premier Support Services (MPS-2)

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

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

Ordering Expires: 31 Mar 11

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

NetIQ

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

Contractors:

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

Northrop Grumman – authorized reseller

Federal Technology Solutions, Inc. – authorized reseller

Ordering Expires: 05 May 14

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

Planet Associates

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

Contractor: ***Planet Associates, Inc.*** (N00104-09-A-ZF36); Small Business; (732) 922-5300 ext. 202

Ordering Expires: 01 Jun 14

Web Link:
http://www.public.navy.mil/usff/itumbrella/Pages/AllDocuments.aspx

Quest Products

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

Contractors:

Quest Software, Inc. (W91QUZ-05-A-0023); (301) 820-4800

DLT Solutions (W91QUZ-06-A-0004); (703) 708-9127

Ordering Expires:
Quest: 30 Sep 10 (Please call for extension information.)
DLT: 01 Apr 13

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

Enterprise Resource Planning

Oracle

Oracle – *See information provided under Database Management Tools on page 45.*

RWD Technologies

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

Contractor: ***RWD Technologies*** (N00104-06-A-ZF37); (410) 869-3014

Ordering Expires: Effective for term of the GSA FSS Schedule

Web Link:
http://www.public.navy.mil/usff/itumbrella/Pages/AllDocuments.aspx

SAP

SAP Products – Provide software licenses, software maintenance support, information technology professional services and software training services.

Contractors:

SAP Public Services, Inc. (N00104-08-A-ZF41); Large Business; (202) 312-3515

Advantaged Solutions, Inc. (N00104-08-A-ZF42); Small Business; (202) 204-3083

Carahsoft Technology Corporation (N00104-08-A-ZF43); Small Business; (703) 871-8583

Oakland Consulting Group (N00104-08-A-ZF44); Small Business; (301) 577-4111

Ordering Expires: 14 Sep 13

Web Link:
http://www.public.navy.mil/usff/itumbrella/Pages/AllDocuments.aspx

Information Assurance Tools

Data at Rest Solutions BPAs offered through ESI/SmartBUY

The Office of Management and Budget, Defense Department and General Services Administration awarded multiple contracts for blanket purchase agreements (BPA) to protect sensitive, unclassified data residing on government laptops, other mobile computing devices and removable storage media devices.

These competitively awarded BPAs provide three categories of software and hardware encryption products — full disk encryption (FDE), file encryption (FES) and integrated FDE/FES products. All products use cryptographic modules validated under FIPS 140-2 security requirements and have met stringent technical and interoperability requirements.

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

Service component chief information officers (CIO) are developing component service-specific enterprise strategies. Accordingly, customers should check with their CIO for component-specific policies and strategies before procuring a DAR solution. The departments of the Navy and Army released service-specific DAR guidance for their personnel to follow. Go to the ESI website at www.esi.mil for more information.

The DON CIO issued an enterprise solution for Navy users purchasing DAR software. See the information provided on page 50 under Department of the Navy Agreements. The Department of the Army issued an enterprise solution for Army users purchasing DAR software. See the information provided on the Army CHESS website at https://chess.army.mil/ascp/commerce/contract/FA8771-07-A-0301_bpaorderinginstructions(2)_ARMY.jsp. As of this printing, the Air Force has not yet provided a DAR solution.

Mobile Armor – ***MTM Technologies, Inc.*** (FA8771-07-A-0301)

McAfee, formerly Safeboot – ***Rocky Mountain Ram*** (FA8771-07-A-0302)

Information Security Corp. – ***Carahsoft Technology Corp.*** (FA8771-07-A-0303)

McAfee – ***Spectrum Systems*** (FA8771-07-A-0304)

SafeNet, Inc. – ***SafeNet, Inc.*** (FA8771-07-A-0305)

Encryption Solutions, Inc. – ***Hi Tech Services, Inc.*** (FA8771-07-A- 0306)

Pointsec/Checkpoint – ***immix Technologies*** (FA8771-07-A-0307)

SPYRUS, Inc. – ***Autonomic Resources, LLC*** (FA8771-07-A-0308)

WinMagic, Inc. – ***Govbuys, Inc.*** (FA8771-07-A-0310)

CREDANT Technologies – ***Intelligent Decisions*** (FA8771-07-A-0311)

Symantec, formerly GuardianEdge Technologies – ***Merlin International*** (FA8771-07-A-0312)

Ordering Expires: 14 Jun 12 (If extended by option exercise.)

Web Link: www.esi.mil

McAfee

McAfee – Provides software and services in the following areas: Anti-Virus; E-Business Server; ePolicy Orchestrator; GroupShield Services; IntruShield; Secure Messaging Gateway and Web Gateway.

Contractor: ***En Pointe*** (GS-35F-0372N)

Ordering Expires: 16 Sep 11

Web Link: www.esi.mil

Antivirus Web Links: Antivirus software available at no cost; download includes McAfee, Symantec and Trend Micro Products. These products can be downloaded by linking to either of the following websites:

NIPRNET site: https://patches.csd.disa.mil
SIPRNET site: https://www.cert.smil.mil/antivirus/av_info.htm

McAfee (formerly Securify)

McAfee – Provides policy-driven appliances for network security that are designed to validate and enforce intended use of networks and applications; protects against all risks and saves costs on network and security operations. McAfee integrates application layer seven traffic analysis with signatures and vulnerability scanning in order to discover network behavior. It provides highly accurate, real-time threat mitigation for both known and unknown threats and offers true compliance tracking.

Contractor: ***Patriot Technologies, Inc.*** (FA8771-06-A-0303)

Ordering Expires: 04 Jan 11 (If extended by option exercise)

Web Link: www.esi.mil

Symantec

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

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

Ordering Expires: 12 Sep 10 (Please check the ESI website at www.esi.mil for extension information.)

Web Link: http://var.immixgroup.com/contracts/overview.cfm or www.esi.mil

Symantec Antivirus:

Notice to DoD customers regarding Symantec Antivirus Products: A fully funded and centrally purchased DoD enterprise-wide antivirus and spyware software license is available for download to all Department of Defense (DoD) users who have a .mil Internet Protocol (IP) address.

Contractor: ***TVAR Solutions, Inc.***

Antivirus Web Links: Antivirus software can be downloaded at no cost by linking to either of the following websites:

NIPRNET site: https://patches.csd.disa.mil

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

Websense (WFT)

Websense – Provides software and maintenance for Web filtering products.

Contractor: ***Patriot Technologies*** (W91QUZ-06-A-0005)

Authorized Users: This BPA is open for ordering by all DoD components and authorized contractors.

Ordering Expires: 31 Aug 11

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

Xacta

Xacta – Provides Web Certification and Accreditation (C&A) software products, consulting support and enterprise messaging management solutions through its Automated Message Handling System (AMHS) product. The software simplifies C&A and reduces its costs by guiding users through a step-by-step process to determine risk posture and assess system and network configuration compliance with applicable regulations, standards and industry best practices, in accordance with the DITSCAP, NIACAP, NIST or DCID processes. Xacta's AMHS provides automated, Web-based distribution and management of messaging across your enterprise.

Contractor: ***Telos Corp.*** (FA8771-09-A-0301); (703) 724-4555

Ordering Expires: 24 Sep 14

Web Link: http://esi.telos.com/contract/overview

Lean Six Sigma Tools

iGrafx Business Process Analysis Tools

iGrafx – Provides software licenses, maintenance and media for iGrafx Process for Six Sigma 2007; iGrafx Flowcharter 2007; Enterprise Central; and Enterprise Modeler.

Contractors:

Softchoice Corporation (N00104-09-A-ZF34); (416) 588-9002 ext. 2072

Softmart, Inc. (N00104-09-A-ZF33); (610) 518-4192

SHI (N00104-09-A-ZF35); (732) 564-8333

Authorized Users: These BPAs are co-branded ESI/GSA SmartBUY BPAs and are open for ordering by all Department of Defense (DoD) components, U.S. Coast Guard, NATO, Intelligence Community, authorized DoD contractors and all federal agencies.

Ordering Expires: 31 Jan 14

Web Links:

Softchoice
http://www.public.navy.mil/usff/itumbrella/Pages/AllDocuments.aspx
Softmart
http://www.public.navy.mil/usff/itumbrella/Pages/AllDocuments.aspx
SHI
http://www.public.navy.mil/usff/itumbrella/Pages/AllDocuments.aspx

Minitab

Minitab – Provides software licenses, media, training, technical services and maintenance for products, including: Minitab Statistical Software, Quality Companion and Quality Trainer. It is the responsibility of the ordering officer to ensure compliance with all fiscal laws prior to issuing an order under a BPA, and to ensure that the vendor selected represents the best value for the requirement being ordered (see FAR 8.404).

Contractor: ***Minitab, Inc.*** (N00104-08-A-ZF30); (800) 448-3555 ext. 311

Authorized Users: This BPA is open for ordering by all Department of Defense (DoD) components, U.S. Coast Guard, NATO, Intelligence Community and authorized DoD contractors.

Ordering Expires: 07 May 13

Web Link:
http://www.public.navy.mil/usff/itumbrella/Pages/AllDocuments.aspx

PowerSteering

PowerSteering – Provides software licenses (subscription and perpetual), media, training, technical services, maintenance, hosting and support for PowerSteering products: software as a service solutions to apply the proven discipline of project and portfolio management in IT, Lean Six Sigma, Project Management Office or any other project-intensive area and to improve strategy alignment, resource management, executive visibility and team productivity. It is the responsibility of the ordering officer to ensure compliance with all fiscal laws prior to issuing an order under a BPA, and to ensure that the vendor selected represents the best value for the requirement being ordered (see FAR 8.404).

Contractor: ***immixTechnology, Inc.*** (N00104-08-A-ZF31); Small Business; (703) 752-0661

Authorized Users: All DoD components, U.S. Coast Guard, NATO, Intelligence Community, and authorized DoD contractors.

Ordering Expires: 14 Aug 13

Web Link:
http://www.public.navy.mil/usff/itumbrella/Pages/AllDocuments.aspx

Office Systems

Adobe Desktop Products

Adobe Desktop Products – Provides software licenses (new and upgrade) and maintenance for numerous Adobe desktop products, including Acrobat (Standard and Professional); Photoshop; InDesign; After Effects; Frame; Creative Suites; Illustrator; Flash Professional; Dreamweaver; ColdFusion and other Adobe desktop products.

Contractors:

Dell Marketing L.P. *(formerly ASAP)* (N00104-08-A-ZF33); (800) 248-2727, ext. 5303

CDW-G (N00104-08-A-ZF34); (703) 621-8211

GovConnection, Inc. (N00104-08-A-ZF35); (301) 340-3861

Insight Public Sector, Inc. (N00104-08-A-ZF36); (443) 306-7885

Ordering Expires: 30 Jun 12

Web Link:
http://www.public.navy.mil/usff/itumbrella/Pages/AllDocuments.aspx

Adobe Server Products

Adobe Server Products – Provides software licenses (new and upgrade), maintenance, training and support for numerous Adobe server products including LiveCycle Forms; LiveCycle Reader Extensions; Acrobat Connect; Flex; ColdFusion Enterprise; Flash Media Server and other Adobe server products.

Contractor:

Carahsoft Technology Corp. (N00104-09-A-ZF31); Small Business; (703) 871-8503

Ordering Expires: 14 Jan 14

Web Link:
http://www.public.navy.mil/usff/itumbrella/Pages/AllDocuments.aspx

Microsoft Products

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

Contractors:

CDW-G (N00104-02-A-ZE85); (888) 826-2394

Dell (N00104-02-A-ZE83); (800) 727-1100 ext. 7253702 or (512) 725-3702

GovConnection (N00104-10-A-ZF30); (301) 340-3861

Hewlett-Packard (N00104-02-A-ZE80); (978) 399-9818

Insight Public Sector, Inc. (N00104-02-A-ZE82); (800) 862-8758

SHI (N00104-02-A-ZE86); (732) 868-5926

Softchoice (N00104-02-A-ZE81); (877) 333-7638

Softmart (N00104-02-A-ZE84); (800) 628-9091 ext. 6928

Ordering Expires: 31 Mar 13

Web Link:
http://www.public.navy.mil/usff/itumbrella/Pages/AllDocuments.aspx

Red Hat/Netscape/Firefox

Through negotiations with August Schell Enterprises, DISA has established a DoD-wide enterprise site license whereby DISA can provide ongoing support and maintenance for the Red Hat Security Solution server products that are at the core of the Department of Defense's Public Key Infrastructure (PKI). The Red Hat Security Solution includes the following products: Red Hat Certificate System and dependencies; Red Hat Directory Server; Enterprise Web Server (previously Netscape Enterprise Server); and Red Hat Fortitude Server (replacing Enterprise Server). August Schell also provides a download site that, in addition to the Red Hat products, also allows for downloading DISA-approved versions of the following browser products: Firefox Browser; Netscape Browser; Netscape Communicator; and Personal Security Manager. The Red Hat products and services provided through the download site are for exclusive use in the following licensed community: (1) All components of the U.S. Department of Defense and supported organizations that utilize the Joint Worldwide Intelligence Communications System, and (2) All non-DoD employees (e.g., contractors, volunteers, allies) on-site at the U.S. Department of Defense and those not on-site but using equipment furnished by the U.S. Department of Defense (GFE) in support of initiatives which are funded by the U.S. Department of Defense.

Licensed software products available through the August Schell contract are for the commercial versions of the Red Hat software, not the segmented versions of the previous Netscape products that are compliant with Global Information Grid (GIG) standards. The segmented versions of the software are required for development and operation of applications associated with the GIG, the Global Command and Control System (GCCS) or the Global Combat Support System (GCSS).

If your intent is to use a Red Hat product to support development or operation of an application associated with the GIG, GCCS or GCSS, you must contact one of the websites listed below to obtain the GIG segmented version of the software. You may not use the commercial version available from the August Schell Red Hat download site.

If you are not sure which version (commercial or segmented) to use, we strongly encourage you to refer to the websites listed below for additional information to help you to make this determination before you obtain the software from the August Schell Red Hat download site (or contact the project manager).

GIG or GCCS users: Common Operating Environment Home Page
www.disa.mil/gccs-j/index.html
GCSS users: Global Combat Support System
www.disa.mil/gcssj

Contractor: ***August Schell Enterprises*** (www.augustschell.com)

Download Site: http://redhat.augustschell.com
Ordering Expires: 14 Mar 11
All downloads provided at no cost.

Web Link: http://iase.disa.mil/netlic.html

Red Hat Linux

Red Hat Linux – Provides operating system software license subscriptions and services to include installation and consulting support, client-directed engineering and software customization. Red Hat Enterprise Linux is the premier operating system for open source computing. It is sold by annual subscription, runs on seven system architectures and is certified by top enterprise software and hardware vendors.

Contractors:

Carahsoft Technology Corporation (HC1028-09-A-2004)

DLT Solutions, Inc. (HC1028-09-A-2003)

Ordering Expires:
Carahsoft: 09 Feb 14
DLT Solutions, Inc.: 17 Feb 14

Web Link: www.esi.mil

Operating Systems

Apple

Apple – Provides Apple Desktop and Server Software, maintenance, related services and support as well as Apple Perpetual Software licenses. These licenses include Apple OS X Server v10.5; Xsan 2; Apple Remote Desktop 3.2; Aperture 2; Final Cut Express 4; Final Cut Studio 2; iLife '08; iWork '08; Logic Express 8; Logic Pro 7; Mac OS X v10.5 Leopard; QuickTime 7 Pro Mac; and Shake 4.1 Mac OS X. Software Maintenance, OS X Server Support, AppleCare Support and Technical Service are also available.

Contractor: ***Apple, Inc.*** (HC1047-08-A-1011)

Ordering Expires: 10 Sep 11

Web Link: www.esi.mil

Sun (SSTEW)

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

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

Ordering Expires: Dependent on GSA schedule until 2011

Web Link: www.disa.mil/contracts/guide/bpa/bpa_sun.html

Research and Advisory BPA

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

Gartner Group (N00104-07-A-ZF30); (703) 378-5697; Awarded 01 Dec 2006

Ordering Expires: Effective for term of GSA contract

Authorized Users: All DoD components. For the purpose of this agreement, DoD components include: the Office of the Secretary of Defense; U.S. Military Departments; the Chairman of the Joint Chiefs of Staff; Combatant Commands; the Department of Defense Office of Inspector General; Defense Agencies; DoD Field Activities; the U.S. Coast Guard; NATO; the Intelligence Community and Foreign Military Sales with a letter of authorization. This BPA is also open to DoD contractors authorized in accordance with the FAR Part 51.

Web Link:
http://www.public.navy.mil/usff/itumbrella/Pages/AllDocuments.aspx

Department of the Navy Agreements

Oracle (DEAL-O) Database Enterprise License for the Navy

On Oct. 1, 2004 and May 6, 2005, the Navy established the Oracle Database Enterprise License, effective through Sept. 30, 2013. The enterprise license provides Navy shore-based and afloat users, to include active duty, Reserve and civilian billets, as well as contractors who access Navy systems, the right to use Oracle databases for the purpose of supporting Navy internal operations. Navy users in joint commands or supporting joint functions should contact Dan McMullan, NAVICP Mechanicsburg contracting officer, at (717) 605-5659 or e-mail daniel.mcmullan@navy.mil, for further review of the requirements and coverage.

This license is managed by the Space and Naval Warfare Systems Center (SPAWARSYSCEN) Pacific DON Information Technology (IT) Umbrella Program Office. The Navy Oracle Database Enterprise License provides significant benefits, including substantial cost avoidance for the department. It facilitates the goal of net-centric operations by allowing authorized users to access Oracle databases for Navy internal operations and permits sharing of authoritative data across the Navy enterprise.

Programs and activities covered by this license agreement shall not enter into separate Oracle database licenses outside this central agreement whenever Oracle is selected as the database. This prohibition includes software and software maintenance that is acquired:

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

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

Web Link:
http://www.public.navy.mil/usff/itumbrella/Pages/AllDocuments.aspx

Data at Rest Solutions BPA - Navy Agreement only

The DON CIO has issued an enterprise solution for Navy users purchasing DAR software. Visit the DON CIO website at www.doncio.navy.mil and search for "Data at Rest" to read the new policy. The DON awarded MTM Technologies a BPA for purchase of the DON Mobile Armor software bundle. For Navy users, all purchases of DON enterprise DAR solutions must be executed through the enterprise BPA, which can be found on the DON IT Umbrella Program website at www.it-umbrella.navy.mil. Procurement of other DAR solutions for Navy users is prohibited.

Navy Enterprise BPA for DAR Users:

Mobile Armor – ***MTM Technologies, Inc.*** (N00104-09-A-ZF30)

Web Link:
http://www.public.navy.mil/usff/itumbrella/Pages/AllDocuments.aspx

Need Help?

The DON IT Umbrella Program offers great customer service – Go to the Websites below for assistance

Enterprise Cost $avings for your command and the departments of the Navy and Defense are just a click away

www.public.navy.mil/usff/itumbrella/Pages/AllDocuments.aspx

www.esi.mil

www.chips.navy.mil

or

www.public.navy.mil/usff/chips/Pages/default.aspx

Visit our e-commerce site www.itec-direct.navy.mil for your technology needs

West Coast DON IT Conference

San Diego Convention Center

January 24-27, 2011

Go to the DON CIO website: www.doncio.navy.mil for details

DEPARTMENT OF THE NAVY
COMMANDING OFFICER
SPAWARSYSCEN ATLANTIC
CHIPS MAGAZINE
9456 FOURTH AVE
NORFOLK, VA 23511 - 2130
OFFICIAL BUSINESS

PERIODICAL POSTAGE AND
FEES PAID NORFOLK, VA AND
ADDITIONAL MAILING OFFICE
SSC ATLANTIC
CHIPS MAGAZINE
USPS 757-910
ISSN 1047-9988