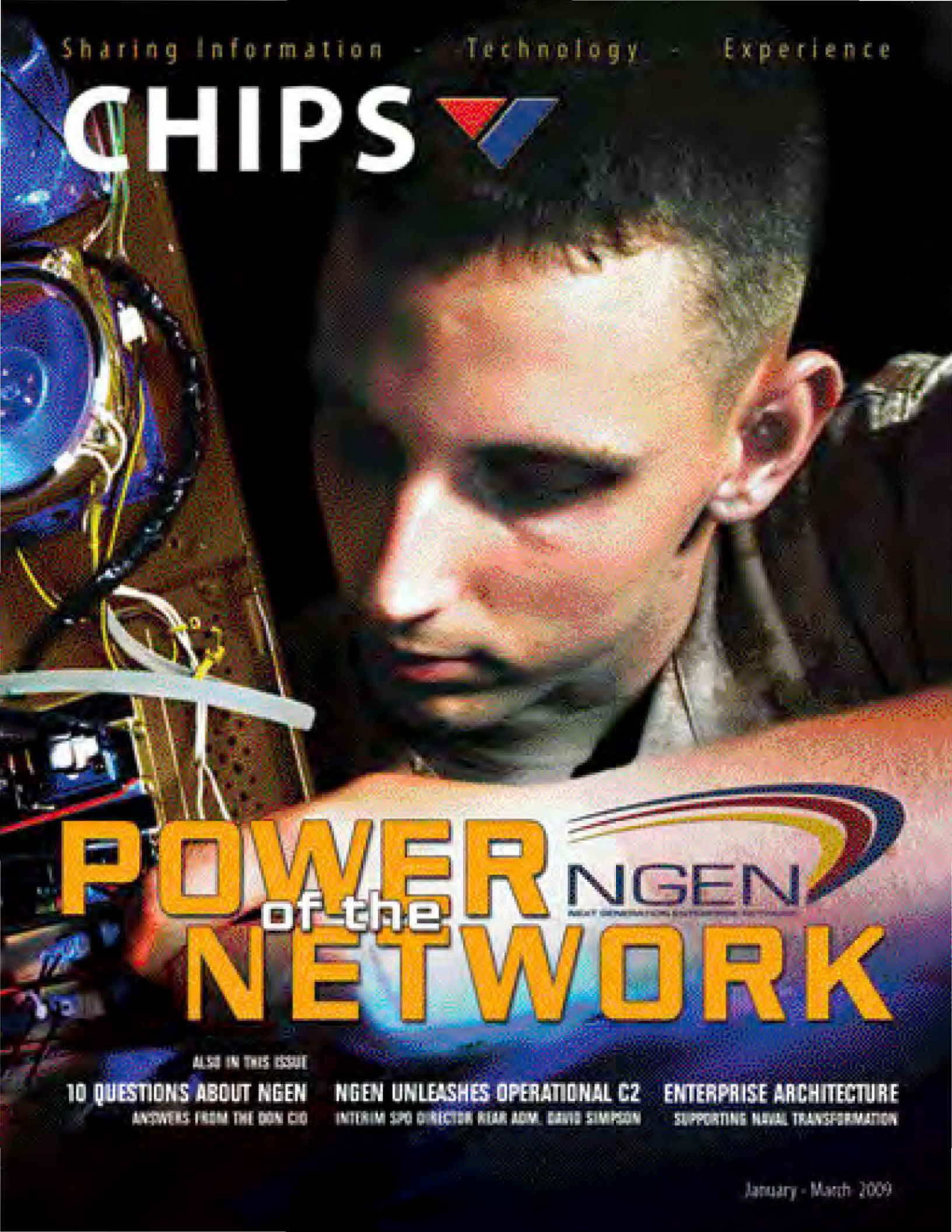
Sharing Information - Technology - Experience

CHIPS



POWER of the NETWORK

NGEN

ALSO IN THIS ISSUE

10 QUESTIONS ABOUT NGEN
ANSWERS FROM THE DON CIO

NGEN UNLEASHES OPERATIONAL C2
INTERIM SPO DIRECTOR REAR ADM. DAVID SIMPSON

ENTERPRISE ARCHITECTURE
SUPPORTING NAVAL TRANSFORMATION

January - March 2009

CHIPS January – March 2009

Volume XXVII Issue I

Department of the Navy Chief Information Officer
Mr. Robert J. Carey

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

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 – Deborah Midyette – DON IT Umbrella Program

Don't miss a single issue of CHIPS! To request extra copies or send address changes, contact CHIPS editors at chips@navy.mil or (757) 444-8704, DSN 564.

Statement of Ownership, Management and Circulation

The U.S. Postal Service requires all publications to publish a statement of ownership, management and circulation.

Date	1 October 2008
Title of Publication	CHIPS
Title of Publisher	U.S. Navy
USPS Publication Number	ISSN 1047-9988
Editor	Sharon Anderson
Frequency of Issue	Quarterly
Owner	U.S. Navy
Total No. of Copies Printed	32,700
No. Copies Distributed	32,335
No. Copies Not Distributed	365
Total Copies Distributed and Not Distributed	32,700
Issue Date for Circulation	October-December 2008
Location of Office of Publication	SPAWARSYSCEN Atlantic CHIPS Magazine 9456 Fourth Ave Norfolk, VA 23511-2130

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

Requests for distribution changes or for other assistance should be directed to Editor, CHIPS, SSC Atlantic, 9456 Fourth Ave., Norfolk, VA 23511-2130, or call (757) 444-8704; DSN 564. E-mail address: chips@navy.mil; fax (757) 445-2103; DSN 565. Web address: www.chips.navy.mil/..

Features

6 Department of the Navy Chief Information Officer Robert J. Carey answers the top 10 questions about the department's Next Generation Enterprise Network, or NGEN

8 Director Navy Networks Rear Adm. David G. Simpson responds to questions about NGEN governance and command and control

11 NGEN Program Manager Capt. Timothy Holland outlines the reasons for the NGEN evolution and the need for better security and global connectivity

14 Commander, Regional Maintenance Centers Rear Adm. J. Clarke Orzalli describes the work of the RMCs in support of fleet customers

Navigation Guide

Editor's Notebook

Happy Safe Networking! So says longtime CHIPS author, retired Air Force Maj. Dale J. Long, in this issue's installment of the "Lazy Person's Guide." You may be amused by the reference to Happy Safe Networking instead of the traditional Happy New Year greeting, but think of how miserable we are when the network is down or working at less than optimal performance, or worse yet, there has been a security violation.

It isn't just a matter of inconvenience. When you think of the national security data, proprietary data and Department of the Navy intellectual capital that ride on DON networks, security becomes the single most important factor in naval operations.

When you consider what is at stake, we should be inspired, not disheartened, and approach network security as an opportunity to innovate new solutions, not only to defend and secure DON networks, but at the same time to take advantage of technologies that help us do our jobs better, make the nation more secure and empower the warfighter on the pointy end of the spear.

With inspiration and innovation in mind, we take a close look at the Next Generation Enterprise Network, the follow-on to the Navy Marine Corps Intranet. NGEN will replace the NMCI with better security, flexibility to embrace new technologies and, most importantly, allow the network to truly become a command and control node in the naval arsenal, according to DON leadership.

But the best network security in the world will fail — if we become careless. Not surprisingly, users are the weakest link in network security. In this issue, Dale Long takes a look at social engineering — that insidious, ever-present collection of scams, hacks and schemes that tricks users into providing information that aids cyber terrorists in infiltrating DoD and DON networks. Security studies indicate that increasingly these attacks are politically motivated, and not just attempts to extort money or steal personally identifiable information, such as Social Security and credit card numbers.

The statistics are bone-chilling! For more information about social engineering techniques and ways to protect yourself and the network, go to the U.S. Computer Emergency Readiness Team Web site at www.us-cert.gov and the Department of the Navy Chief Information Officer Web site at www.doncio.navy.mil.

In November, the CHIPS staff joined Team SPAWAR in an exhibit that showcased the C4I products and information technology systems that Team SPAWAR engineers for the warfighter at the MILCOM conference. Thanks to those readers who stopped to say hello.

Welcome new subscribers!

Sharon Anderson

Team SPAWAR exhibit at MILCOM 2008 at the San Diego Convention Center Nov. 17-19, 2008. Team SPAWAR participants included SPAWAR Systems Centers Pacific and Atlantic, SPAWAR headquarters, Program Executive Office Space Systems, PEO Enterprise Information Systems (EIS), PEO Command, Control, Communications, Computers and Intelligence (C4I) and JPEO Joint Tactical Radio System (JTRS).

Hope to see you at the West Coast DON Information Management/Information Technology (IM/IT) Conference Feb. 10-13, 2009, at the San Diego Convention Center. The DON CIO is hosting the IM/IT Conference at the same time and location as West 2009, a conference sponsored by AFCEA International and the U.S. Naval Institute. To register for the conference and for more information, go to the DON CIO Web site at www.doncio.navy.mil.

Information sharing has long been a hallmark of information technology. We have proven its worth on the battlefield as directly contributing to the commander's ability to make more agile and better decisions. More than ever before, information has to be shared securely with those who need it — across the Department of the Navy (DON), throughout the Department of Defense and with other government agencies, coalition and allied partners. Therefore, our days of living in stove-piped or silo environments are over. A net-centric strategy with interconnectivity of our networks has enabled increased access to information, but we must always be mindful to balance access with security. This balancing act is the premise of information assurance, which combines information security with information availability, and it has become vitally important in this information age.

Protecting networks and information, especially in the face of the ostensible popularity of malware and cyber terrorism, has become a challenge for all federal agencies. The DON has made great strides in this area over the last several years. The Navy Marine Corps Intranet (NMCI) was the launching point for the greatly enhanced security posture of the nearly 700,000 Sailors, Marines and civilians who rely on it. Each month it blocks approximately 9 million spam messages and detects more than 1,200 intrusion attempts and an average of 60 viruses before they can infect the network. NMCI has implemented and enforced the DoD Public Key Infrastructure (PKI) cryptographic logon (CLO) mandate; usernames and passwords have been replaced by the use of DoD PKI to cryptographically log on to DON networks.

In addition to the security enhancements afforded by NMCI, the department has improved security through the use of public key-enabled Web sites and role-based access. Most of these enhancements require no more effort for the user than logging on to the computer using CLO, but the benefits are immense. Using PKI, users can access secure Web sites, digitally sign forms, and encrypt and digitally sign e-mails. BlackBerry users can now use secure Bluetooth BlackBerry Common Access Card readers for digital signature and encryption capability, to ensure the proper protection of information contained on those devices which are simply an extension of our networks. While this may seem to be a burdensome layer, adding to the time it takes to respond to e-mails securely, it is worth it.

Some of the areas in which the department has beefed up security are not as transparent as the NMCI/CAC/PKI solutions. These include encryption of data at rest (DAR) and the decision to block access to sites such as Gmail, YouTube, Second Life, Hotmail and Yahoo mail to decrease the likelihood of network vulnerabilities.

Encrypting data at rest is a solution that responds to the loss of personally identifiable information (PII) — the information that can be used to identify and steal the identity of a Sailor, Marine or DON civilian and wreak financial havoc. Identity theft is a real and growing trend that we must take seriously. There are three main types of media that are vulnerable to loss: hardware, which usually translates to the loss or theft of laptops or thumb drives; paper, which is usually the loss of PII printed on paper; and electronic, which is the erroneous posting of PII on Web sites or contained in e-mail.

We must take every precaution necessary to minimize the amount of PII collected and shared, and make it accessible to only those with a need to know. We have implemented a number of policy initiatives designed to modify behavior and improve privacy awareness across the DON. However, our DAR effort is also important in protecting DON sensitive information which includes more than PII.

As we move from NMCI to the Next Generation Enterprise Network (NGEN), protection of our networks and information will continue to be a priority. The threat environment to IT networks has changed significantly over the last eight years since NMCI was implemented. The NGEN design and operations will be flexible enough to adapt and change with evolving threats and accommodate new technologies and capabilities as they become critical to operations.

Security will be a key component of all aspects of NGEN. Security will come from every user who connects; each of us is a cyber-warrior and must understand facets of IT never before required. This will be true for services and functions provided by industry, as well as those managed by the government. The government must have visibility into, and control of, network operations to ensure this critical asset is fully supporting user needs. Therefore, ultimate responsibility for security of DON networks will reside with the government.

We don't know what the next cyber security issue of significance will be. But just as the combination of NMCI and other solutions has successfully defended our networks up to this point, we are working to make sure that security under NGEN will be just as strong.

Robert J. Carey

Top 10 Questions about NGEN with answers from the DON CIO Rob Carey

The Department of the Navy Chief Information Officer, Robert J. Carey, is one of a group of high-level DON leaders planning for the implementation of the Next Generation Enterprise Network, or NGEN, the name used for the follow-on network to the Navy Marine Corps Intranet. The DON will transition to NGEN when the NMCI contract ends Sept. 30, 2010.

A well-recognized advocate of innovative technology tools and process models, Carey was among the first government executives to establish a blog and among the first to embrace the use of Web 2.0 tools to improve communication and collaboration within the DON CIO team and across the DON.

In a policy memo, Carey wrote that IT tools, including wikis, blogs and Web feeds, will give warfighters seamless access to critical information. The memo, issued Oct. 20, 2008, is available on the DON CIO Web site at www.doncio.navy.mil.

When CHIPS asked Mr. Carey to discuss NGEN, he responded to the top 10 questions that he is most often asked.

Q: Why are you going with a segmented approach to NGEN implementation?

A: The acquisition strategy for NGEN is still under development and hasn't been approved yet by the Department of the Navy, but we are aligning the work necessary to manage NGEN by segments. This means we may have one or more contracts to deliver the services needed to support the department's mission. This will be decided once we complete the Analysis of Alternatives (AoA), the output of which will feed the acquisition and subsequent contracting strategy.

We studied the ITIL (Information Technology Infrastructure Library) process and believe it is the most logical way to proceed. Our research indicates that a segmented approach has become an industry best practice over the last few years. Segmenting the work provides greater flexibility for the government and increased opportunities for industry to compete to provide NGEN services.

Q: How did you decide on what functions to keep in house and what to outsource. Is security outsourced?

A: We have developed notional schemes of what functions will be directly performed by government personnel and those that will be accomplished by contractors. All of those final decisions will be informed by the AoA and the acquisition strategy selected.

Q: What are some of the major lessons learned from the NMCI, and how will you apply those lessons in NGEN?

A: Some of the most important lessons learned were the things that worked well with NMCI. For example, NMCI provided the department with a true enterprise network. It eliminated the 'haves and have-nots,' and provided nearly 700,000 DON users the necessary IT capabilities to perform their critical missions and functions. In addition, it provided an interoperable capability across our enterprise, facilitating the sharing of data, information and services. Most importantly, it allowed us to gain consistent control of the information assurance/computer network defense posture of our largest enterprise IT network.

On the downside, the contract language for NMCI did not allow us to respond as quickly to emerging requirements; making changes became a contract negotiation. We've learned that lesson, and NGEN will take us to where we'll have ownership of the network. We also learned that we can't treat this network as if it were a weapon system; we must treat it as part of the critical infrastructure necessary to execute our mission.

The threat to IT networks has changed significantly over the last eight years and the world of IT changes at a rapid pace. This means that the NGEN design and operations must be flexible enough to keep pace with the ever evolving security threat and flexible enough to adapt to the reality of rapidly changing IT.

Q: How will the changeover to NGEN be accomplished?

A: The transition from NMCI to NGEN must be accomplished in such a way as to ensure continuity of service across the enterprise. Therefore, the transition will be performed in a well thought out and executed manner.

The highest levels of the DON have been fully engaged in development and approval of the plans for NGEN, and the department recently established a System Program Office to coordinate the activities associated with bringing NGEN to fruition. The establishment of this new organization demonstrates the DON's commitment to making the transition to NGEN successful, with no opportunity for a gap in this critical service.

Q: How difficult will it be to extend NMCI/NGEN to warships at sea?

A: The scope of the initial block of NGEN will be identical to that of NMCI. It will provide network and computing services to more than 700,000 DON users located within the continental United States and at select locations overseas. It will not provide services directly to afloat users.

Afloat users will be provided services by the Integrated Shipboard Network System, ISNS, and its follow-on, the Consolidated Afloat Networks and Enterprise Services (CANES).

We want to make sure CANES and NGEN are interoperable through implementation of common technical standards, business processes and well-defined interfaces.

Q: What training will be needed for NGEN use and maintenance?

A: From the end-users' perspective, the transition from NMCI to NGEN will be almost transparent. As you know, network security is paramount to the success of the Navy-Marine Corps team, so we can expect each user to become a cyber warrior, armed with the knowledge of what it takes to protect and defend information.

The government personnel required to control network operations of NGEN will undergo function-specific training initially, and periodically as required, to maintain proficiency in their particular position. The major areas of training will include network operations, security operations and service life-cycle management.

Q: What other aspects of Navy IT will be affected by the move to NGEN? What upgrades to hardware and software will be needed?

A: As the department prepares for the transition to NGEN we will focus on three areas: (1) continuing to make necessary improvements to the capabilities provided by NMCI; (2) continuing to eliminate redundant legacy network environments; and (3) moving toward the procurement of software and hardware as an enterprise commodity. This will better prepare us for NGEN to be the true DON enterprise-wide network.

NGEN will inherit the NMCI capabilities at the end of the NMCI contract; therefore, no new hardware or software will be required as part of the initial rollout of NGEN. But similar to NMCI, NGEN will undergo a continuous process of technology refresh, for both hardware and software.

As we implement subsequent 'blocks' of NGEN and as we head toward our vision of a future Naval Networking Environment (NNE), it is likely that new hardware and software will be required to achieve these capabilities. We are in the process of defining a roadmap for achieving the future NNE to include what improvements need to be made in what years, and developing the resources to accomplish these interim goals. This roadmap will identify the convergence and alignment of IT investments across the department to support this vision and strategy.

Q: Will NGEN provide a mechanism to find personnel in the other services via e-mail to really connect a joint force?

A: A limited version of this capability already exists across the Department of Defense, with the Joint Enterprise Directory Service. NMCI today, and NGEN in the future, will be fully compliant with the JEDS standard, which allows the DoD to continue to migrate toward a true enterprise e-mail and directory service capability.

Q: Will the NGEN be structured so that users can take advantage of new technologies, like Web 2.0, when they come along?

A: The department embraces the use of Web 2.0 collaboration and working from anywhere we can connect to the network. Web 2.0 does not use new technologies; it is primarily different applications of current technology. Web 2.0 tools present many opportunities for collaboration and information sharing that support becoming a transparent organization, and they are becoming vital to keeping pace in today's environment. So yes, the NGEN infrastructure will support it, just like the NMCI infrastructure today supports it.

My hope is that commands will come onboard and fully exploit the use of Web 2.0 commensurate with necessary security requirements. I mention security because the implementation of any new tools in the DoD requires a cautious risk management approach for ethical use and to protect the confidentiality, integrity, and availability of the data.

Q: Will the DON be able to take advantage of the DoD-wide Enterprise Software Initiative and federal SmartBUY licensing agreements or other cost-saving strategies that support large volume buys to acquire software and services for NGEN?

A: Yes, all DoD Enterprise Software Initiative and SmartBUY Enterprise Software Agreements are available for use under NGEN. The scope of the ESAs, as well as regulation and policy, are all written to enable and encourage their use regardless of the NGEN strategy. CHIPS

Interview with Rear Adm. David G. Simpson
Director, Navy Networks
Deputy Chief of Naval Operations Communication Networks (N6)


Rear Adm. David G. Simpson

Rear Adm. Simpson was named the interim Assistant Chief of Naval Operations Next Generation Enterprise Network (NGEN) and Director of the NGEN System Program Office. The SPO is a new ACNO position created by the Secretary of the Navy, the Chief of Naval Operations and the Commandant of the Marine Corps on Oct. 15 to ensure that NGEN is developed with strong central governance from an office serving as the single focal point for policy, resources and requirements, acquisition, and technical authority and operations.

ACNO NGEN will work directly with the Department of the Navy Chief Information Officer (DON CIO), OPNAV N6, Headquarters Marine Corps (HQMC C4), Program Executive Office Enterprise Information Systems (PEO EIS), PEO C4I, Space and Naval Warfare Systems Command (SPAWAR), Marine Corps Systems Command (MARCORSYSCOM), Naval Network Warfare Command (NNWC) and Marine Corps Network Operations and Security Command (MCNOSC) to field and sustain a reliable and secure network that is responsive to Navy and Marine Corps warfighter needs, as well as the needs of the overall DON workforce.

Rear Adm. John W. Goodwin has been named ACNO NGEN and will arrive in January to fill the two-star director billet. ACNO NGEN will be responsible for delivery of Navy and Marine Corps enterprise network capabilities.

Rear Adm. Simpson will continue to support NGEN, leading the Navy's NGEN resources and requirements efforts from his position as Director of Navy Networks on the OPNAV N6 Staff.

NGEN will replace the Navy Marine Corps Intranet (NMCI) and many of today's legacy terrestrial networks for which NMCI was not well suited. Since its inception, NMCI has produced a very capable enterprise network that has provided both the Navy and Marine Corps a solid enterprise foundation from which to build NGEN.

NMCI transformed Naval network services starting with the initial NMCI contract award in October 2000 and has improved customer satisfaction each year. With nearly 700,000 active users and a wide range of information technology services available, NMCI is the largest corporate intranet of its kind. NMCI has greatly improved the ability of the Navy and Marine Corps to centrally manage information technology service, control IT spending — and provide strong security.

Rear Adm. Simpson has been working on the requirements for NGEN with Navy and Marine Corps stakeholders within the DON since his assignment to OPNAV N6 in the spring of 2008. The acquisition approach is notional at this stage because an Analysis of Alternatives, directed by the Secretary of Defense, is currently in progress.

Respecting the competition sensitive nature of some of the finer details, CHIPS asked the admiral to discuss some of the high level plans for NGEN.

Q: According to the NGEN program office, the NGEN acquisition approach will be based on a notional segmentation concept that breaks existing network functions into groups and separate services so that some may be run by the Navy and others may be outsourced. Will the Navy be the integrator for the segmented services?

A: IT services under NGEN will be managed using the IT Infrastructure Library (ITIL) version 3, Service Delivery Model. This industry-developed, open standard framework is being used to define each of the processes and interfaces associated with the delivery of NGEN services. Responsibility for a given process and/or interface will be defined in concert with the Service Design Specification.

ITIL v3 is organized into Service Strategy, Design, Transition, Operations and Continuous Improvement processes. Both the Navy and Marine Corps will have process owners for each of the high level NGEN processes. NGEN Service Operations leads will be the Naval Network Warfare Command for Navy and the Marine Corps Network Operations and Security Command for the Marines. These organizations will have command and control responsibilities for the end-to-end provision of network service working closely with the supporting military, government and contract team.

The program manager for NGEN is working closely with DON stakeholders and industry to define integration requirements as part of the ITIL Services Management framework.

During the requirements generation phase, the NGEN team spoke with CIOs from several large corporations that successfully balanced in-source/outsource segmentation to understand the value in that service delivery model. There is a good body of

"Every attempt at network intrusion, whether it is successful or not, provides a network attacker useful information. In order to stay ahead of the threat, DON networks must *learn* from each attempted intrusion or attack and improve our defense."

Rear Adm. David G. Simpson
Director Navy Networks

knowledge for industry best practices that we want to emulate.

We are currently working through the process of determining if there is a smart grouping that would suggest a number of segments or a single segment covering all those functions. We are looking at that trade space to see what will work best for the department and its IT partners.

Q: The Department of the Navy has determined that it must exert greater oversight and direct control of the design and operations of NGEN. Why?

A: To meet the command and control needs of our personnel, the DON must have operational and design control of our networks. This refers to the assignment of priorities, direction and policies within an accountable framework with well-defined standards, policies and enforcement mechanisms.

Naval IT networks must have exceptionally high levels of agility and flexibility in order to keep pace with evolving mission challenges and an ever-increasing cyber threat. A strong central governance is required to ensure that decisions impacting a wide range of DON stakeholders can be made quickly, in response to changes in the network environment.

Networks represent a significant investment for the department, one that requires a daily balance between provision of service and affordability. Navy and Marine Corps command and control of NGEN will provide the strong governance necessary within a supported/supporting commander structure led by Navy and Marine Corps NETOPS forces, aligned operationally underneath U.S. Strategic Command's Joint Task Force-Global Network Operations (JTF-GNO), and Navy and Marine Corps service components.

Q: Some in the DON would say that the "network is a weapon." What will NGEN deliver to operational commanders?

A: First and foremost, the network must deliver robust, reliable communications between commanders and supporting forces. NGEN will do this as a military capability with a government workforce ready to defeat potential adversaries who would seek to deny or exploit Navy and Marine Corps network services.

Every attempt at network intrusion, whether it is successful or not, provides a network attacker useful information. In order to stay ahead of the threat, DON networks must *learn* from each attempted intrusion or attack and improve our defense.

NGEN will include a robust security operations segment that will work within Navy and Marine Corps computer network defense organizations, coordinating closely with JTF-GNO and [STRATCOM's] Joint Functional Component Command Network Warfare (JFCC-NW) to proactively address cyber threats.

Q: How will NGEN address the needs of the fleet? Will NGEN support deployed Marines and Navy individual augmentees?

A: NGEN will be the foundation for the Naval Networking Environment. It will introduce a consistent set of operational standards and services to provide warfighter and business IT capabilities across the fleet and Marine force.

NGEN will continue to provide embarkable IT assets for use afloat as well as tailored solutions for an increasingly mobile DON workforce. Over time this will include OCONUS networks as well as shared services between the afloat and shore environments.

Currently, individual augmentees will continue to be supported by the network service provider of their assigned unit. NGEN will, however, ensure that commonly adopted standards for services and data are implemented across the DON to ensure interoperability with the rest of DoD, with other agencies, and with our coalition partners.

Future NGEN increments will seek to deliver capabilities required to realize the Chairman of the Joint Chiefs of Staff Global Information Grid 2.0 vision for global joint warfighter access to network services on any part of the GIG.

Q: With the Department of the Navy's plan to retain control and oversight of NGEN within the Navy and Marine Corps, are there plans under development to determine what skill sets and types of civilian and military billets are needed to operate and maintain the new network?

A: A fully trained and qualified government workforce is an essential part of the DON's NGEN implementation. The billets and positions are resourced in the Future Years Defense Program (FYDP) and the demand signal captured in the respective service Total Force Manpower Management System.

ACNO NGEN is working closely with N1, HQMC C4 and DON civilian human resources specialists to define the required skill sets and generate recruitment, hiring and training plans to deliver a capable NGEN government workforce on time.

Q: Given that NMCI is owned and operated by the current contractor, how will the DON ensure that EDS does not have an unfair competitive advantage?

A: The DON is working to ensure a level playing field. NGEN will utilize an open standard (ITIL) for the Service Delivery Model that should be widely recognizable to IT service providers. NGEN will continue to seek feedback from industry on the Service Design Specification and subsequent implementation plans.

NGEN will continue to provide as much information as is allowed to educate potential vendors on DON requirements for NGEN while respecting the acquisition sensitive nature of the program.

Q: What should the current nearly 700,000 users of the NMCI understand about moving to NGEN? Is there anything that NMCI users can do to prepare for the transition?

A: Current NMCI users should understand that continuity of existing service is the No.1 priority for NGEN. There will not be a flip of a switch on Oct. 1, 2010, with a 'hard' cutover. Instead, NGEN will employ a conservative transition plan to assume operation of the current NMCI environment, develop the DON NETOPS workforce, and introduce NGEN ITIL structured services operated by a military, civilian, contractor team.

Planning for the transition is underway. Early transition activities are being defined to ensure continuity of service throughout the process. Users should continue to participate in required network security training and work with their claimant's techical representative and assistant CTR to understand changes in network governance as we get closer to the transition period.

Q: Will the department be able to take advantage of the DoD-wide Enterprise Software Initiative and federal SmartBUY licensing agreements to acquire software and services for NGEN?

A. Yes. Use of ESI, where it makes sense, is an NGEN goal. Specific utilization will be determined by the acquisition strategy.

Q: The SPO will also be working to consolidate legacy networks. What types of networks are remaining and will their functions be part of NGEN?

A: Through operation Cyber Asset Reduction and Security (CARS), the Navy has made significant progress in the last two years in lowering the number of Navy legacy networks from over 1,000 to fewer than 500. The NNWC-led CARS team has set a goal to reduce an additional 200 networks in 2009, and eliminate the rest of the legacy environment in 2010.

More significantly, CARS has led Navy's efforts to improve the security environment for both enterprise and 'excepted' Navy networks. Recent response to DOD-wide security threats proved the value of this program as Navy was able to rapidly develop an effective response through CARS implementation.

Both Navy and the Marine Corps benefited from their strong commitment to enterprise-wide networks with service-wide implementation of directed information assurance achievable in a minimum amount of time.

The Naval Networking Environment will continue to include a number of excepted networks requiring some degree of isolated access or unique technical capabilities, but we will ensure that they are as vigilantly protected and efficiently operated as our enterprise network. Similarly, the DON will continue to work to reduce legacy applications, databases and data centers.

This is an exciting time for naval networks with both NGEN, the Marine Corps Enterprise Network (MCEN), and the Consolidated Afloat Networks and Enterprise Services (CANES), delivering improved security and warfighting capabilities across the DON operational spectrum.

The department will build upon the Naval Networking Environment to meet the increasing cyber threat, empower Millennial Sailors and Marines, and produce a consistent collaborative information environment across the fleet and Marine force.

Go to Navy News Service at www.navy.mil and click on the Navy Leadership link to view Rear Adm. Simpson's biography. CHIPS

CNO Names Next Generation Enterprise Network Chief

By Eddie Riley – NGEN Public Affairs

On Nov. 20, Chief of Naval Operations Adm. Gary Roughead named the commander of Naval Air Force Atlantic to lead the Department of the Navy's largest, enterprise-wide IT initiative as the new Assistant Chief of Naval Operations for the Next Generation Enterprise Network System Program Office. As ACNO (NGEN), Rear Adm. John W. Goodwin will oversee the DON's development, acquisition and deployment of NGEN — the follow-on to the Navy Marine Corps Intranet contract that ends Sept. 30, 2010.

The NGEN SPO, a first-of-its-kind organization in the DON, was approved by the CNO and Commandant of the Marine Corps earlier this year. It brings together the DON's governance areas for NGEN — policy, resources and requirements, acquisition, and fleet readiness, support and operations — under a single command. The elevated coordination at the ACNO level will ensure stakeholders are included in the design and implementation process and help facilitate a smooth transition from NMCI to NGEN with continuity of services to end users.

The SPO includes all of the functions of the existing NGEN, NMCI and OCONUS Navy Enterprise Network (ONE-NET) program offices. The SPO resides within the Navy staff, leveraging the institutional support of both CNO and Headquarters Marine Corps staffs.

Goodwin will join the NGEN SPO in January. Interim ACNO (NGEN), Rear Adm. David G. Simpson, will lead the SPO until Goodwin arrives. Simpson continues to set the foundation as the NGEN resource sponsor in his assigned position as the director of Navy Networks on the deputy chief of Naval Operations for Communication Networks (OPNAV N6) staff. Marine Corps Col. David M. Hagopian will continue to serve as the deputy director, NGEN SPO.

The NGEN initiative is focused on re-establishing government design and operational control over Naval networks, creating a more secure and agile intranet, and recruiting and developing the future Naval IT workforce. It is a central pillar in the department's goal of building the Naval Networking Environment (NNE), the DON's vision for a highly secure reliable enterprise IT system that provides ready access to data, services and applications when and where needed.

The NGEN SPO will coordinate continued service for existing shore and garrison networks, including NMCI; support consolidation of legacy networks; and direct the transition to NGEN while providing implementation oversight to enable enhanced capabilities within the future NNE by 2016.

The NGEN initiative is currently in the pre-decision phase with a requirements document approved earlier this year by the CNO and CMC. A system specification, currently under development, will further define the required system functions and performance parameters. The acquisition approach, currently under draft, is expected to be based on a notional segmentation concept that breaks existing network functions into groups and separates services into those that may be run by the DON and others that could be outsourced.

Under the current NMCI contract, network services are provided by one prime contractor. The DON has released four Requests for Information and held one industry day to get feedback from the information technology community on the NGEN initiative.

– Edited from Navy News Service Dec. 2, 2008

10 • 1 • 10 – The Evolution Begins

A new era in command and control expeditionary networking

By Capt. Timothy Holland

If you work in or with the Department of the Navy (DON), two years or so from now, you will be using a new intranet to conduct business. The current Navy Marine Corps Intranet contract ends Sept. 30, 2010. On Oct. 1, 2010, the DON will be transitioning to the Next Generation Enterprise Network (NGEN).

Currently, every NMCI user is provided a complete suite of applications and services at each "seat" — consisting of connectivity to local area networks, wide area networks, guaranteed network performance, security, network support, all help desk support, training, cryptographic logon, identity management and attribute-based access. The combination of this set of services has tremendous value.

The current design provides secure, universal access to integrated voice, video and data communications, and a common computing environment across the DON, which has played a critical role in dramatically improving security across the enterprise while greatly improving business efficiency and the exchange of information.

Innovation, Security and Global Connectivity

With NGEN, the DON's vision is to transition to a network that will have a secure, reliable capability that capitalizes on its significant investment and improves focus on the warfighter. This will be accomplished by first enabling command and control (C2) of naval network resources, and second, by improving Navy enterprise business and administrative functions.

NGEN, over time, will provide a state-of-the-art, global networking environment that is responsive to the operational commander, that unleashes the collaborative nature of the Millennium Generation and empowers our future warriors. It will build on the lessons learned in developing the world's largest intranet, the NMCI, and allow visibility into the network's control and cost to help the DON migrate from costly, vulnerable legacy networks.

NGEN represents the evolution of naval IT networks. It is a central pillar in the DON's goal of a single-enterprise network within the overall Naval Networking Environment. The NNE 2016 is the DON's vision for a highly secure and reliable enterprise providing ubiquitous access to data, services and applications from anywhere across all program and operational boundaries. The NNE is an iterative set of integrated, phased programs that will guide the DON toward a future net-centric enterprise environment.

The NNE will be bound by an enterprise architecture, common standards and a common governance and operational construct that is consistent with the joint goals for Defense Department-wide access to information technology services around the world.

It will allow U.S. Naval forces to partner, communicate and share information with a diverse array of multinational, federal, state, local and private sector organizations given a particular operational requirement tailored to a specific mission.

Over the next two years, and at the initial delivery of NGEN, you won't notice much change. There will not be a flip of a switch Sept. 30, 2010, when the NMCI contract ends. Users will still have access to current systems and tools, but NGEN will be well on the way to realizing needed improvements.

Capt. Timothy Holland
NGEN Program Manager

Why change?

Since 9/11, the requirements of the commands currently supported by NMCI have changed as the department engaged in the global war on terror. Shore-based and forward operational commanders in the fleet view all of the DON's enterprise networks as extensions of their ability to wage war and have stated that coalition and multinational command, control, communications and computers (C4) interoperability remains the top fleet priority.

There are compelling reasons to move to NGEN, NNE 2016 — and beyond — as outlined below.

✓ To make DON networks better

Today, DON networks are no longer just a business support system. They must be built in ways that allow them to be interoperable across commands. Continuous improvement means constant evaluation of process and progress and making necessary changes to succeed. In other words, NGEN is part of the NNE strategy that will bring about the integration of multiple simultaneously moving pieces across the Navy and Marine Corps.

The keys to the success of NNE 2016 are:

- A common enterprise architecture;
- Adoption of and adherence to enterprise standards, including the use of enterprise purchase agreements for our most common hardware and software components used across the department;
- A common governance structure and operational construct;
- Access for Sailors, Marines and civilians who should not be administratively bound to any one computer seat. With their Common Access Card and proper authorizations, they should be able to sit down at any personal computer or computing device and log in to receive "their" information with access to their data;
- Shared services; and
- Common IT service delivery across the operational spectrum.

Shore-based and forward operational commanders in the fleet view all of the DON's enterprise networks as extensions of their ability to wage war and have stated that coalition and multinational C4 interoperability remains the top fleet priority ...

✓ To support the warfighter

The job of naval networks is to deliver mission-critical information to DON personnel when and where they need it. Warfighters will have the ability within the NGEN footprint to execute assigned missions and exercise command and control. At the same time, NGEN will defend the cyber domain by defeating ever increasing cyber threats with a military capability designed to fight, win and prevent cyber attacks.

NGEN will provide service for a number of warfighting and Navy corporate activities. It must support an embarkable category of users, such as Sailors and Marines, whose in garrison command location is ashore.

Embarkable users need to be able to transition seamlessly to Navy's afloat IT environment without loss of identity or functionality. Marine Corps expeditionary users similarly need to transition seamlessly from garrison to the fight forward within a consistent IT environment.

The DON has expeditionary NGEN users who need to be supported over low-bandwidth connections, and the DON has numerous users with challenging mobile requirements. Think of Navy recruiters who travel hundreds of miles to high schools and storefront locations, they need their information to be available and accessible while traveling.

While not in the first increment, the DON will want NGEN to help achieve a better balance between security and the need for a few Navy users to have broader Internet access to take full advantage of emerging technologies, in addition to social and business Web technologies. A layered defensive strategy will be an important characteristic of NGEN service.

Our service men and women need to know that the DON supports them and that its Naval Networking Environment allows them to do their job effectively without interruption.

✓ To ensure optimum security

Modern day conflicts are increasingly moving from the traditional battlefield to cyberspace. Due to ever-increasing cyber threats and the military's increasing dependency on IT infrastructure, continuous security improvements are required to protect against this insidious threat. A security failure could result in a loss of credibility, capital — or worse — lives.

Security refers to assured information sharing; network defense; confidentiality; a high rate of available enterprise access; assured mission management; integrity; and non-repudiation of data and users.

The DON is dedicated to protecting, defending and safeguarding information and information systems (including networks and applications) by ensuring their availability, integrity, authentication, confidentiality and access control through technical, managerial and operational means.

Cpl. Michael K. Kono is on his second deployment in support of Operation Iraqi Freedom. A computer network administrator, Kono is in charge of constantly updating the security of the networks and making sure the base's air boss is always able to contact other bases to coordinate 2nd Marine Aircraft Wing's mission throughout Iraq. Marine Corps photo by Sgt. Juan Vara, 2nd MAW July 2005.

✓ Governance to operate and adaptability

To meet the command and control needs of DON personnel, the department must have operational and design control over naval networks. Governance refers to the assignment of decision rights and accountability framework (standards, policies and enforcement mechanisms) to encourage desirable behavior in the use of IT. Adaptability refers to the ability of our network to field new, modified or additional services in a timely manner at an agreed service level.

Department of the Navy IT contingencies must allow unprecedented agility and flexibility. NGEN governance is focused on creating a process for decision making in which all stakeholders, including leadership, internal customers and related areas, such as acquisition, have appropriate channels to provide necessary input. This mitigates problems and improves system performance, adaptability and cost effectiveness for the DON.

NGEN will use an IT Service Management (ITSM) framework based on industry best practices. Use of the Information Technology Infrastructure Library (ITIL) version 3 will allow the DON to apply an open standard that is consistent across the entire operational spectrum. It will allow the department to bring maximum competition to bear on specific functional segments of NGEN without detracting from end-to-end interoperability.

ITIL's systematic approach will bring a tested, rigorous, efficient service delivery model to DON network operations that is consistent with recognized international standards. It is a model that many of the DON's industry partners use.

ITSM is a discipline for managing IT systems centered on meeting an organization's requirements on the part of internal

Out of the box, NGEN must be at least as good as NMCI and must be capable of growing to meet warfighter needs ...

or external customers. The output is a strategy for the design, implementation, maintenance and continual improvement of the service as an organizational capability and a strategic asset.

ITIL is a set of concepts and techniques for managing IT infrastructure, development and operations. Processes are designed to be compatible with the requirements for performing IT service strategy, design, transition and operations functions that will result in the optimum service management infrastructure.

Since there is no existing DON standard for ITSM implementation, NGEN is leading the effort in implementing ITSM partnering with the Naval NETWAR FORCEnet Enterprise (NNFE) to develop and maintain an enterprise IT maturity model.

Embracing ITSM from the start of NGEN development will better position the Navy to manage life-cycle processes. We expect to have a consistent organization that captures requirements, delivers, monitors, optimizes and enhances IT service with a mature, coherent and transparent process.

✓ To ensure the utmost reliability

Department networks are mission critical. Preventing and rapidly responding to failures or breaches and building redundancies are essential. Reliability means that protected data is consistently available when needed. Reliability refers to the ability of the network to maintain operations at agreed service levels during normal operations, peak demands and disaster situations.

Out of the box, NGEN must be at least as good as NMCI and must be capable of growing to meet warfighter needs. It must be capable of providing assured information exchange for Navy's critical command and control nodes and key supporting command operations centers.

What is the risk of not moving to NGEN or NNE?

As the NGEN program manager, I must stress that NGEN signifies much more than how we buy information transport services; it is really about how the DON executes network operations across Navy and Marine Corps operational and business core mission areas.

As we move further into the millennium, network users will become more dependent on access to information. To ensure the DON stays ahead and prevents information dependence from becoming a liability, the department must practice continual service improvement.

NGEN is the first milestone in the evolution of Naval IT networks; it promises to deliver operational command and control, robust security and exciting technology innovations.

Capt. Timothy Holland is a 1982 graduate of the U. S. Naval Academy with a bachelor's degree in engineering and a master's of science degree from the Naval Postgraduate School. He reported to the Program Executive Office for Enterprise Information Systems as the NGEN program manager in June 2007. CHIPS

DON Releases Service Specifications for NGEN

By Eddie Riley – NGEN Public Affairs

The Assistant Chief of Naval Operations for the Next Generation Enterprise Network released the Draft NGEN Block 1, Increment 1 Service Specification document Dec. 4. This release is the most recent Department of the Navy industry interaction and builds on information previously provided during the NGEN Industry Day earlier this year.

The draft represents the DON's first articulation of an approach to implementing the NGEN environment. The document provides service specifications for the initial occurrence of NGEN, which is Block 1, in addition to the framework for how those services will be provisioned, managed and supported. The document is available by searching for "NGEN" on the Federal Business Opportunities Web site at www.fbo.gov.

The DON believes the specifications will establish a framework for the transition of services from the Navy Marine Corps Intranet to NGEN; specify performance measures for the delivery and provision of services; and define and allocate Information Technology Infrastructure Library (ITIL) functions that will facilitate the increased DON operational and design control desired in NGEN.

"This document deconstructs the Department of the Navy's NGEN requirements into an industry-defined open standard service delivery model. It identifies the processes and subprocesses for IT service strategy, service design, service transition, service operations and continuous service improvement using the ITIL framework," said Rear Adm. Dave Simpson, interim ACNO NGEN. "We would like to receive comments from interested industry partners on our representation of the process definitions, as well as their associated interfaces.

"This draft does not constitute a commitment by the government to acquire NGEN exactly as outlined in the document but will help us develop RFPs that are equally relevant to government and industry. The acquisition approach, specified services and allocation of ITIL functions are all still in development, and we'll adjust design specifications in the document based on input from industry," the admiral said.

Simpson also outlined DON's ramp-up for NGEN governance. "Rear Adm. John Goodwin has been named ACNO NGEN and will arrive in January to fill the two-star director billet. ACNO NGEN will solidify [the] DON's top-level governance for NGEN, bringing together the authorities for resources, requirements, policy, acquisition and operations into a single office. ACNO NGEN will be the sponsor responsible for delivery of USN and USMC enterprise network capabilities."

Simpson will continue to support NGEN, leading the Navy's NGEN resource and requirements efforts from his position as director of Navy Networks on the OPNAV N6 staff.

The opportunity for feedback and comments from industry partners on the draft service specifications closed Jan. 9.

The Navy and Marine Corps service chiefs approved the requirements for the NGEN program in April. This document is an interpretation of those requirements that NGEN stakeholders will approve in near-term. Industry should view the document as a demand signal for the resources and expertise required to operate and support the DON's primary enterprise network. Feedback will be valuable at this stage to validate the proposed Service Delivery Model prior to the DON's release of a formal request for proposal.

The next step for NGEN will be to turn the specifications into a statement of work and request for proposal(s).

Interview with Rear Admiral John Clarke Orzalli Commander, Regional Maintenance Centers

Rear Adm. John Clarke Orzalli

A Naval Academy graduate, Rear Adm. Orzalli is the commander of the Navy's Regional Maintenance Centers (CRMC). He holds a Bachelor of Science degree in marine engineering and master's degrees in materials science and engineering and systems management from the Massachusetts Institute of Technology and Golden Gate University, respectively.

CRMC was established in 2007 to manage the seven Regional Maintenance Centers located in fleet concentration areas worldwide. The Atlantic Fleet RMCs are located in Norfolk, Va.; Mayport, Fla.; and Ingleside, Texas. The Pacific Fleet RMCs are located in Pearl Harbor, Hawaii; San Diego, Calif.; Yokosuka, Japan; and Bremerton, Wash.

RMCs combine the waterfront activities involved in ship repair into a single maintenance enterprise to increase fleet readiness, improve ship maintenance processes and reduce costs to the Navy. The consolidation merged the functions of the repair Supervisors of Shipbuilding (SUPSHIPs), Readiness Support Groups (RSG), Shore Intermediate Maintenance Activities (SIMAs), Fleet Technical Support Centers (FTSCs) and port engineers.

This consolidation enables the RMCs to leverage the strengths of the different organizations in work brokering and contracting. The establishment of the ship's Maintenance Team has increased information exchange among all parties concerned and thereby ensured the right maintenance is being completed at the right time. In addition, the implementation of an innovative contract vehicle, Multi-Ship, Multi-Option (MSMO), has increased the partnership between the Navy and private sector, improving response time and saving money.

The RMCs' ultimate mission is to sustain the nation's investment in a fleet of 283 deployable ships by providing cost-wise maintenance to the fleet. CHIPS talked with Rear Adm. Orzalli in November about ship maintenance at the RMC headquarters located on the waterfront of the Norfolk Naval Base.

CHIPS: Was the driver for consolidation of these different fleet support activities to gain efficiencies?

Rear Adm. Orzalli: Yes, by consolidation of activities involved in ship maintenance in a region there are great opportunities for efficiencies. The consolidation takes advantage of improved communication tools and information technology systems in order to provide a better, more consistent service to the fleet.

The process actually started in the early '90s with the consolidation of back shop functions, such as motor rewind capability and pump repairs. The classic example was here in Hampton Roads where we had 17 different organic activities that were capable of rewinding a motor.

We established Regional Repair Centers which provided a single location for a specific maintenance function with common processes and training. By doing this we gained efficiencies and reduced our footprint. Those successes spurred further regionalization efforts.

CHIPS: Do you work with the shipyards?

Rear Adm. Orzalli: In actuality some of our Regional Maintenance Centers are also naval shipyards. A case in point, I was the commander at Puget Sound Naval Shipyard when we stood up the Northwest Regional Maintenance Center.

In this case, Pacific Northwest, Puget Sound Naval Shipyard, is the Regional Maintenance Center, and they are responsible to me as CRMC to execute functions of technical support and contract oversight on work that is done in the private sector.

CHIPS: When I think of ship maintenance, I think of pumps and paint, not technology. But maintenance is so much more complex.

Rear Adm. Orzalli: The information and communication systems available today have provided the Navy maintenance community significant capabilities. To the point where we can and have implemented a one-call solution to assist ships.

We have established a global call center that will take worldwide calls and direct them to the proper technician to get the question answered. These technicians immediately work to resolve the problem with the ships via distance support, where they talk the shipboard personnel through the processes, procedures and checks to troubleshoot and repair the system.

If it [issues] cannot be resolved via distance support we will go to the ship. Our technicians are located close to the waterfront, so if the ship is located in port, we can rapidly respond to the ship's needs. If they are overseas, we deploy technicians necessary to provide support.

For the systems which the RMCs don't have the expertise necessary, especially the newer ones, we go immediately to the in-service engineering agent, the SPAWAR [Space and Naval Warfare] Systems Center, or the equipment manufacturer.

The RMCs are the ship's initial call for maintenance support. They solve approximately 95 percent of the problems, but if they can't handle the job, they'll bring in partners. To support this, we have been working with Rear Adm. "Grunt" Smith, vice commander [of] SPAWAR, to reduce response time, to correct system problems, and to make sure all of us are using the same information sharing tools.

CHIPS: Do you have a prescribed time that you want to be able to respond to a problem?

Rear Adm. Orzalli: It depends on how it is identified to us. If the casualty significantly degrades one of the ship's primary warfare

missions (category 3/4 casualty), we have specific timelines to meet. If it is a category 2 casualty, meaning the ship can still operate, but is degraded within a functional area, then we will use budget considerations as part of our thought process. We will prioritize the maintenance to determine when it is the right time to repair it. Many times that's right away.

CHIPS: Do you work with the Surface Warfare Enterprise?

Rear Adm. Orzalli: Quite a bit, as most of our work is aboard surface ships, and I am on the Surface Warfare Enterprise Board of Directors and Executive Committee. However, we support the Surface Warfare Enterprise, the Undersea Enterprise, as well as the Naval Aviation Enterprise, in providing services to the ships.

A lot of the systems that we work on, especially in communication and information systems, are on all types of platforms. In working with all the enterprises, I have executed performance agreements which establish expectations of timeliness, costs and metrics. We are driving the RMCs to meet the expectations of the customers.

CHIPS: Does your organization include contract specialists?

Rear Adm. Orzalli: One of the functions of the Regional Maintenance Centers is contracting for private sector maintenance. We have shipbuilding specialists on the deckplate to provide oversight for the contractors for the work, but we also have a contracts department that negotiates with our private sector partners on the contracts.

We have multiple contract vehicles. One of the current initiatives is using portfolio contracts where we have contract vehicles in place for specific functions so we can rapidly put work in place.

In addition, for maintenance availabilities, we have Multi-Ship, Multi-Option contracts for each specific ship type within a homeport. This allows us to develop partnerships and teaming arrangements with a prime contractor for that ship type. They are a one-year contract with multiple option-years designed to improve responsiveness to the ships.

MSMO contracts also provide an opportunity for learning, since one prime contractor owns the contract for maintenance in scheduled availabilities and in unscheduled availabilities. This enables us to make better economic decisions on when to complete the maintenance. We have them for almost every ship and almost every homeport.

CHIPS: What happens if ships are deployed when a casualty occurs?

Rear Adm. Orzalli: We have maintenance facilities at Naples, Italy, in the 6th Fleet; Manama, Bahrain, in the 5th Fleet; and Yokosuka, Japan, in the 7th Fleet. Deployed ships are provided maintenance support according to where they are located.

Each RMC is assigned an area of responsibility to respond worldwide. If the ship is not in the vicinity of our facilities, or they do not have the capability to complete the work, then we can provide worldwide voyage repair by deploying fly-away teams to meet the ship.

CHIPS: Do you coordinate planned maintenance as well as repairs? Is planned maintenance difficult to schedule with the current operational tempo?

Rear Adm. Orzalli: Yes. We work with the ships and the Type Commanders to schedule and execute planned maintenance over the ships' life cycle. The current world situation has increased the operational tempo in support of the Fleet Response Plan. This does make it more difficult to coordinate completion of maintenance in support of the ships' schedules. However, our Multi-Ship, Multi-Option contract partnership has helped us to respond to both the planned maintenance and made us more responsive to meet the emergent maintenance needs.

CHIPS: If SPAWAR had a new software upgrade to ships' systems, would they first come to you for scheduling?

Rear Adm. Orzalli: It depends. For example, in our surface ships we have a maintenance and modernization business plan that we have put together based on proposed alterations for the ship during that execution year, as well as the maintenance budget. Any scheduled availabilities are identified during that time and what work is scheduled to go on during those scheduled availabilities and integration of the alteration work with the maintenance.

For a lot of alterations, we use alteration installation teams and, in some cases, some of the support work for those alteration installation teams goes to the Multi-Ship, Multi-Option contractor to provide support. We try to balance the amount of work that is in alterations to ensure we don't overtax the skill set required for the maintenance or modernization package.

We have had some recent availabilities with huge modernization efforts such as the Iwo Jima here in the Hampton Roads area. This required extensive coordination to manage the interfaces between the alterations and maintenance work packages. We are working to include management measures necessary to ensure coordination by including the Joint Fleet Maintenance Manual.

CHIPS: Are the RMCs responsible for upgrades on radar or weapon systems?

Rear Adm. Orzalli: If it is done on the waterfront and part of an availability, then the Regional Maintenance Center is designated the Navy's supervising activity. This means they are responsible for the integration, execution and final certification of the work on that availability even though it is sponsored and paid for by a program manager. This requires strong lines of communication between CRMC and SPAWAR. Our organizations have recognized that if we are to succeed we must work on alignment and communication. Recently, we have made significant strides with communications and teaming partnerships.

CHIPS: I have heard from leadership that there are legacy systems on the ships that they would like to see replaced with modern technology. Would the CRMC be the driver for that?

Rear Adm. Orzalli: We look at this issue from two perspectives. The first is that we do alterations to reduce required maintenance. The Regional Maintenance Centers have an engineering

department that provides technical support and oversight of the technical aspects of the repair efforts. If we determine a system has a high failure rate due to a technical or operational issue we can make recommendations to modify components that would reduce the necessary maintenance.

In such cases, we prioritize in order to get the best return on our investment. An example is that we shifted from pumps that require packing, to pumps with mechanical seals, and thereby significantly reduced the repacking requirement. We may also change material types or find replacement components that don't fail as often.

The second perspective is the modernization of systems to support the ships' warfighting capability. We buy ships and keep them in service for 30 to 40 years. In the later years of a ship's service life, finding spare parts and technical expertise for originally installed equipment can be a problem. In addition, systems may become obsolete. In these circumstances the equipment may be performing a function fine, but providing repair parts and technical support become cost prohibitive.

The RMCs provide input for the metrics that we track, which might reveal these trends. We work with the CLASSRONs (Class Squadrons) and the warfare enterprises to determine if a system is troubled and make recommendations to correct the problem.

CHIPS: The job of keeping Navy ships combat ready is extremely challenging. What is the composition of your staff?

Rear Adm. Orzalli: I initially had orders as the commander of the Mid-Atlantic Regional Maintenance Center. From that position it was difficult to implement standard processes and procedures across the RMCs, while coordinating the maintenance on the waterfront. Therefore, a year ago CRMC was formally stood up. From the beginning, my goal was not to raise a large staff but to tap into the individual Regional Maintenance Centers for support and expertise so I wouldn't have to retain it at headquarters.

I have a senior civilian as an executive director that helps me understand the business. I have a senior military officer, a captain, who is my principal interface with all my customers. Since the customers are primarily warfighters, it helps to have a uniformed guy that can speak the same language with the customer.

My staff includes a financial group that not only does the oversight of execution, but is responsible for putting together the capability plans that will generate the RMCs' requirements in order to get programming and funding. We have a process improvement person, who employs the principles of Lean Six Sigma to standardize and improve our processes.

I have a group of information technology specialists who keep the maintenance applications operating. Our assessment person taps into the other RMCs or other activities for expertise to certify that the activities are operating in accordance with the requirements of the Joint Fleet Maintenance Manual.

CHIPS: Where does your funding come from?

Rear Adm. Orzalli: We are funded by Fleet Forces Command out of the ship maintenance funding.

CHIPS: I read on Navy dot-mil that you went to the Mega Rust Corrosion Conference in August. It sounds like your job would offer more excitement than that. Seriously, I know that rust is a huge concern for the Navy.

Rear Adm. Orzalli: You stole one of my lines. I was at the Mega Rust Corrosion Conference and [Rear] Adm. James McManamon from SEA 21 [deputy commander for Surface Warfare] was there. I started my discussion by saying, I was asked by a friend where I was going. When I told her that I was going to the Mega Rust Conference, she said, 'Boy, that sounds exciting,' and rolled her eyes.

When at graduate school at MIT, I worked in the Corrosion Lab for three semesters, so corrosion is a passion of mine from an academic pursuit. The conference brought together a diverse group of scientists, engineers, salesmen and innovators. All of them were looking to address some of the significant issues that we have to deal with from the naval perspective. Rust is generally thought of as a nuisance, but in the Navy, it is a huge cost driver.

We build ships, principally out of steel, and we sail them in salt water. It doesn't take a degree from MIT to recognize that we are going to have corrosion issues. There are three components to the rust issue: the material, the environment and the electrical potential.

The maintenance community attempts to tackle all three. We choose materials that are not susceptible in the environment. However, non-corrosive material suitable in ship applications can be very expensive, so they may not be available from an overall cost perspective. The second thing is to isolate the material, and we often do that with paint.

The third thing is the electrical potential so in multiple systems we have impressed current where we change the electrical potential so even if we don't have paint, the electrical potential is such that the susceptible material is stable. Our paint systems have become much more complicated.

At the conference, we got good synergy and commitment between the paint manufacturers to work on systems that will last in the environment that we are subjected to. There were not any breakthroughs from a technology perspective, but the Navy is committed to using one coat of paint that has a rapid cure with the qualities of longevity and durability that we need to reduce our overall life-cycle costs. Industry recognizes where we are going and that we are committed to it.

CHIPS: Can you talk about the ship paint process?

Rear Adm. Orzalli: It depends; different portions of the ship have different paint cycle requirements depending on the environment. We will paint based on the inspected condition of the tank or surface. Sometimes it depends on how well the initial application stands up. We will do a local area or spot touch-up, or sometimes we will do a full blast, take it down to white metal and start over again.

The systems we are installing today have design life cycles of 10 to 20 years in the salt water environment. The cost of paint is not the biggest cost when you do a paint job. It's the cost of preparation to prepare the surface to accept the paint. If we can reduce the number of times that we have to paint — we will drive down the cost.

We are working on some other things like embedded sensors.

A tank with a painted surface could have a sensor inside that will measure the electrical activity in the tank, and thereby tell us if we have a breach in the paint system. There are limited applications at this point, but it enables us to find the problem early and therefore limit the damage and cost.

CHIPS: Can you talk about some the successes that you have had?

Rear Adm. Orzalli: There have been some significant changes in the RMCs since I first reported aboard, and this has been accompanied by some successes. If you look at the population of non-shipyard Regional Maintenance Centers, since standing up in October of 2004, we have reduced from about 8,000 people to a little over 3,000. This reduction has enabled us to reduce the infrastructure and overhead required, as reflected by the Mid-Atlantic Region alone reducing the number of facilities from 17 to five buildings.

One of the areas in which we have made clear progress since the standup of the Regional Maintenance Centers is in availability planning. The RMCs used to conduct the preponderance of detailed planning necessary to execute availabilities, and the contractor would duplicate this effort. Since implementing Multi-Ship, Multi-Option contracts, we simply identify the work, and the contractor identifies the detailed planning that is necessary to complete the work, including material ordering and technical work specifications. This has made a significant impact on responsiveness and cost.

CHIPS: I've read some discussion on the need for more "hands-on" maintenance training for Sailors to replace current computer-assisted training. Do have a hand in recommending training for ship maintenance?

Rear Adm. Orzalli: The RMCs provide limited training opportunities to our Sailors. When our technicians go aboard ship, our Sailors gain experience by observing and participating in the troubleshooting process.

We conduct some limited classroom type training on specific systems within our facilities. In addition, the shipyards and some of the RMCs operate a journeyman-level training program called Navy Afloat Maintenance Training Strategy.

As far as the issue of computer-based training, I was the graduation speaker at Great Lakes two months ago, and I had an opportunity to visit the Navy's training facilities for A School. They have some computer-based training, but the Sailors also get the opportunity to conduct hands-on troubleshooting and repair of the actual equipment.

Since the ships are the driving factor in the training pipeline for our Sailors, my role in this area is different. I talked with the Fleet Master Chief to ensure that we have a good feedback mechanism between the ships on the waterfront with the schoolhouse. We need to continually review our training programs to ensure that they meet the ships' requirements and identify where the maintenance community can provide support.

To view Rear Adm. Orzalli's biography, go to www.navy.mil and click on the Navy Leadership link. For more information about the Regional Maintenance Centers, go to www.crmc.navy.mil. CHIPS

San Diego Mayor Visits SPAWAR Systems Center Pacific

By Jim Fallin, SSC Pacific Corporate Communications and Public Affairs

The working relationship and longstanding partnership between the City of San Diego and Space and Naval Warfare Systems Center Pacific (SSC Pacific) took a significant step forward over the month of December following a command visit by San Diego Mayor Jerry Sanders and two subsequent meetings where Capt. Mark Kohlheim, SSC Pacific's commanding officer, and other senior SSC Pacific staff members, joined Sanders for meetings with the city's Economic Roundtable and for briefings with the mayor's personal staff and Inter-government Committee on Economic Development.

During the mayor's visit in early December, Capt. Kohlheim and SSC Pacific's Technical Director Carmela Keeney talked about SSC Pacific's lab's role as the Department of Defense designated Center of Excellence for Command and Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance, and its many recent accomplishments in providing support to America's warfighters and the global war on terror.

Sanders also received a detailed overview of the command's business model and numerous mechanisms for partnering with industries from Mr. Gary Wang, SPAWAR's chief technology officer and head of SSC Pacific's science, technology and engineering department, and a comprehensive overview of the lab's increasing efforts to promote interest in math and science throughout San Diego schools by Dr. Jim Rohr, director of SSC Pacific's educational outreach programs.

At the conclusion of his visit, Mayor Sanders commented that, based on his own personal and firsthand experience, SSC Pacific clearly rivaled Lawrence Livermore National Laboratory, Los Alamos National Lab and Oak Ridge National Lab in bringing innovation and technologies to bear, and in successfully partnering with local businesses and the local community. Sanders went on to say that SSC Pacific represented an extraordinary and unique local resource that San Diego and the region must recognize.

On Dec. 10, Capt. Kohlheim responded to a personal invitation from Mayor Sanders to join him at his Economic Roundtable for discussions with other local business and community leaders on the development of a strategic plan for San Diego's future. One week later, on Dec. 17, Capt. Kohlheim, Gary Wang and Jim Rohr joined the mayor at City Hall to deliver a command briefing to the mayor's staff and other city officials.

"I welcome this recent and increased contact with the mayor and his enthusiastic support for the command," Kohlheim said. CHIPS

SSC Pacific Commanding Officer Capt. Mark Kohlheim, San Diego Mayor Jerry Sanders and SSC Pacific Technical Director Carmela Keeney.

SSC Pacific signs largest ever DoD patent license agreement

More than 90 Navy inventors represented in new licensing agreement to commercialize a portfolio of Navy-developed technologies bringing important inventions from the lab to the marketplace ...

By Ed Budzyna and Dr. Stephen Lieberman

Space and Naval Warfare Systems Center Pacific finalized a patent license agreement with Elemental Wireless LLC, a wireless and software product development firm headquartered in Delaware in September 2008. This innovative technology transfer agreement, which builds on guidance from the Deputy Under Secretary of Defense for Advanced Systems and Concepts, Office of Technology Transition, took more than two years to negotiate and contains more than 60 patents.

The agreement represents the combined work of more than 90 individual inventors at SSC Pacific, the Navy's premier laboratory for information technologies. The lab, which employs about 2,000 scientists and engineers, has a portfolio of about 300 already issued patents.

The new agreement includes a multi-million-dollar up-front payment, according to Dr. Stephen Lieberman, who is the director of SSC Pacific's Office of Research and Technology Applications.

"All told, this agreement contains the single largest up-front licensing fee ever negotiated by the U.S. Navy and the Department of Defense," Lieberman said. "The agreement will help facilitate the commercialization of an entire portfolio of Navy-developed technologies focused on computer software and hardware, advanced algorithms, artificial intelligence semiconductors, digital imaging, communication protocols, lasers and optics."

Patenting and patent licensing are two important mechanisms used in the Navy technology transfer program. Patents protect the Navy's research and development investment, and make inventions more valuable to private sector entities seeking to commercialize a technology.

Patent licensing supports economic development in the United States by leveraging the products of the Navy's research and development enterprise.

"This license agreement will provide a path for moving important technologies from the lab to the marketplace, as well as a vehicle for creating high-tech private sector jobs, while providing a significant financial return to the Navy," Lieberman said.

When scientists or engineers working in the SSC Pacific lab invent something that they believe is potentially patentable, they file a patent disclosure with SSC Pacific's patent office.

The in-house office attorneys perform an initial patent search and evaluation, if the idea passes screening, the attorneys will file a patent application with the U.S. Patent and Trademark Office, according to Lieberman.

The USPTO evaluates the patent application against other patents and published information to see if it is novel and worthy of patenting.

"The process for getting the patent could take up to several years. The initial step of disclosing the idea gets it into the pipeline. Then the patent office can take anywhere from weeks (that would be in the best case) to sometimes more than a year to file that patent application which goes to the USPTO. It depends on how many are in the pipeline," Lieberman said.

Additionally, and under the terms of the patent license negotiated with Elemental Wireless, the inventors will receive additional payments when their inventions are sublicensed to other companies.

"Inventors that assign their rights to the government are entitled to a share of the royalties from licensing the invention. Once patent applications are filed, my office tries to market those inventions to let industry know they are available for licensing," Lieberman explained. "The payment that the inventors would get is not from the patent; it is from the licensing of these government inventions to a commercial entity."

This tech transfer of innovations to industry through licensing agreements is critical for getting the technology to market and getting it into a form that can be

The Space and Naval Warfare Systems Center Pacific patent licensing agreement team members. Top row, left to right: Stephen Lieberman, Vincent Crowley, Natalie Pope and Scott Miller. Bottom row, left to right: Ryan Friedl, Ana Smith and Carye Concha.

Other team members not pictured include: Peter Lipovsky, Eric Anderson, Soheil Atari, Jonathan Lim, Irene Tan and Michael Kagan.

The new licensing agreement represents the transfer of Navy-developed technologies to the marketplace. Technologies include: software and hardware, advanced algorithms, artificial intelligence semiconductors, digital imaging, communication protocols, lasers and optics.

reacquired by the Defense Department to support the warfighter, according to Lieberman.

"The Navy generally will not be the one to take the product into a robust, fully supportable form — or even to its most useful format. Often, it requires the commercial sector to do that. The biggest success for us is what we call 'spinning the technology out' or licensing it out of the government to a provider, so that provider can spin it back into the government as a product."

The big benefit to the Navy and DoD is the acceleration of technology into usable products that fulfill warfighter requirements.

"When Navy scientists and engineers invent things, it is usually cutting-edge innovation," Lieberman added.

Sometimes developed technologies have dual use in both DoD and the civilian community.

"We will see both cases. A lot of our inventions are focused on software, communications, and a number of broad categories and technologies. It is likely that there will be products that the DoD will be interested in, and there will also be commercial applications," Lieberman said.

"We have had several technologies in the past that we have licensed. One was a technology that offered an efficient way to test the toxicity of water. It was a technology developed here in the lab that uses bioluminescence. Dinoflagellates are marine organisms that produce a blue-green light like a firefly. The amount of light the organism produces decreases if it is exposed to toxicants. It is like the canary in a cage that coal miners used to detect poison gas," Lieberman continued.

"One of our scientists discovered that this luminescence decreased when exposed to toxicants. The Navy patented his discovery, and we licensed it to a company here in San Diego County that has now created a commercial product for rapid testing of toxicity in water. He is now marketing it internationally."

Lieberman said it has also brought benefits back to the DoD because the Navy is looking at it as an improved method for conducting some of the toxicity tests that it is required to do.

Lab personnel work closely with the Office of Naval Research and the Acting Director for the Office of Technology Transition, Ms. Cynthia Gonsalves, for guidance, according to Lieberman.

"All of the tech transfer guidance and oversight is done at the Office of Naval Research. That office provides us with basic guidelines and even the basic templates for Navy license agreements.

"We also report our activity on licensing up to the OSD level, to Cynthia. We had a meeting a couple of weeks ago, hosted by Cynthia. It is an annual tech transfer meeting where we all get together and share best practices and get updates on new legislation that affects tech transfer within the DoD," Lieberman said.

SSC Pacific was designated by the Department of Defense as the Center of Excellence for Command and Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) in the Maritime Domain and for Research, Development, Acquisition, Test and Evaluation (RDAT&E) and the Integrated RDAT&E Center for Maritime C4ISR for Information Technology.

SSC Pacific is the nation's only full spectrum C4ISR laboratory providing research, development, acquisition, test and evaluation and full life-cycle support across systems that integrate the military's sensors, networks, command and control, and weapons into a fully netted combat force with full spectrum dominance.

A sampling of SSC Pacific-developed technologies include:

- Wearable Ultra-broadband Antenna
- Enhanced Touchpad
- Ultra-sensitive, Low Power Magnetometer
- Algorithm for Minimum Antenna Size
- Flexible Video Display
- Microsensor Medical Condition Monitor
- MEMS Displacement Sensor Ultra Sensitivity – Just licensed!
- Robotic Radio Communications System
- Object Selection in 3D Environment
- Increasing Network Communication Capacity
- Red Blood Cell Deglycerolization System
- Autonomous Remote Biohazard Surveillance System
- Motion Generated Electricity
- Electroactive Polymer Biaxial Braid
- Intelligent Decision Support System
- Water Quality Profiling System and Autonomous Sensor Buoy
- Microprocessor Power Reduction
- Exponentially Tapered Biconical Antenna
- Non-Destructive Evaluation of Microwave Tubes

For a complete list, go to http://enterprise.spawar.navy.mil/body.cfm?topic_Id=2678&Type=R&category=29&subcat=211.

Dr. Lieberman and the lab team work hard to publicize the lab's work to maximize the up-front investment that has been made in developing technologies.

"We don't want to see our innovations sitting on a shelf. We want them to be exploited for commercial use. When I started heading our Technology Transfer Office, I would often find when networking with the entrepreneurial community that most of the community was not aware that the DoD or federal government was a great source of innovative technologies.

"They always are familiar with universities being a source of innovation, but we are not on their radar screen.

"We are looking ahead and trying to embrace some more novel and exciting ways to inform the public about the availability of our technologies," Lieberman said.

SSC Pacific's Technology Transfer Office is developing videos that highlight technologies that are available for licensing. The first marketing video has not only been successful at attracting industry interest to a particular technology, but Lieberman also sees it as a powerful recruiting tool for drawing young scientists and engineers into working in Navy labs.

Navy scientists and engineers work with groundbreaking technologies and also can benefit from licensing agreements with industry. At the same time, their work supports the warfighter.

You can view the video at http://enterprise.spawar.navy.mil/body.cfm?topic_Id=2678&Type=R&category=29&subcat=211.

"There is a trend with YouTube — all this video stuff is becoming so common. Young people pay attention to it. We want young people to see what we are doing. It's exciting," Lieberman said.

CHIPS

Fleet begins transition to new reporting system

Web services and a service oriented architecture provide robust tools for faster and better combat readiness reporting and decision making

By U.S. Fleet Forces Public Affairs

Feeling out of SORTS? That's because the current readiness reporting system, Status of Resources and Training System, commonly known throughout the fleet as "SORTS," is being replaced with a new Web-enabled database system that leverages single-entry authoritative data from across the naval enterprise.

The new Defense Readiness Reporting System-Navy provides unit commanders with detailed resources information to assist in assessing readiness. The fleet began transition to DRRS-N Oct. 1.

DRRS-N is based on a service oriented architecture and uses Web services to move data. This change provides Navy and joint commanders continuous access to unit and group level capability-based readiness assessments.

Commanders will use Business Intelligence for decision support. BI provides a flexible decision-support mechanism that allows the generation of an assortment of ways of reporting — everything from static reports to graphical dashboards. BI allows the rapid and relatively inexpensive development of a virtually limitless variety of readiness reports to support higher level commanders in making readiness and resource allocation decisions.

The old SORTS system is based on a formatted naval message with a rigid line construct transmitted via naval message traffic. DRRS-N uses a completely different construct, but can collect specific comments related to overall mission essential tasks (MET), capability readiness, or individual resource deficiencies, as appropriate.

A Web dialogue displays the last reported readiness assessment for each capability and task. The commander can make any appropriate changes and insert comments as required. The data input by the commander is then forwarded via Web services to be recorded in the main DRRS-N database.

DRRS-N is a major shift in readiness thinking and reporting, moving the focus from reporting unit resources and training, to assessing and managing force capabilities.

Using a suite of applications, the program provides leaders and force managers a much more robust package of tools and information to aid in crafting rapid responses to emerging crises while also providing greater ability to assess operational risks.

"DRRS-N will enhance operational decision-making processes by providing accurate, near real-time information about combat readiness to our operational commanders," said Deputy Chief of Staff for U.S. Fleet Forces Command (USFF) Operational Readiness and Training, Rear Adm. Rich O'Hanlon.

The journey to DRRS-N implementation began in 2002 when the Defense Department mandated that all the services develop a capabilities-based readiness input into the DoD Readiness Reporting System (DRRS).

To meet this requirement, USFF, in coordination with the Chief of Naval Operations, is the Navy's executive agent for DRRS-N development and transition.

Afloat units are currently receiving the DRRS-N hardware and software to facilitate the transition. Virtually all Commander, Navy Installation Command shore stations and regional commanders worldwide are already reporting in DRRS-N. Many other shore-based commands have begun the transition as well.

The Fleet Response Plan, in execution of the maritime strategy and combatant commander requirements, reinforces the need for an efficient and modernized readiness management system that provides accurate and relevant readiness information for planning and risk assessment.

DRRS-N will also be more user-friendly than the current readiness system, SORTS. Designed with the Sailor in mind, a significant milestone in the upcoming fleet transition is the capability to automatically populate SORTS data fields. This eliminates the requirement for operational units to report in both DRRS-N and SORTS during the transition period.

"We wanted to minimize DRRS-N data input by using unit resource data that is already provided through a variety of other authoritative systems in a Web serviced environment. Since data only has to be entered once in the right system, that will lighten the burden on Sailors," said Sue Tysor, program manager for DRRS-N.

For more information about DRRS-N, Common Access Card holders can go to https://www.fleetforces.navy.mil/drrs-n. CHIPS

Naval Station Great Lakes (Nov. 14, 2008) Adm. Jonathan W. Greenert, commander, U.S. Fleet Forces Command, inspects a recruit drill team as the reviewing officer for a recruit graduation ceremony at Recruit Training Command. Greenert also toured RTC facilities and many of Training Support Center's A and C Schools during a two-day visit to Naval Station Great Lakes. U.S. Navy photo by Scott A. Thornbloom.

The DoD Travel Assistance Center

Complete service for the defense traveler before, during and after temporary duty travel

By Sharon Anderson

Ever wonder about the dedicated people behind the Defense Travel System (DTS), the fully integrated, electronic, end-to-end financial management system that transformed temporary duty travel for Defense Department personnel? To fully appreciate their efforts, you need to take a closer look at DTS and what it does for the DoD traveler.

DTS meets unique DoD mission, security and financial system requirements within the guidelines of federal and DoD travel policies and regulations. Before DTS, federal travelers went one place to get their travel orders, and to still another to make transportation, lodging and rental car arrangements.

After completing their travel, they filed a travel voucher through one of many travel systems in use throughout the DoD. Many submitted hardcopy forms they filled out manually along with their receipts to be processed — and then waited — sometimes not so patiently for reimbursement.

Travel Assistance Center program manager Jim Deming with deputy program manager Lonnie Cole.

About the Defense Travel System

The Defense Travel System (DTS) is a fully integrated, digitally secure, electronic system that automates temporary duty (TDY) travel authorizations, reservations, and voucher processing of DoD travel transactions. It is specifically tailored to meet unique DoD mission, security and financial system requirements while remaining within the guidelines of federal and DoD travel policies and regulations. For more information on DTS, please visit the Defense Travel Management Office Web site at www.defensetravel.dod.mil/.

DTS, in contrast, enables travelers to complete all these transactions from the convenience of their desktop computers. According to the Defense Travel Management Office (DTMO), the organization that serves as the single focal point for commercial travel within DoD, DTS processed more than 3 million temporary duty travel vouchers with an average voucher payment time of 7.8 days during fiscal year 2008.

DTS enables better oversight of the multibillion-dollar DoD travel enterprise and ensures compliance with applicable federal and DoD travel policies and regulations, according to the DTMO.

Enter the TAC

To expand assistance provided to DoD travelers, the DTMO established the Travel Assistance Center (TAC) to provide 24-hour assistance (including federal holidays) to DoD personnel before, during and after official travel. The staff can answer questions about travel-related topics including the DoD travel card, travel policy, commercial travel services and programs, as well as provide assistance with DTS to all defense travelers — both military and civilian — regardless of military service or defense agency.

The TAC complements the assistance provided by defense travel administrators (DTA), according to Jim Deming, the TAC program manager. DTAs are typically designated to assist personnel working in their activity.

"In the beginning, our customer base was mainly made up of defense travel administrators. This past summer we opened our services to all military service and defense agency travelers. This was a phased approach that began in October 2007. Today, we execute the call center function for DTMO for DTS assistance, and recently expanded our mission to answer all travel-related questions, including questions on the new DoD [Citi] travel card transition, commercial travel services and travel policy," Deming said.

The TAC also assists recruits traveling from their Military Entrance Processing Station (MEPS) to their first training base. From the time a recruit leaves a MEPS to the time that a camp or station accepts the trainee for an individual training assignment, the TAC makes sure each recruit gets from place to place.

"You would think that was an easy task, but somebody can get sick, flights can be delayed or canceled, and you can have inclement weather issues. We take calls from the recruits, and we put them in hotels and get them fed because these individuals travel sometimes with little cash, and have not yet been issued a DoD travel card.

"For a lot of them, it is their first time away from home and they are young — sometimes as young as 18. We are their lifeline. We work with major hotels that are located close to airports to provide lodging and meals, and we work with the United Service Organizations, the USO, so they can assist," Deming said.

At the time of the interview with Deming, the DoD transition to the new Citi travel card was just over the horizon — Nov. 30. Deming said transition planning had been going on for more than a year to ensure a smooth transition for travelers.

"Do you know that Citi opened a state-of-the-art 33,000 square-

foot support facility in Norfolk? We are meeting with Citi representatives to finalize plans for the transition — that's one more link to providing good service to DoD travelers.

"We have a message on the TAC interactive voice recording system so that customers that have travel card questions or issues can select from a menu to speak directly to an analyst at the TAC, or be transferred to Citi's support desk for card service issues. We know that this will be a big change for travelers, and we have been working for a year on the type of support that we anticipate travelers will need," Deming said.

Space and Naval Warfare Systems Center Atlantic has managed the travel call center for the Navy since 2004, so when DTMO established a call center for DoD travelers, SPAWAR offered its expertise in this competency area. Deming, a retired Army colonel with 26 years of active service, oversees the TAC and its staff of 35 personnel, 32 of which provide direct support to the call center. Many on the staff are former military service members with experience in travel-related services.

What the TAC Does

In simple terms, customers call the TAC at 1-888-Help1Go and speak to an analyst based on their type of problem. For first time callers, the analyst will first create a traveler profile and call center ticket so they will be able to track the progress of the ticket and retain a record of the help received.

The analyst then records the problem and resolution on the call center ticket. If the analyst cannot resolve the issue during the call, the ticket is escalated to either DTMO or the DTS vendor for resolution.

DTMO recently launched Travel Explorer (TraX), a user-friendly Web solution that is an extension of the TAC and offers a centralized source of travel information. TraX allows users to submit a call center ticket, track the progress of open tickets while TAC representatives conduct research, or search and review responses to previously submitted questions.

Before submitting a help ticket, users are encouraged to explore the self-help features for instant access to hundreds of frequently asked questions, as well as to view various training opportunities and trip planning tools.

Customers receive timely assistance and many issues are resolved with the first communication with the TAC. September was a particularly busy month with more than 15,000 call center tickets issued. "That was a new record for us," Deming said.

The TAC leadership team coordinates with the DTMO daily to discuss any emerging issues. When it is time for a DTS software upgrade, meetings expand to include the DTS-PMO. The program management office is in charge of acquisition of the system, development, integration and maintenance of DTS.

In the last three months, DTS underwent three software upgrades, crossed the fiscal year, and adapted to the new DoD travel card. During these events, TAC lead analysts performed functional tests, often working weekends and late hours to ensure proper functionality.

Customers contact the TAC from all over the world including the Middle East and Pacific. Since quality customer service is the hallmark of the TAC, each Tuesday the team offers a "DTS Outreach Call" for anyone from the DoD travel community. Calls last about two hours and are held at 8:00 a.m., and 1:00 and 10:00 p.m. EDT to accommodate those in each time zone. Typical topics include the top call center tickets for the week, the latest DTS software upgrades and other emerging travel-related topics.

TAC Quality Initiatives

The TAC follows a philosophy of continuous process improvement — team members learn this on the first day of work. Personnel avidly embrace the tenants of the ISO 9001:2000 Quality Management System (QMS). All team members are expected to routinely contribute to better ways of doing business.

"We hold a TAC improvement meeting every week where analysts come up with suggestions to improve service to the customer, whether it entails changes to our interactive voice recordings or changes to the call center ticket management system. Some of these suggestions we use as rapid improvement events. We employ them quickly to improve the overall customer experience," Deming said.

The TAC uses, in addition to other highly regarded sources, Help Desk International (HDI), as a benchmark for customer ser-

The DoD Travel Assistance Center Team.

vice. Guided by an international panel of industry experts and practitioners, HDI is a leading resource for call center emerging trends and best practices.

"We use Help Desk International standards for gathering metrics data and analyze it to make sure that we are within certain standards for our key performance indicators," Deming said.

The TAC utilizes Lean Six Sigma techniques to identify and refine processes. The team integrated scheduling techniques with inbound call metrics to optimize staff scheduling, eliminating excess capacity when call volume is low and ensuring maximum staffing during peak call hours.

The TAC also employs state-of-the-art technology to maximize the efficiency of the workforce. Some of the technologies used are described below.

- AltiGen Automatic Call Distribution System. The team continually analyzes and refines this tool to meet the changing needs of the travel community. Recently, the team found a way to reduce caller wait time. Compounded annually the savings are significant. This high-tech telephone network allows the team to "home source" analysts to minimize weather-related commuting problems and continuity of operations challenges. Additionally, it significantly minimizes staff turnover and has demonstrated increased analyst productivity.

- RightNow Ticket Management System. The team continually analyzes and refines the look and feel of the product to promote ease of use for the analyst in gathering pertinent information to assist the customer. Effective use of the reporting capability provides management with appropriate dashboard metrics to measure effectiveness.

- LCD Display System. Multiple large screen display systems are used to monitor queues and to communicate important notices to team members. The recruit assistance team uses the displays to monitor national weather patterns and airport delays to anticipate disruptions affecting recruit movements.

- Plantronics Wireless Headphone System. The TAC believes that continuous improvement and improved quality of life can be achieved without costly intensive changes. For example, the TAC recently moved from using standard headsets to wireless headsets.

Initially implemented for weekend and overnight shift employees, who often have to get up from their desks at a time when staffing is light, the benefits of wireless headsets were subsequently extended to the staff during peak staffing hours. Analysts were able to access resources located away from their desks while continuing to assist callers.

How the TAC is Organized

The TAC is composed of several teams — generalist, commercial travel office (CTO), financial and technical.

The generalist team is the first contact point for customers. In addition to answering travel-related questions, TAC general analysts assist with DTS document or system error resolution, and research and update submitted tickets. They also route tickets to other TAC teams when required.

The Defense Travel Management Office (www.defensetravel.dod.mil/) was established to serve as the single focal point for commercial travel within the Department of Defense to establish strategic direction, set policy and centrally manage commercial travel programs.

The DTMO maintains central oversight for commercial travel management, travel policy and implementation, customer support and training, DoD travel card program management, and functional oversight for the Defense Travel System.

The TAC CTO team troubleshoots DTS documents that might not transmit properly between DTS and the global distribution system, resolves passenger name record (PNR) errors, verifies approvals in PNRs and confirms reservations.

All CTO analysts have access to DTS and the three major global distribution systems: Sabre Travel Network, Apollo Travel and Worldspan.

"Our CTO analysts assist in updating reservations so that the quality checks performed by Sabre and DTS allow the document to update in DTS and process through the routing chain so the traveler can get an authorization approved," Deming said.

The TAC finance team addresses issues and tickets that are related to centrally billed accounts and debt management and specializes in resolving accounting system rejects.

One of the more popular questions from travelers is "Where is my reimbursement for travel?" according to Deming.

"Our average voucher payment time is 7.8 days. DTS interfaces with many partner financial systems with which we have to coordinate and research issues. DTS is a very complex system that complies with and far exceeds the standards for payments to DoD employees outlined in the DoD Financial Management Regulation," Deming said.

The TAC technical team monitors DTS health along with the developers and maintainers of the system. Every morning the technical team lead checks all the connections and servers to the global distribution systems for the airlines to make sure that they are all *awake* and working.

"We perform different scenarios to ensure the system is up to peak performance. If it isn't, we immediately report that to DTMO," Deming explained.

"If a caller tells us that they are having trouble connecting to DTS, we put them through a series of troubleshooting exercises to see if it is DTS or the network at the installation where the customer resides."

TAC employees go through a rigorous 60-day training program. The training plan takes them through all possible scenarios in DTS and call center operating procedures. CHIPS

Travelers can contact the TAC 24 hours a day, seven days a week by calling 1-888-Help1Go or DSN 312-564-3639. Users can create an account in TraX and submit call center tickets online.

To access TraX, please visit www.defensetravel.dod.mil/Passport. Participation information and a schedule of upcoming topics for the DTS "Outreach Call" can be found in the announcement section of TraX.

DON CIO Releases Web 2.0 Policy

Web 2.0 tools promote greater user input, creativity, information sharing and collaboration

By Christy Crimmins

On October 20, 2008, the Department of the Navy Chief Information Officer (DON CIO) released a memo providing initial guidance to all Navy and Marine Corps commands regarding the use of Web 2.0 tools.

"I wanted to provide guidance and encourage its [Web 2.0] use among Navy and Marine Corps commands," Mr. Robert Carey, DON CIO said. "Web 2.0 tools present many opportunities for collaboration and information sharing. They are becoming vital to keeping pace in today's environment."

Although Web 2.0 can be defined in a variety of ways, it is generally accepted as a collective term for Web technologies that promote greater user input, creativity, information sharing and collaboration.

Popular Web 2.0 tools like Wikipedia, YouTube and Facebook are primarily driven and maintained by user input. For example, if a user notices an error in an entry on Wikipedia, rather than e-mailing an author or webmaster, the user can simply apply for an account and make the correction.

This method leads to a much quicker release of accurate and updated information while improving direct collaboration among interested parties. Imagine how using this tool could improve the processing and release of DON "taskers" and correspondence.

Over the last few years, use of Web 2.0 applications has grown. Facebook currently has more than 120 million active users — up from 70 million less than a year ago. The social networking site is also the fourth most trafficked Web site in the world, according to statistics published by Facebook.

Carey points out that as more and more "Millennials" (those born between 1980 and 2000) join the workforce, these Web 2.0 technologies will be used, needed — and even expected — more than they are today. Consider that the number of 120 million Facebook users is nearly equivalent to half of the number of U.S. taxpayers.

Consequently, the DON CIO team has begun incorporating a variety of Web 2.0 tools into their business processes. They are using wikis to capture corporate knowledge and lessons learned, as well as to develop policy and work with other government organizations.

The DON CIO spectrum team recently used a wiki to gather comments on its draft Electromagnetic Spectrum Policy document. This allowed those from the larger spectrum community

Figure 1.

the opportunity — not to just comment on the draft — but to help create it.

In addition, Carey writes a blog that is posted on the DON CIO Web site.

"I use this online journal to explore IT issues that are facing my office and the larger department," he said. "This forum has opened up a dialogue within the community and even with those outside of the department. The feedback I receive is a key component of this blog and Web 2.0 tools in general."

The DON as a whole is using Web 2.0 tools in a variety of ways. For example, U.S. Fleet Forces Command is creating a work-related online social environment that leverages its task management system. It is also using a social network functionality to provide better visibility of personnel skill sets. This functionality gives the command the ability to form task-related working groups much more quickly and efficiently.

The Naval Research Laboratory set up a wiki for user documentation written by the developers and users of a particular telescope program. Also, Commander, Carrier Strike Group Twelve executed a successful combined fleet, joint and coalition test for afloat chat capability over the NIPRNET.

Chat had been used on the SIPRNET side, but not on NIPRNET due to security vulnerabilities. The test used the open standard Extensible Messaging and Presence Protocol, or XMPP, which has security features built in and has been approved for use by the Department of Defense.

Additionally, the Defense Information Systems Agency (DISA) is piloting E-CollabCenter and Defense Connect Online — also known as Button One and Button Two. These two collaboration tools facilitate virtual meetings and work groups through Web conferencing, chat rooms and one-on-one chat.

While the DON CIO memo does encourage commands to seek out opportunities to employ Web 2.0 tools, users are also warned that use of the tools must not compromise data integrity or confidentiality. Commands are also encouraged to "[A]here to existing information assurance (IA) and privacy policy, guidance, and best practices."

"As a DoD organization, we must be more mindful of security and cannot freely do everything that, say, an industry organization can," Carey said.

Additionally, the memo suggests ways in which Web 2.0 tools can be implemented. Among these examples are developing policy using wikis and broadcasting information via podcasts and blogs. Figure 1 shows an expanded list of some Web 2.0 tools and suggested uses. Mr. Carey points out that the list is not meant to limit the use of Web 2.0, but to provide suggestions for a starting point.

Christy Crimmins provides communications support to the DON CIO. CHIPS

Go to the DON CIO Web site at www.doncio.navy.mil and search under the Policy and Guidance link to view the Web 2.0 Guidance Memorandum. To blog with DON CIO Rob Carey, go to www.doncio.navy.mil/blog.aspx. The CIO blog is a forum for information management and information technology matters affecting the IM/IT workforce and the department. Carey has also launched a podcast series on a variety of topics that can be accessed from the DON CIO Web site.

More News from the DON CIO

Home Use for Microsoft Products Approved for DON Personnel

The Department of the Navy, through its contract with EDS for the Navy Marine Corps Intranet (NMCI), is entitled to use Microsoft Corp.'s Home Use Program. The HUP allows Navy and Marine Corps government civilian and uniformed personnel, who are presently NMCI users, to obtain a licensed copy of Microsoft Office, Project or Visio desktop applications to install and use on a home computer if these applications are installed on their NMCI computer. Contractors are ineligible to participate.

The HUP shall continue for the term of the HUP agreement and Department of the Navy personnel may take advantage of this offering provided they are employed by the DON and abide by the Home Use Rights End User License Agreement. The DON is not responsible for individual employee compliance with the terms and conditions of the EULA. The Department of the Navy shall undertake reasonable efforts to ensure that DON employees are notified of Microsoft provisions concerning the HUP.

The authorized HUP applications are accessible by logging on to the NMCI Homeport at https://www.homeport.navy.mil/news/articles/hup-license-info/. Should this link fail, enter "HUP" in Homeport's search feature to locate the Home Use Program page. Access to the Microsoft HUP Web site is limited to Navy and Marine Corps government civilian and uniformed personnel with authorized NMCI e-mail addresses only.

All DON personnel are reminded that personally identifiable information (PII) and controlled unclassified information (CUI) are not to be stored or otherwise used on personally owned laptops, desktops, personal electronic devices and other media storage.

There is a charge for paying the administrative costs of obtaining the software, including media and shipping. Navy and Marine Corps government civilian and uniformed personnel purchasing this offering may use the software as desired, provided they abide by the limitations stated above: PII and CUI are not to be stored on personal electronic media.

Navy and Marine Corps government civilian and uniformed personnel participating in the HUP may obtain only one version of the software at any given time and must comply with all licensing requirements.

Eligible software and ordering directions may be found at https://www.microsoft.com/licensing/sa/benefits/home_use_rights.mspx. Eligible licenses for this program are also listed.

Information Literacy Toolkit v. 2.1

The Information Literacy Toolkit is a practical and comprehensive guide to making information work for the individual, the organization and the enterprise. The Internet provides access and connectivity that requires new knowledge, skills, abilities and behaviors to take advantage of the great opportunities available to the DON workforce. Individuals must be able to recognize what information is needed when, and how to locate, evaluate, use and effectively communicate it. These skills are essential to bridging the gap between the sea of information available and an individual's ability to access, understand and apply it.

Go to the DON CIO Web site at www.doncio.navy.mil and click on the Products link to download the toolkit.

GOING MOBILE

BECOMING WIRELESS

By Tom Kidd, Department of the Navy, Director of Strategic Spectrum and Wireless Policy

In April 2008, the Department of the Navy Chief Information Officer (DON CIO) released a report called "Department of the Navy Enterprise Mobility 2008." This concise report describes the strategy the DON would use to leverage the significant advantages that commercially available wireless technologies can deliver to our warfighters and those who support them. The report is available for download on the DON CIO Web site at www.doncio.navy.mil under the Products link.

Enterprise mobility affects everyone and everything, everywhere across the DON. Though it may be less obvious for some of us than for others, we are all dependent on technology that connects to either a wired or wireless infrastructure. One of the department's greatest strengths is the interconnection of people and processes. Because of its unique mobility requirements, the DON has many more wireless connections than our civilian counterparts in industry.

As we move into the second decade of the 21st century, even more of these connections will become wireless. Before we enter the third decade, enterprise mobility through wireless technology will expand access to information wherever warfighters are located, regardless of the existence of a wired infrastructure.

However, all wireless technologies have inherent drawbacks and resultant concerns. Some of the key concerns are described below.

- Information Assurance. Can the traffic be intercepted and read by an adversary or easily jammed, thereby preventing information from getting through? This is particularly important as classified voice and Secure Internet Protocol Router Network (SIPRNET) communications will increasingly utilize wireless transport modes.
- Interference. Will introducing new radio frequency emanations into a military environment negatively impact existing systems? Interference can hamper communications, degrade the performance of collocated electronics, or even cause ordnance to malfunction, an effect called Hazards of Electromagnetic Radiation to Ordnance, or HERO.
- Robustness. Will the solution work across settings? For example, different frequencies have different propagation characteristics; what works well in a wide open environment may not work nearly as well in a shipboard environment with its numerous metallic enclosed spaces.
- Non-standard spectrum allocation. Differing spectrum assignments in some countries mean that some equipment cannot be used globally unless there is permission to operate from the host nation.

Implementation of wireless technologies cannot go forward until these potential drawbacks are satisfactorily addressed. Department of the Navy Enterprise Mobility 2008 describes the strategy the department is following in assessing and adopting commercially available wireless products.

To establish a governance framework and information repository to enable deployment of secure, interoperable, cost effective and capability enhancing wireless architectures, the DON CIO chartered the DON Wireless Working Group (DWWG) for Enterprise Mobility under the DON Information Executive Committee. The DWWG is a problem-solving forum. It makes recommendations to the DON Information Executive Committee regarding wireless solutions and strategies suitable for enterprise application.

The DWWG is a critical component of the department's efforts to minimize and manage the risk involved in introducing new technologies to the DON technical architecture. Since it was chartered in 2005, the DWWG has published policy and guidance and continually works to align wireless opportunities and capabilities with mission needs and DON deficiencies.

The key to the DWWG's success is the participation of DON employees with expertise in the enterprise application of commercial wireless technology and strategic planning, along with industry experts that have been invited to participate at discretionary junctures. Though chartered to emphasize virtual communication and collaboration, the DWWG periodically meets face-to-face to engage a broad audience of key stakeholders around the most promising and critical wireless issues facing the DON.

These face-to-face meetings have evolved into an annual summit. The 2009 DWWG Annual Summit will be held in conjunction with the DON Information Management/Information Technology (IM/IT) Conference Feb. 10-13, 2009, at the San Diego Convention Center in San Diego, Calif. Included in the agenda will be a wide variety of topics for discussion.

The DWWG Annual Summit is open to registered participants of the DON IM/IT Conference, which is held at the same time and location as West 2009, a conference cosponsored by AFCEA International and the U.S. Naval Institute. Details are available at www.doncio.navy.mil or www.west2009.org.

For more information about the DWWG, contact the DON Wireless Team at donwirelessteam.fct@navy.mil.

Tom Kidd is the Department of the Navy director of Strategic Spectrum and Wireless Policy. In addition to "Going Mobile" he also authors the CHIPS continuing series "Can You Hear Me Now?" which focuses on bringing the complex and often esoteric issues of electromagnetic spectrum to the broader DON community.

CHIPS

Trident Warrior 09 / Operational Level Command and Control

"Expanding the Maritime Experimentation Scope"

By Brad Poeltler, Tom Forbes and James Gabor

In December more than 250 representatives from 70 organizations, services and nations attended the main planning conference for Trident Warrior 09 aboard Naval Station Norfolk, Va. Trident Warrior is the premier annual FORCEnet Sea Trial event that executes in a series of experiments conducted ashore and at sea.

Vice Adm. H. Denby Starling II, commander of Naval Network Warfare Command, explained the benefits of Trident Warrior.

"Trident Warrior is an excellent opportunity to take a close look at up-and-coming capabilities in the maritime environment," he said. "Ultimately, it [TW 09] is designed to accelerate or deliver new or improved capabilities to the warfighter. Our objective is to find which systems and technologies are compatible with warfighter needs and which ones need to be improved upon."

Norfolk, Va. – Commander, U.S. Second Fleet, Vice Adm. Mel Williams Jr., gives his opening remarks to representatives from more than 70 organizations during the main planning conference for Trident Warrior 09. TW 09 will be hosted by Commander, U.S. Second Fleet and Naval Network Warfare Command, as the seventh experiment of the annual FORCEnet Sea Trial event, which will expand on the maritime experimentation scope from previous Trident Warrior experiments. U.S. Navy Photo by Mass Communication Specialist 1st Class Lolita M. Lewis.

TW tests command and control technology and doctrine

This is the seventh experiment in this annual event, and this year, TW 09 will expand the maritime experimentation scope. Directed by NETWARCOM, and 2nd Fleet, the TW 09 fleet sponsor, TW typically focuses on the at-sea technical experimentation of critical maritime technologies. However, this year TW 09 will take advantage of the installed networks and committed assets of 2nd Fleet, supported by Navy Warfare Development Command (NWDC), to examine Maritime Headquarters with Maritime Operations Center (MHQ w/MOC) operational-level processes under the Sea Trial experiment titled: Operational Level Command and Control (OLC2).

According to Vice Adm. Melvin Williams, Second Fleet commander, "The Trident Warrior 09 Operational Level of Command and Control experiment is an excellent opportunity for 2nd Fleet and Naval Network Warfare Command to explore experimental concepts and technologies to benefit the Navy and joint forces.

"It will influence future force development, as well as enhance teaming with our allies and partners while exploring operational command and control flexibility, consistency, capability and capacity towards improved mission effectiveness," Williams said.

This effort leverages the capabilities of a global maritime partnership, along with emerging tools, processes and procedures to reduce uncertainty and speed decision making, thus improving maritime security among maritime partners.

"The merging of Navy technical and doctrinal experimentation in partnership with our allies will further operational level of war processes and supporting tools development," said Capt. Steve Swittel, NWDC's experimentation director.

TW 09, including OLC2, will be conducted during June and July 2009 ashore at commands in the Norfolk area and at sea on ships in the Virginia Capes operating area.

Ashore commands involve more than 14 nodes including 2nd Fleet headquarters, Naval Computer and Telecommunications Area Master Station Atlantic and the Unified Atlantic Region Network Operations Center.

The OLC2 experiment will be the inaugural experiment using the capabilities of Maritime Operations Center-Experimental (MOC-X) collocated with 2nd Fleet Maritime Headquarters in Norfolk, Va. Featuring a global network of maritime headquarters among U.S. and multinational partners, the products of the experiment will contribute to doctrine and tactics, techniques, and procedures development. The at-sea portion will be conducted on USS Nassau (LHA 4), USS Normandy (CG 60), USS Farragut (DDG 99), USS Bulkeley (DDG 84) and USS Alexandria (SSN 757).

TW 09 and OLC2 are planned and conducted by an experienced, highly skilled planning staff from 2nd Fleet, NETWARCOM, NWDC, Space and Naval Warfare Systems Command (SPAWAR) and the Naval Postgraduate School, with specific skills in experiment design and operational planning.

"The level of experience and expertise that everyone brings to Trident Warrior each year just keeps getting better and better," Starling said. "When you bring people of this caliber together in a venue such as this, you're saving valuable time when assessing these technologies and processes. When looking at the big picture, this allows us to move these capabilities to the warfighter much sooner."

Technical experimentation from TW 09 and OLC2 is designed to provide answers to detailed analytical questions involving more than 115 separate FORCEnet technologies. These efforts will involve more than 30 shore-based and 70 shipboard installations with each one adhering to ship maintenance, security

accreditation, network certification, Fleet Readiness Certification Board, and Regional Maintenance and Modernization Coordination Office processes. A tremendous effort by all process owners is required to facilitate this large volume of installations in a short window.

To carry out this huge effort, technologies are organized into 10 specific focus areas:

✓ Networks: Among the 16 networking technologies will be the installation and experimentation with Consolidated Afloat Networks and Enterprise Services (CANES) blade servers both ashore and afloat operating on classified and non-classified networks.

✓ Coalition: Seventeen technologies to be used by the AUSCANNZUKUS alliance, which includes Australia, Canada, New Zealand, United Kingdom and the United States, will be tested aboard U.S. and coalition ships and in host nations.

✓ Information Operations: Several new signals intelligence (SIGINT) detection and integration capabilities will be included in 16 information operations technologies.

✓ Command and Control applications: Several common operational picture and situational awareness collaboration tools are among 16 individual technologies is this focus area.

✓ ISR: Multi-source integration of manned and unmanned space, air, surface and subsurface sources will be included in 11 intelligence, surveillance and reconnaissance related technologies.

✓ Electronic Warfare: Precision targeting technologies are among the six technologies to be tested in this focus area.

✓ Distance Support: Several technologies designed to provide automated logistic and maintenance information from deployed ships back to shore analysis nodes are part of the eight technologies being tested.

Second Fleet's Goals for TW 09 and OLC2 Experimentation

Fleet Operations to achieve mission
- Fleet operations – safe and effective day-to-day
- Joint Task Force capable headquarters sustainment
- 2nd Fleet MHQ w/MOC development

Providing ready maritime forces for global assignment
- Fleet training and readiness
- Global force management
- Future force development
- Develop Leaders

Teaming with allies and partners in execution of the maritime strategy
- Combined Joint Operations from the Sea Center of Excellence (CJOS COE)
- Allied and multinational maritime partnerships

✓ Information Assurance/Cross Domain Solutions: Tools designed to defend against cyber attacks will be tested by an aggressive Red Team assault and are among 11 information assurance and CDS-related technologies being examined.

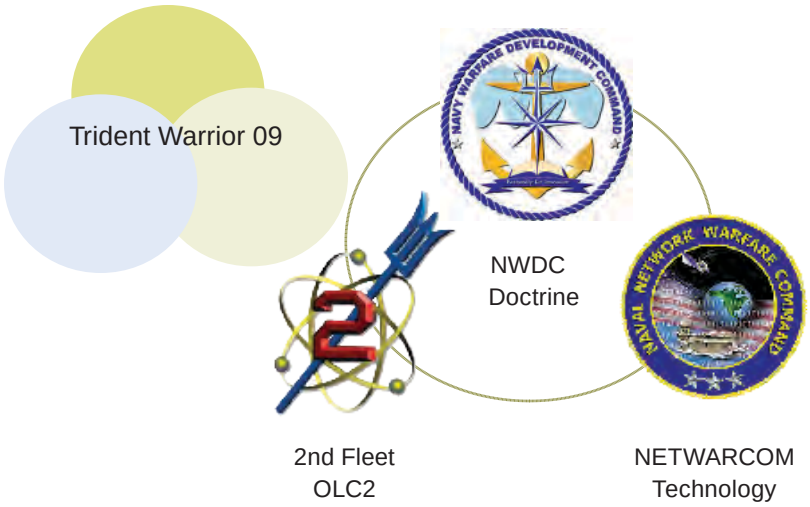
✓ Information Transport: C2 High End Warfare (warfighting in a satellite denied environment) will be one of the major focus points in this area which includes seven new technologies.

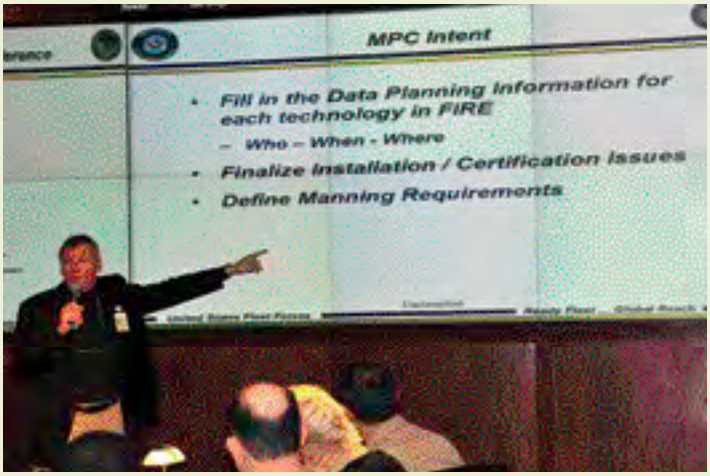
✓ Maritime Domain Awareness: Rapid sharing of vital information concerning ships, passengers and cargo within the U.S. and coalition military forces and law enforcement is the focus of the 10 MDA tools to be tested.

TW 09 and Operational Level Command and Control (OLC2) doctrinal and process experimentation will provide procedural insight into the following four major focus areas:

• MOC-to-MOC and coalition collaboration – Test and explore the MHQ MOC-to-MOC core planning cycle processes in response to a maritime threat. Explore and evaluate MOC-to-MOC

TW 09 Combines Doctrine with Technology





Norfolk, Va. – Brad Poeltler, deputy director for Trident Warrior, briefs representatives from more than 70 organizations on the planning and mission for Trident Warrior 09. Trident Warrior is the Navy's major annual operational FORCEnet experimentation event encompassing discovery, review, selection, analysis, and assessment of networks, technologies, processes and procedures that will provide significant advancements or improvements in naval forces command and control.

Norfolk,Va. – Mr. Magnus Addico, Secretary General of the Maritime Organization of West and Central Africa (MOWCA), briefs representatives from more than 70 organizations, while attending the main planning conference for Trident Warrior 09, addressing his concerns for maritime security along the Gulf of Guinea and the steps in which working with the Africa Partnership Station (APS) will help to establish coastal security. U.S. Navy photos by Mass Communication Specialist 1st Class Lolita M. Lewis.

collaborative processes to support maritime threat prosecution monitoring. Examine the operational effectiveness of communications networks and systems needed to facilitate and support MOC-to-MOC collaboration.

• Information Operations – Identify and evaluate capabilities and limitations associated with mission planning support, course of action development and mission analysis from the federated IO domain. Identify and evaluate the INTEL/SIGINT processes and support required to satisfy IO requirements to meet MOC assessment, planning and execution.

• Maritime Situational Awareness (MSA) – Develop and examine external MOC MSA processes, collaboration and information sharing requirements between U.S. Navy MOCs and intelligence centers, other Defense Department and U.S. agencies' operations centers and coalition MOCs.

• Seabasing – Identify required capabilities of the sea base supporting low-intensity missions. Evaluate considerations required to position, embark and sustain forces on a sea base conducting low-intensity missions. Analyze the responsibilities and supporting relationships between the sea base and the supported theater headquarters and potential MOC forward element in force management, logistics and command and control.

TW recommends programs of record development

Each TW experiment is presented to the Sea Trial Executive Steering Group (STESG) with specific recommendations. Typically these recommendations are to develop or accelerate a program of record (POR) or deliver a first of a kind capability within the budget cycle.

"What the STESG typically doesn't see are feedback and design improvements to existing PORs which often happen on the spot at the technician or action officer level. These make up the vast majority of a TW's success and applicability. TW has made a tremendous impact on the fleet's warfighting capabilities since 2003," said Capt. Vince Giampaolo, director for NETWARCOM innovation and experimentation.

Prior to implementation of the Trident Warrior series in 2003, each systems command (SYSCOM) conducted independent network experimentation programs with each program focused on testing one or two technologies at a time. This method provided limited objective experiments (LOE) for each SYSCOM each year. Each of these LOEs required separate planning, design, network development, asset coordination, data collection and analysis teams. There was not a formal or consistent reporting process or an event data repository.

Since Trident Warrior's inception, SYSCOMs have come to rely on TW as a dependable FORCEnet experimentation event which provides the Navy with a quality venue to experiment with more than 100 technologies annually.

"One single team plans, designs, develops networks, collects data and provides analysis. TW also records all of the planning and analysis information in a single Web-based planning and data collection repository," said Dr. Shelley Gallup, TW lead for data collection and analysis from the Naval Postgraduate School.

"TW 10 planning is already underway to continue this beneficial experimentation series next year. In concert with Commander, Third Fleet during [the] RIMPAC 10 multinational exercise, TW 10 will continue to focus on FORCEnet technology development, but we'll do it, as in TW 09, with a procedural and doctrinal point of view," said Cmdr. David Varnes, NETWARCOM's director for the Trident Warrior series.

Brad Poeltler is a retired U.S. Navy captain and the deputy director of Trident Warrior.

Tom Forbes is a retired U.S. Navy captain and the 2nd Fleet science advisor.

Jim Gabor is a retired U.S. Navy commander and the NWDC deputy director for OLC2 experimentation.

CHIPS

DON Enterprise Architecture Development Supports Naval Transformation

By Victor Ecarma

Introduction

Federally mandated enterprise architectures (EA) are a strategically-based means for the departments of Defense and the Navy (DON) to capitalize on their vast technological assets and make sound decisions about investments in new technology that will support the warfighter.

The DON is a complex organization with disparate architecture development efforts and finite resources. Effective, cross-departmental decision making in today's environment relies upon information technology as a fundamental enabler, yet the DON information infrastructure is quite complex and subject to continual change. Herein lies the requirement for a DON EA that would create the framework for effective, real-time, decision making and policy implementation across multiple DON departments. The DON EA's success is dependent upon its relevance and value to DON decision makers.

As the chief architect, the DON Chief Information Officer (CIO) is leading the effort to design and develop a single DON EA, using a strategy that federates with external partners and incorporates an integrated, coordinated, flexible and long-term strategically focused approach. The DON EA describes the processes, information flows, solutions, data descriptions, technical infrastructure and standards that are integrated to achieve current and future DON strategic goals and objectives.

The DON EA assists decision makers in the execution of major decision processes such as the Defense Acquisition System, Planning, Programming, Budgeting and Execution, and the Joint Capabilities Integration and Development System.

The creation and implementation of a DON EA will support naval transformation in delivering value by:

- Creating IT Agility. Create the foundation for planning future capabilities and adapting to changing environments.
- Reducing Complexity. Minimize duplication of technology in the infrastructure by consolidating products and tools providing similar functionality. Enable Information Technology/National Security Systems (IT/NSS) to consolidate expertise around fewer technologies.
- Lowering Operational Costs. Reduce the cost of business operations by optimizing IT/NSS acquisition, support, maintenance and training costs. Enable reusability and drive standard technologies.
- Enhancing Portfolio Management. Eliminate duplicative investments; re-prioritize investments — invest once — use many.

EA Strategy: External Federation and Internal Integration

Since the release of the Global Information Grid (GIG) Federation Strategy in August 2007, the DON CIO has tailored the federated approach in developing and managing the DON EA. The DON EA will federate with DoD and other external partners.

Federation is defined as "a process for relating disparate architectures that allows for uniqueness and autonomy while maintaining line-of-sight to strategic objectives. This process focuses on aligning architecture to a high-level taxonomy. The aligned architectures and their architecture information are then located and linked via the employment of an architecture management service using a standard set of metadata to allow for consistent search and discovery."

Federation techniques allow disparate architectures to be meaningfully related and permit acceleration of new architecture efforts across the DoD community to support decision makers.

The DON EA provides an integrated approach that uses common architecture descriptions and data elements across all architecture products and views. An architecture is considered an integrated architecture when models and their constituent architectural data elements are developed such that architecture data elements defined in one view are the same (i.e., same names, definitions and values) as architecture data elements referenced in models in another view. For more information, refer to DoD Architecture Framework (DoDAF) version 1.5.

To enable this integrated approach, the DON CIO, in collaboration with DON Deputy CIO (Navy), DON Deputy CIO (Marine Corps), and Assistant Secretary of the Navy for Research, Development and Acquisition (ASN(RDA)) Chief Systems Engineer (CHSENG), is developing the following:

- ✓ DON EA Hierarchy – a structure based on the Joint Staff-developed Joint Capability Areas (JCAs) to relate the complete set of activities occurring within the DON.
- ✓ DON EA Governance – an overall governance structure that clearly defines the roles and responsibilities for development, review, verification and validation, approval, use and enforcement of architectures across the DON.
- ✓ Naval Architecture Elements Reference Guide (NAERG) – standardized architectural elements, based on common terms, which form the elemental building blocks of the architecture.
- ✓ DON EA Implementation Plan for the GIG Architecture Federation Strategy – a single set of DON-level federation rules and guidance for use by all developers of DON Segment Reference Architectures (SRAs) to federate with external partners.
- ✓ DON EA Product Style Guide – formatting and style requirements for architecture products.
- ✓ DON EA Project Management Plan – a schedule for developing Segment Reference Models, SRAs and supporting governance and other management processes.
- ✓ DON EA Development Management Process – DON EA development criteria and process to manage EA development activities of DON SRAs and enterprise solutions to ensure EA efforts align to DON strategic goals and objectives.

Compliance

The Federal Enterprise Architecture Framework was established in response to the Clinger-Cohen Act (CCA) of 1996 mandating that executive agencies develop and maintain an EA. One of the compliance criteria of the CCA requires that acquisitions are consistent with Defense Department IT policies and architectures.

To make the DON EA relevant and not "architecture for architecture's sake," the DON CIO, in close coordination with Deputy Chief of Naval Operations for Communication Networks (OPNAV N6); Headquarters Marine Corps, Command, Control, Communications, Computers (HQMC C4); and ASN(RDA) CHSENG, is currently strengthening processes to tie investment decisions to assessments of architectural compliance making the DON EA a compliance component for IT/NSS investments through the following initiatives.

✓ The DON Deputy CIO (Navy) issued the Navy Enterprise Architecture and Data Strategy April 7, 2007, which states that Navy programs, projects, systems, capabilities and investments that are not in compliance with the DON EA and Navy architectures will have their funding withheld.

✓ The DON Deputy CIO (Navy) stood up the IT Management Council in May 2008 to oversee the development of Navy architectures.

✓ The DON Deputy DON CIO (Marine Corps) stood up a Marine Corps Enterprise Architecture Working Group in May 2007 to provide policy and guidance to enable Marine Corps EA planning, development, use and evolution throughout the entire life cycle of the Marine Corps EA program.

✓ The DON CIO is drafting a DON EA policy that will implement similar enforcement mechanisms across the DON.

✓ ASN(RDA) CHSENG is using DON EA compliance as criteria during acquisition program reviews.

✓ The DON CIO is in the process of developing a proactive approach to CCA certification for Major Automated Information Systems and DON IM/IT Special Interest Programs. A key component of this proactive approach will be assessment of proposed investments against the DON EA.

This policy is part of the evolving implementation of Title 40/CCA aimed at reinvigorating oversight, maximizing up-front involvement in the IT investment process and eliminating redundancies. (Title 40 of the United States Code formerly Division E of the Clinger-Cohen Act of 1996 for Major Automated Information Systems (MAIS) and Major Defense Acquisition Programs (MDAP) in the Department of Defense.)

Describing the DON EA

The DON EA is a framework comprised of a Capstone Layer and

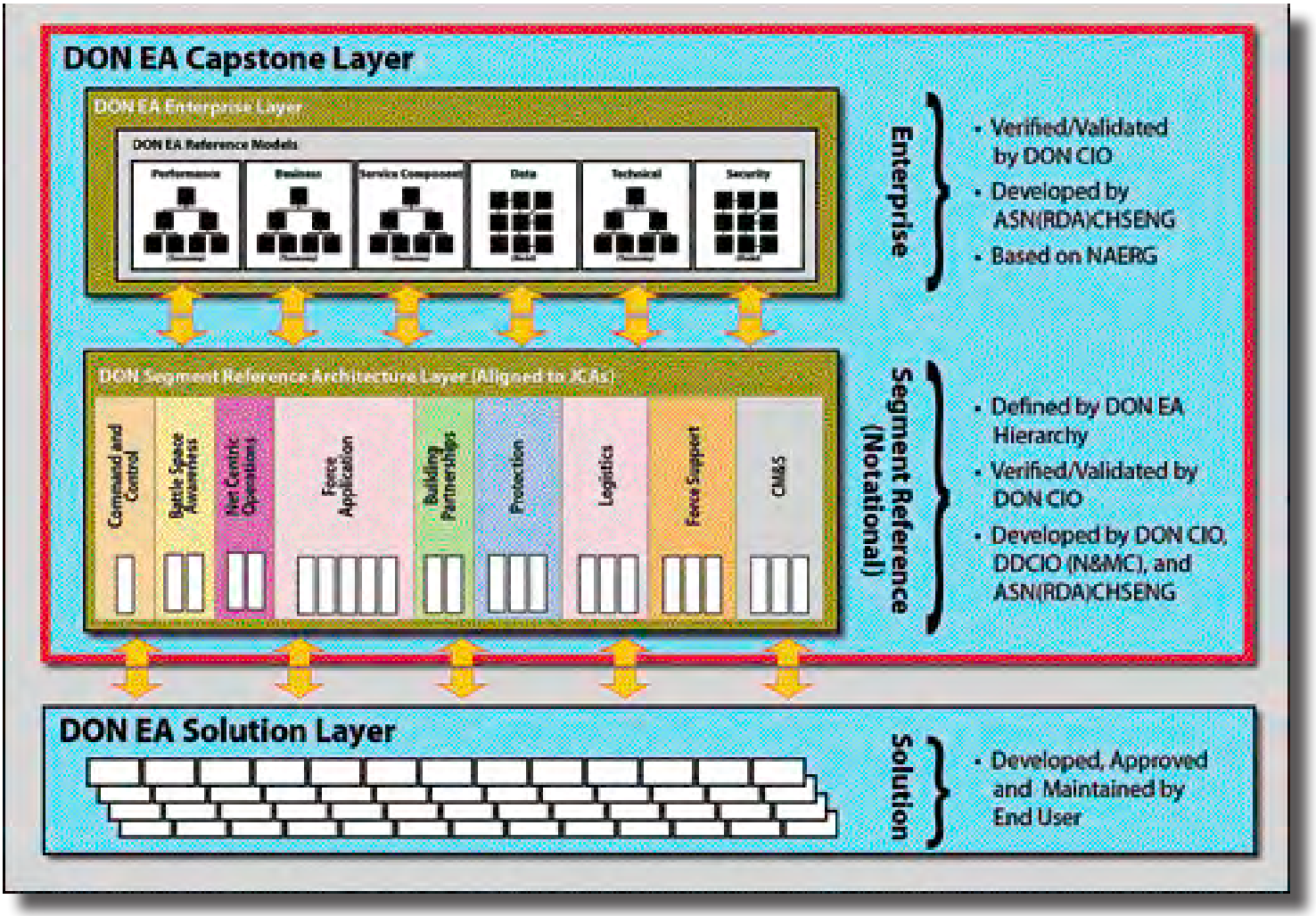


Figure 1. DON Enterprise Architecture Framework.

a Solutions Layer as shown in Figure 1. The DON EA Capstone will be comprised of two tiers: the DON EA Reference Models and DON Segment Reference Architectures. The reference models will be based on the Federal Enterprise Architecture (FEA) reference models and will provide the standards to which architectures are to be developed, approved and used. The Department of the Navy SRAs will define what DON missions are aligned to each Joint Capability Area.

Establishing standards before development occurs ensures interoperability and integration between distributed architectures. The Reference Models provide a framework for understanding significant entities and relationships between them within an environment.

Using the analogy of a city blueprint, an architecture blueprint is an important EA tool that creates a plan for a city's assets. The reference architecture defines the building codes and standards. Architects use the reference architecture as a lens to understand the current state of the architecture portfolio of assets and map the architecture transition to the future state.

The FEA consists of a set of interrelated "reference models" designed to facilitate cross-agency analysis and the identification of duplicative investments, gaps and opportunities for collaboration within and across agencies. Collectively, the reference models comprise a framework for describing important elements of the FEA in a common and consistent way.

There will be six DON EA Reference Models derived from the FEA reference models that will provide the codes and standards to build the DON EA:

✓ Performance Business Reference Model – Provides frameworks or standards to measure the performance of major IT investments and their contribution to program performance.

✓ Business Reference Model – Provides an organized, hierarchical construct for describing day-to-day business operations.

✓ Service Component Reference Model – Business and performance driven, functional framework that classifies service components with respect to how they support business and performance objectives.

✓ Data Reference Model – Describes, at an aggregate level, the data and information supporting government program and business line operations.

✓ Technical Reference Model – Component driven, technical framework used to categorize the standards, specifications and technologies that support and enable the delivery of service components and capabilities.

✓ Security Reference Model – Provides a methodology for developing low risk enterprise information security designs and delivering security infrastructure solutions that support critical business initiatives directly from the Business Reference Model.

Within the DON EA Segment Reference Architectures, there is a hierarchy that provides a structure to relate the complete set of activities occurring within the DON. This hierarchy is intended to provide the link between the DON SRAs and program-level architectures. It does so by placing these activities in relation to the DoD EA; the Joint Staff Joint Capability Areas; the Business Transformation Agency Business Enterprise Architecture; the functional areas defined by the Assistant Secretary of Defense for Networks and Information Integration; and those functional areas to be defined by the intelligence community.

In addition, the Department of the Navy SRAs will be collaboratively updated and used as a tool by DON senior leadership and Functional Area Managers to drive: (1) net-centric transformation and data sharing; (2) business transformation and process standardization; (3) investment recommendations and decisions; and (4) financial audit ability and internal controls.

The goal of the architecture design is to improve direct and indirect support to the Secretary of the Navy, Commandant of the Marine Corps and Chief of Naval Operations, thus enhancing the DON's ability to execute its mission.

DON EA Development Management Process

The DON EA Development Management Process aligns and synchronizes Navy and Marine Corps EA development and initiatives that contribute to the development and use of the DON EA to support naval transformation. The process will manage EA development activities within the DON EA Segment Reference Architectures and identified enterprise solution architectures; ensure EA efforts align to DON strategic goals and objectives; determine the value provided by each effort; and monitor and track progress.

The DON EA Development Management Process will enable transformation of business processes and modernize supporting IT/NSS systems to minimize overlap and maximize interoperability.

DON EA Development Management Process goals will:

✓ Align non-architecture strategic goals with DON EA development initiatives;

✓ Describe DON EA goals and how to determine success;

✓ Capture milestones and metrics to guide improvements in business and warfighting capabilities;

✓ Identify tangible benefits for each investment in naval transformation; and

✓ Identify gaps where architecture efforts are needed to solve non-architecture problems and support non-architecture initiatives.

The DON EA development management and process will require EA development efforts before they are started to identify and document the value to the DON, ensure there is no duplication of effort and prioritize activities to maximize resources while producing the most benefit.

Although this process will be maintained by the DON CIO, it will be created and treated as a living document and continually revised by key stakeholders.

The DON CIO is laying the foundation for the DON EA to be relevant and sustained within the department. The DON EA will achieve the DoD's vision of a more agile and integrated organization whose systems are aligned and synchronized.

Through incremental steps, this effort will contribute to naval transformation by shifting away from isolated stovepiped requirements development to one in which organizations understand and embrace cross-community development.

For information on the DON CIO's DON EA development efforts, please visit the DON CIO Web site at www.doncio.navy.mil. CHIPS

CAN YOU HEAR ME NOW?

HOW ONE IDEA CAN CHANGE THE WORLD

By Tom Kidd
Department of the Navy, Director of Strategic Spectrum and Wireless Policy

In less than two years, nearly 150 distinguished ambassadors and more than 2,000 delegates from across the globe will gather for the United Nations International Telecommunication Union's (ITU) World Radiocommunication Conference. During this four-week marathon, committed delegations will scrutinize, debate, create and revise the international treaties that govern the regional and global use of electromagnetic spectrum or radio frequency spectrum.

The final acts of World Radiocommunication Conference 2011 (WRC-11) will receive little if any fanfare beyond stakeholder communities, such as those engaged with cellular telephone service, advanced wireless services and other spectrum-related services, even though the results of this gathering will have direct, significant and global implications to all of us who depend on wireless capabilities that can only be enabled by use of the electromagnetic spectrum — and in the 21st century — it is impossible to imagine a life that isn't directly, or indirectly, dependent on the electromagnetic spectrum.

Much of our modern way of life would be impossible without access to the electromagnetic spectrum. The Department of the Navy (DON) is highly dependent on spectrum-enabled capabilities that provide a multitude of the Navy's and Marine Corps' communication, sensor, intelligence, combat and other capabilities that are vital to the naval services' ability to meet their global responsibilities.

Due to the significant implications to Navy and Marine Corps spectrum capabilities, the DON either closely monitors or actively participates in every WRC preparatory venue to protect the naval services' equities or to advocate for changes that enhance their capabilities.

Additionally, the DON ensures its interests and positions with WRC issues are known and aptly represented by the United States delegation, which includes personnel from the Department of Defense, as well as the DON.

The issues that will be decided at WRC-11 are incredibly diverse as they have been in past conferences. Items on the WRC-11 agenda of particular interest to the DON include current, emerging and future radio applications; unmanned aircraft systems; ship and port safety systems; sea surface radar; and software defined radios. The complete WRC-11 agenda will be available on the DON Chief Information Officer (CIO) Web site at www.doncio.navy.mil, or you can view it now on the ITU Web site at www.itu.int/.

It is inarguable that one of the most important WRC-11 agenda items is the one that requests and ultimately determines future agenda items for later WRCs. Proposed agenda items can be submitted by all participating delegations.

However, the genesis of any particular agenda item is often traced to one or more individuals in organizations involved with research, development, or the operation of spectrum-enabled capabilities. More often than not this can be traced back further to one idea — one idea that ultimately will change the world.

As such, DON program managers, spectrum managers and anyone else in the department associated with research, development, acquisition, governance, or the operation of spectrum-dependent systems or devices, has an opportunity to propose issues that may result as a WRC agenda item.

International governance, spectrum services, radio frequency interference and emerging technologies are just a sampling of issues that "bubble up" from individuals with a regional or global spectrum challenge or a spectrum solution.

It is through the WRC that DON personnel are able to defend and advance the capabilities of the Navy and Marine Corps by improving or modifying the world's use of spectrum. Regulations and procedures for frequency management, in the United States, and the host nations in which our troops train, are grounded in the international treaties that are made and modified at the WRC.

American anthropologist Margaret Mead said, "Never doubt that a small group of thoughtful, committed citizens can change the world. Indeed, it's the only thing that ever has."

Ideas to change the world, or recommendations for future WRC agenda items, should be sent to the DON Spectrum Team at donspectrumteam@navy.mil.

Tom Kidd is the Department of the Navy director of Strategic Spectrum and Wireless Policy and was a delegate to the World Radiocommunication Conference in 2007. In addition to "Can you hear me now?" he also authors the recurring CHIPS series "Going Mobile" which makes its debut in this issue and focuses on enterprise mobility and the DON Wireless Working Group. CHIPS

In 1979, the Navy initiated the annual Title X Global War Game as part of its Cold War strategy development process. Part of this effort included the analysis of future force structures as part of the Navy's Title X authority to man, train and equip naval forces.

Hosted by the Naval War College in Newport, R.I., these war games were suspended in the years immediately following the terrorist attacks of 9/11, due in part to a lack of "compelling geopolitical reasons," according to Dr. Robert Rubel, Dean of the Center for Naval Warfare Studies at the Naval War College.

However, in response to increased interest by senior Navy and Marine Corps leaders, the Title X Global War Game was reinstated this past summer. The intent of this seminar-style war game is to aid participants' understanding of implications and challenges of implementing the new U.S. maritime strategy: "A Cooperative Strategy for 21st Century Seapower."

The results from Global '08 will be used to inform capabilities analysis, force design and future concept development. The more immediate results are maritime strategy familiarization and to promote international engagement.

From Aug. 4-8, the war gaming department at the Naval War College hosted Global 2008 on behalf of the Chief of Naval Operations in an effort to examine the challenges, issues and implications of implementing the new U.S. maritime strategy.

The 200 participants consisted of individuals from across the maritime services, the joint community; partner countries including representation from 19 navies; U.S. government agencies; international and nongovernmental organizations; and the shipping and defense industries. International participants added their expertise and perspective to the activities.

Team SPAWAR, the Space and Naval Warfare Systems Command, was well represented at Global 2008, which was also attended by members of the director for warfare integration, within the office of the Deputy Chief of Naval Operations for Communication Networks (OPNAV N6).

Attendance by OPNAV N6 contributed to participants' understanding of the capabilities — and limitations — of current and emerging naval networks. It also provided members of the Naval NETWAR FORCEnet Enterprise (NNFE) with a well-nuanced understanding of the operational needs of Navy, joint, interagency and coalition partners.

To this end, Global 2008 explored how the execution of the maritime strategy might look under one of four alternative futures developed by the Navy strategic planning process, from regional and global perspectives.

The scenarios included variations in cooperation by global partners and also included extremist elements. Players developed perspectives on how their particular future would look in their specific region through the lens of political, military, economic, social, infrastructure and information (PMESII) concerns, and then identified the maritime tasks and capabilities that would be required for mission success.

Over the course of the week, several overarching themes emerged. The necessity for interagency and international collaboration as a key requirement of successful implementation of the maritime strategy loomed large. To this end, there was an emphasis on practices and technology that facilitate cooperation and coalition building. Moreover, nontraditional and soft power activities were common threads to three of the four alternative futures, with a clear emphasis on activities aligned to the prevention of war.

With respect to the technology requirements that emerged from Global 2008, one must first caveat that by the game's very nature, specific platforms and systems were not discussed. Instead, looking to the broader themes that emerged from the game, in many of these scenarios one could surmise the applicability of critical technologies to enable the missions that were forecasted by playing out the scenarios.

Consider that the number and size of Navy ships is not likely to increase, but the importance of protecting the global commons will increase. The ability to quickly aggregate forces in response to disruptions to the global system becomes paramount. These disruptions run the gamut from natural disasters and their accompanying humanitarian and disaster relief missions, to pirate attacks in and out of the sea lines of communication, to kinetic missions in response to rogue state and non-state actors, to traditional conflicts with major powers.

Game participants generally agreed that increased maritime domain awareness and information sharing, particularly with organizations outside of the Defense Department, would fill an important requirement in response to a global crisis.

In terms of the kind of technologies that may be needed to support and enable a more agile Navy, one area that comes to mind is more robust C4ISR, or command, control, communications, computers, intelligence, surveillance and reconnaissance, capabilities.

"Daily media communications illustrate that we live in a fast-paced, interconnected and volatile environment. Nonetheless, it is reassuring to know that as guardians of peace, our United States Navy is continually postured across the globe to protect our nation's interests. SPAWARRIORS should be equally proud of our continuing contributions in sustaining and advancing our nation's war on terrorism through science and technology, research and development, and actual installation and sustainment of critical C4ISR and space systems.

"Whether human assistance/disaster relief missions, combating piracy or high-end warfare, SPAWARRIORS are directly contributing to our nation's national security. Likewise, SPAWAR's contributions to CNO's modeling and simulation endeavors, and our most recent support to the Global War Game 2008, illustrate that our role is now expanding.

"I am most proud of our SPAWARRIORS that both supported and participated in Global War Game 2008. Their endeavors highlighted the criticality of our systems in fostering collaboration with interagency, nongovernmental and international organizations in executing a maritime strategy that directly supports our combatant commanders. And equally important, they have significantly contributed to posturing our Navy to better understand and respond to future world events."

Rear Adm. Michael C. Bachmann
Commander, Space and Naval Warfare Systems Command
Oct. 14, 2008

Likewise, operational integration across the services, which presents numerous issues today, will need to become seamless; while the ability to effortlessly operate with our international partners, commercial entities, NGOs and other stakeholders will be the linchpin for a global maritime system.

Doing more with less, the watchword for tomorrow's maritime forces, requires close collaboration. While not explicitly discussed in the game, one could conclude that several technologies in development today may provide the means for the future Navy to perform more tasks with fewer resources.

First, the increasing importance of unmanned systems could serve as a force multiplier allowing not only better ISR, but also strike capabilities across all warfighting platforms.

As pointed out by the Naval Studies Board, "these critical surveillance applications can provide high-leverage knowledge that acts as a force multiplier" for a wide range of missions.

For the Navy to become a more agile force, streamlining manpower requirements is extremely important due to the increasingly high costs of manning, equipping, and training Sailors and Marines. In response to those forcing functions, the second technology trend, better human-systems integration comes into focus.

This begins with interfaces leveraging best practices from today, and technologies of tomorrow, to create the hardware and software that can allow a well-trained 2nd class operations specialist to provide the same or higher level of situational awareness that several Sailors do today.

This will require a C4ISR suite capable of handling thousands of bits of discrete data from many sources and synthesizing these bits of information for a distributed C4I reach-back capability. This integration of commercial, geographic, financial, intelligence and military data sources into a C4I system will help users develop plans of action based on all the available knowledge and information.

The emerging taxonomy known as "Intelligent Composeability" captures the essence of this capability and is one that Team SPAWAR continues to develop as part of its technical vision.

Achieving the ability to "intelligently compose" the capabilities demanded in the operational environment will require a host of technologies including better use of existing bandwidth to support the huge throughput of data required for this to work, through a combination of better data compression, increased data rate technologies, and more efficient use of the radio frequency spectrum.

Along the same lines, a high level of integration within the ship's systems must be complemented by a tightly integrated maritime force, requiring robust data standards, common software and hardware architecture, and in close cooperation with our allies.

Global 2008, by virtue of the alternative futures presented, provided participants with a complex world requiring them to identify issues and derive missions, tasks and capabilities to deal with a set of realistic threats. Based on these futures, participants concluded that the military, and in particular the maritime forces, will be increasingly asked to perform a diverse range of missions including many nontraditional ones to support ad hoc coalitions of joint, interagency, multinational, commercial and nongovernmental organizations.

Participation by Team SPAWAR and the NNFE at Global 2008 contributed to the participants' understanding of the importance of robust C4ISR networks in accomplishing this mission set. For Team SPAWAR participants, it also provided an opportunity to understand how technologies in development today may apply in a range of possible futures.

Once analysis is complete, long-range results from Global 2008 are intended to provide the Navy with strategies for future efforts such as the Quadrennial Defense Review. The analysis will also shape the decision to hold future games in this series.

José Carreño is a senior analyst who works for the Space and Naval Warfare Systems Center Pacific in the Corporate Strategy Group.

Antonio Siordia is a research analyst who works for SSC Pacific in the Corporate Strategy Group.

CHIPS

METOC Data Management for Net-Centric Operations

A strategy for sharing information across the joint METOC community

By Dr. Roy Ladner

The departments of Defense and the Navy have adopted a data sharing strategy that supports network-centric operations on the Global Information Grid (GIG). This strategy redefines interoperability from traditionally defined point-to-point interfaces between databases and applications, to a many-to-many data exchange where many users and applications may leverage the same data on the network.

This level of interoperability is generally made possible where data is made visible on the network, as well as discoverable and understandable through the addition of relevant metadata, for user accessibility. Such data management requires the collaborative efforts of communities of interested users who must exchange data.

The meteorological and oceanographic (METOC) community of interest (COI) has been actively addressing net-centric data management issues through the work of its Data Management Working Group.

The DMWG consists of data managers, subject matter experts and end-users from the Navy, Air Force, Army and Marine Corps; it operates under the governance of the Joint METOC Board. More recently, the National Weather Service and Federal Aviation Administration (FAA) joined the DMWG to address data interoperability issues between those federal agencies and the DoD.

The FAA, for example, has recently adopted the METOC COI data exchange standard, the Joint METOC Broker Language, as a key-enabling technology to exchange meteorological data with the National Oceanic and Atmospheric Administration (NOAA) and DoD for the Next Generation Air Transportation System.

Figure 1 outlines the DMWG's work toward net-centric operations. We began by developing the Joint METOC Conceptual Data Model (JMCDM). A conceptual data model generally describes significant concepts in a given domain and the relationships among them. Subject matter experts working with the DMWG developed JMCDM through collaborative sessions over the course of several years. The resulting model provides an organizational framework for a common understanding of METOC terminology and data attribution.

Once the JMCDM was complete, we began work on a physical data model. Unlike a conceptual model, a physical data model takes into account data organization within a database management system and may identify table structure, indexing, and other data organization elements.

We segmented the physical model by like data elements to provide data organization around high-level data types such as observations, climatology, forecasts and other categories. This resulted in 13 physical database segment models. Some service members of the community implement these physical models while others merely map their existing data stores to the models.

METOC production centers dynamically populate their data stores with perishable environmental data. This is a process in which they ingest, update, archive and delete data on a regular, real-time basis. The management of the data flow into and out of these data stores is performed by numerous data storage systems and data management applications in disparate locations and environments.

To avoid specific point-to-point interfaces for each of these data stores, we developed the data exchange standard interface known as the Joint METOC Broker Language.

JMBL is implemented in Extensible Markup Language (XML) and consists of a series of schema that define the structure of a request for METOC data and the structure of the associated response. JMBL allows each METOC data provider to offer a uniform interface for machine-to-machine access to METOC data on the GIG.

The JMBL schema are associated with a Web Service Definition Language (WSDL) file that lists the service provider's URL and available methods exposed through the service.

We designed JMBL sufficiently broad to be able to address the data needs of a

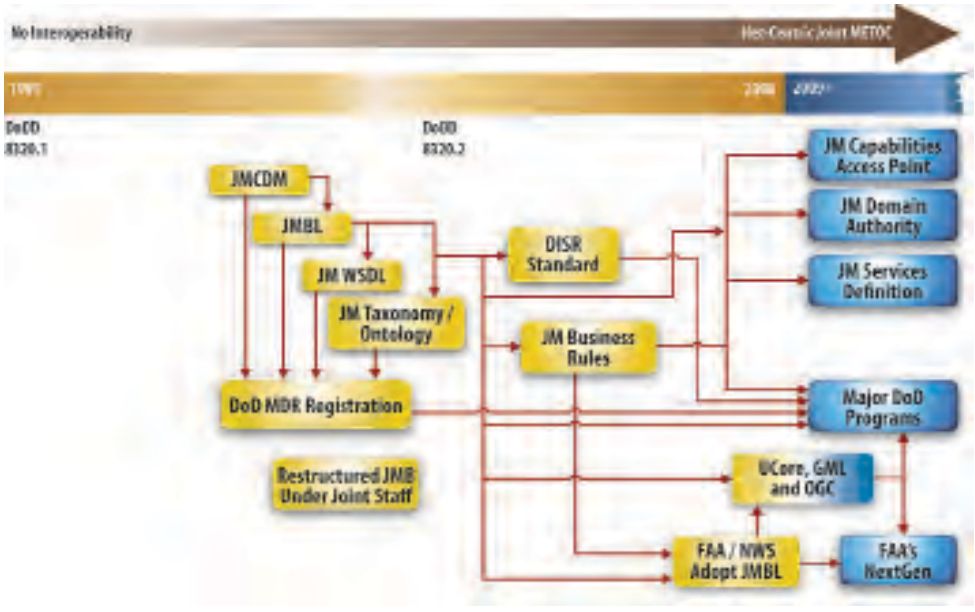


Figure 1.

broad range of users from the novice to trained METOC expert. For example, JMBL permits a user to define time and location relevant to needed data several different ways: five for time and four for location.

A METOC expert may require different combinations of these elements while the novice usually needs only one. Although this aspect of the design adds complexity to the interface, we have taken steps to make the complexity more manageable.

To assist the non-expert user, we have profiled the JMBL schema. Each profile provides a view of a subset of the larger JMBL schema and represents the minimum elements and attributes required to request each of the available METOC data types.

The limited choices in the profiles guide the novice to form a request for data. We have also documented the business rules for JMBL server implementations. The business rules help ensure that different servers provide consistent responses to requests that are similar in structure and content.

The DoD Chief Information Officer has established the DoD Metadata Registry (MDR) as a repository for structural metadata. We have registered JMBL, the WSDL file, JMCDM, and the physical data models in the Metadata Registry and have had JMBL admitted to the DoD Information Technology Standards Registry (DISR) as a mandated standard. The DISR mandates the minimum set of standards and guidelines for the acquisition of all DoD systems that produce, use or exchange information.

We have implemented JMBL data servers at the Naval Oceanographic Office (NAVO), Fleet Numerical Meteorology and Oceanography Center (FNMOC) and the Air Force Weather Agency. These implementations virtualize access to multiple data stores within each organization.

The METOC COI Service Bus (McSB) is currently under development and will further virtualize access to each data provider within the Navy METOC Enterprise, as shown in Figure 2. This single entry point will provide routing, orchestration, mediation and security services for data access from NAVO, FNMOC and other Navy data holder organizations.

If the user is authorized to receive the requested data, the server will split the user's request into fragments based on request content and provider rules. The server will forward each fragment to the appropriate data provider and then aggregate the separate provider responses before supplying a single response to the user.

This rules-based capability will deliver the warfighter's single, authoritative, accurate, timely and relevant METOC answer.

With our joint partners, we are defining the requirements for and design of a similar capability to support joint METOC operations. This is shown in Figure 1 as the Joint METOC Capabilities Access Point. JMCAP, together with Joint METOC domain authority rules and services definition, will virtualize access to multiple databases and data stores maintained by each of the services.

Our work on net-centric data management is not static but continues to evolve to address emerging requirements. We are currently evaluating how and when to integrate the Universal Core with JMBL.

UCore is gaining widespread attention as an information exchange specification and functional element of the "National Strategy for Information Sharing" (available at www.whitehouse.gov/nsc/infosharing/) that should prove useful in net-centric data management.

We have also begun a migration path to include Open Geospatial Consortium Web services standards and specifications. OGC WS is widely used for geospatial data access, and we believe that it will play a meaningful role in distribution of particular types of METOC data products.

The requirements we address often come from the varied communities with which we must exchange data. Our net-centric data management efforts continue to mature as we address the needs of each of these communities of interest.

Dr. Roy Ladner works for the Naval Meteorology and Oceanography Command, data architecture and administration (N62). He is a member of the METOC community of interest's Data Management Working Group.

CHIPS

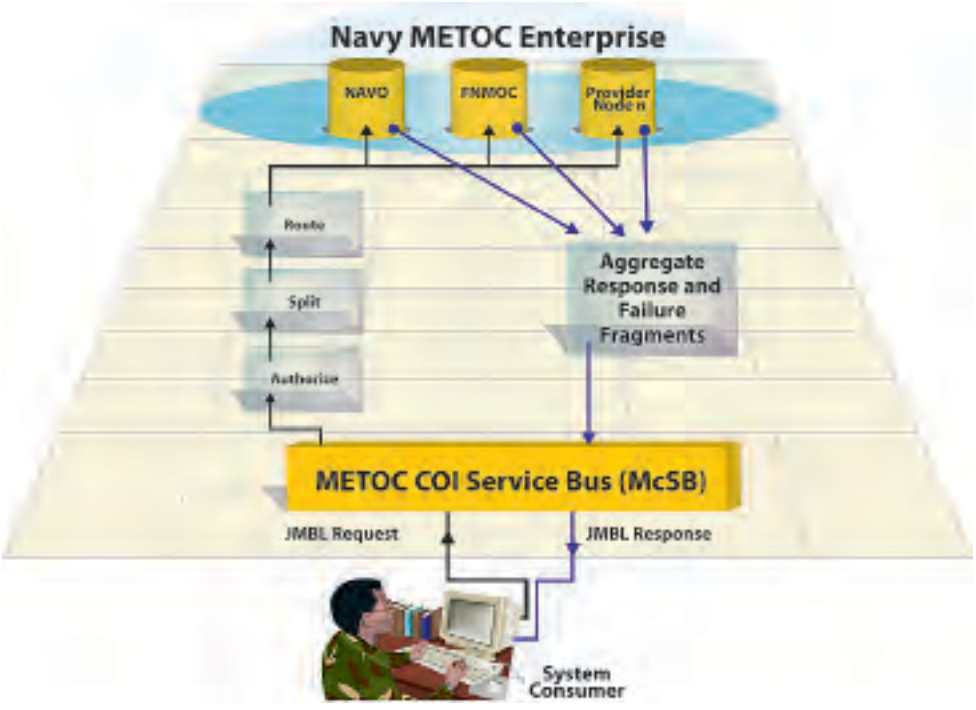


Figure 2. Navy METOC Enterprise.

Information Assurance Training Underway on USS Abraham Lincoln

By Mary Purdy

"The network is down." These four words can wreak havoc on anyone's day, but for Defense Department networks the consequences can be dire. Successful cyberspace operations, including operating, defending and securing the network, ensure cross-domain freedom for U.S. operating forces — and denying that same advantage to adversaries.

The ability to know what is normal and what is abnormal activity in a dynamic network environment of intrusions, viruses and malware is a competency that must be mastered.

The information assurance workforce is essential to assuring the DoD and the Department of the Navy (DON) have adequate security measures to protect and defend information and information systems.

With the increasing threat evidenced by the hundreds of daily attempts to breach U.S. military computer networks, equipping an IA workforce that is educated and trained to meet these challenges is an imperative. Throughout government, efforts are underway to address this requirement.

To address complex information assurance mission requirements, the DoD Chief Information Officer directed the services to improve the skill level of the information assurance workforce (IAWF).

In response to DoD Directive 8570.1, *Information Assurance Training, Certification and Workforce Management,* the DON CIO has chartered a department-wide IA workforce working group (IAWWG) to identify and improve policy, processes and tools to transform the department's future IA workforce. Some of these major initiatives include:

• Improving how IA orientation and refresher awareness training is delivered;

• Identifying standardized IA qualifications, training and certifications; and

• Developing procedures to identify and manage IA positions with trained and certified personnel.

But how do you train a forward deployed force? The Fleet Commanders IAWF Improvement Initiative was designed to meet this challenge.

While on a seven-month deployment, Sailors from the USS Abraham Lincoln (CVN 72) Carrier Strike Group completed a successful IA commercial certification training and testing pilot. This initiative will pave the way for the afloat Navy to meet DoD's goal that requires approximately 110,000 military, civilian and support contractors, throughout all services and agencies, to be IA commercially certified by December 2010.

Led by USS Lincoln's combat systems information officer Lt. Cmdr. David White, the IAWF from the carrier, and its escort ships, chose three different training methods for the pilot program.

Lincoln Strike Group Sailors took Security+ commercially developed training via Navy e-Learning SkillSoft courses; Carnegie Mellon University's Virtual Training Environment that includes labs and mentors; and commercial certification courses.

Anthony Solano, an instructor from the Ultimate Knowledge Institute Corp., led Security+ training classes for about 100 Sailors during Lincoln's deployment. Information systems technician chief petty officers from the ship's combat systems department administered the commercial certification exams using the Pearson VUE electronic testing platform.

Standing up Pearson VUE test centers afloat also enables testing for other certifications, including Adobe and Cisco certifications.

"The ship can claim bragging rights with 95 percent of the Lincoln Strike Group IAWF now holding an IA commercial certification. Overall Navy certification status is at almost 40 percent. Many ashore units have high passage rates, but afloat operational tempo makes it more difficult to achieve," said Mike Knight, Naval Network Warfare Command program manager for IAWF management.

Sailors, afloat and ashore, are studying for commercial certification courses every day so lessons learned from the Lincoln pilot will be shared with other carrier strike groups to facilitate training.

Free exams are available to IAWF Sailors through the Navy's Credentials Program Office. The program office also helps determine eligibility and provides free test vouchers for other commercial certifications. More information can be found on the Navy Credentials Program Web site at https://www.cool.navy.mil.

Being able to train and test underway will help the Navy achieve not only DoD IAWF requirements but also DON continuous learning requirements. The Lincoln pilot also demonstrated that while some Sailors thrive in a live classroom environment, others do well with online courses and in the Virtual Training Environment.

"Deckplate leadership from the chief petty officers, which includes training, mentoring and motivation of the Sailors, was the key to our success," White said.

Mary Purdy provides support to the DON CIO IT Workforce Team.

CHIPS

EVERETT, Wash. (Oct. 12, 2008) Sailors man the rails as the aircraft carrier USS Abraham Lincoln (CVN 72) arrives in its homeport of Everett Wash. Lincoln is returning from a seven-month deployment to the U.S. 5th Fleet area of responsibility. U.S. Navy photo by Mass Communication Specialist 2nd Class N. Brett Morton.

Hold Your Breaches!

By Steve Muck

All Department of the Navy personnel should continue to increase their level of awareness about properly safeguarding personally identifiable information (PII). To learn more about properly safeguarding PII, go to www.doncio.navy.mil.

The following is a reported loss or breach of PII involving a Department of the Navy information system with lessons learned from the event. Incidents such as these will be reported in each subsequent CHIPS magazine to increase PII awareness. Names have been changed or removed, but details are factual and based on reports sent to the DON Chief Information Officer (DON CIO) Privacy Office.

A former civilian contractor, working in support of the Navy Marine Corps Intranet (NMCI), obtained personally identifiable information associated with approximately 17,000 individuals. The PII was downloaded to a thumb drive and consisted of names associated with Social Security numbers, home addresses and other data elements.

The contractor, who had a criminal record, then attempted to sell this information to an individual he believed to be a foreign spy, but who was actually a law enforcement official. The contractor was arrested April 18, 2008, and was later found guilty of aggravated identity theft and exceeding authorized access to a computer for personal gain. He is now awaiting sentencing.

The conviction for exceeding authorized access to a computer for financial gain carries a maximum sentence of five years in prison. Aggravated identity theft carries a mandatory two-year sentence that must be served consecutive to any sentence imposed for the charge of exceeding authorized access. Both counts also include maximum fines of $250,000. A maximum sentence of incarceration for seven years is possible.

This breach attracted national media attention and demonstrated how the insider threat is potentially more damaging than breaches involving human error.

A joint investigation by the Naval Criminal Investigative Service and Federal Bureau of Investigation found that the contractor also sent screenshots of PII to two e-mail addresses of individuals who did not have a need to know and with the intent to sell the contents of the entire database.

The individuals whose PII was compromised via the two e-mails have been notified. The investigation concluded that the bulk of the database was not compromised.

Steve Muck is the DON CIO privacy lead.

CHIPS

Lessons Learned

- The insider threat, with access to large amounts of privacy sensitive data, poses a significant and real danger to the Department of the Navy.

- Defense Department and DON policy require personnel who access PII to receive a favorable personnel security investigation. The background check for the individual involved in this incident was not initiated. See DoD Directive 5200.2-R, *DoD Personnel Security Program*, and Secretary of the Navy Manual, *Personnel Security Program*, SECNAV M-5510.30, for details of this security guidance. Increased awareness of DoD and DON policy is recommended.

- Contract language clearly identified the need to conduct a security investigation for personnel hired to fill the contractor position, but it was not initiated. Improved contract oversight is needed.

- A base security access system that accurately screens criminal offenders was not available and would have provided another means to prevent the perpetrator from gaining access to the base and NMCI network.

To learn more about properly safeguarding PII, go to www.doncio.navy.mil and search for "safeguarding PII" for detailed guidance.

U.S. and Coalition Forces Build Technological Capacity for the Government of Iraq

MNSTC-I trains Iraqi government ministries to design and sustain vital networks

By U.S. Navy Lt. Damian Taylor

Headquartered in the International Zone (IZ), Baghdad, Iraq, the Directorate of Communications (J6), part of the Multi-National Security Transition Command-Iraq, is meeting its mission to help the government of Iraq design and build a new and effective communications infrastructure to support the military and police forces protecting innocent Iraqi citizens from terrorists.

The Iraqi network program managers of the MNSTC-I J6 command, control, communications and computers (C4) capabilities branch provide daily oversight for the Ministry of Interior (MoI) and Ministry of Defense (MoD) command and control networks. Figure 1 below shows the networks under discussion.

Building for Now and into the Future

Over the past two years, MNSTC-I J6's role evolved from providing communications capabilities to the Iraqi government to serving as advisers, educators and mentors to the chief information officers in the ministries of Interior and Defense as they assume greater leadership roles in network management.

In the past year, focus for J6 centered on ensuring the communications infrastructure was ready to sustain the networks.

Initially, MNSTC-I funded these networks and managed them, but the CIOs of the Interior and Defense ministries, working with the MNSTC-I J6, are now providing management and the funds necessary to keep the networks operational, and growing and positioned for the future.

A great example of this shift is the recent successful assessment of MoI's enterprise architecture. The MoI architecture assessment is a joint venture between the Iraqi communications coordination element (ICCE) of the Multi-National Force-Iraq (MNF-I), the MNSTC-I J6 staff and the MoI transition team.

The assessment is designed to identify information technology gaps in the Ministry of the Interior. The assessment will be followed by a series of meetings with MoI officials to identify recommendations to improve Iraqi IT infrastructure and key business practices.

With additional engagements, coalition members continue to earn the respect of key MoI leaders and industry professionals. Teamwork is critical to these efforts, and all stakeholders worked together to identify the strengths and areas for improvement within the Iraqi IT architecture.

Experience and expertise are important ingredients for success in these efforts, so coalition mentors continue to offer sound advice and recommendations for improvement.

The Iraqi police forces are the primary asset of the MoI, and these forces rely on the Iraqi Command and Control Network (IC2N). The coalition funded and procured the necessary hardware for IC2N in 2004. The Ministry of the Interior remains committed to IC2N and has established its own contracts with an industry network provider.

Iraqi networks are growing rapidly and expanding to many sites on Iraq's borders. At the same time, upgrades such as video teleconferencing capability are being added.

"These results show great promise, clearly showing the GoI's (government of Iraq) high level of commitment. Initially, the coalition did most of the managements tasks, but the Iraqis are rapidly assuming the decision-making processes," explained Marine Corps Gunnery Sgt. Mark Henderson, the C4 capabilities branch senior enlisted advisor.

The Defense Ministry uses the Iraqi Defense Network (IDN), which provides the same capabilities as the IC2N to the Iraqi army, navy and air force.

U.S. Air Force Capt. Christopher Wiley, the coalition IDN program manager, was instrumental in the training of his Iraqi counterpart, the MoD IDN program manager. Wiley is justifiably proud of the training's success.

"MoD's IT staff now plans and coordinates their network efforts independently. This is what we have been working toward for the last few years."

The MoD is also funding the operations and maintenance of IDN, and it is actively managing the network and expanding its coverage, making great strides toward self-sufficiency. For example, the MoD is now using indigenous Iraqi installation teams.

The MoD successfully installed three major network nodes and has plans to install at least five more by December 2008. The MoD is also training its staff to manage the network operations center.

Eight MoD students recently graduated from a rigorous four-month systems engineering course. The students are completing on-the-job training to assume complete control of IDN which will eliminate the need for foreign contractors.

MNSTC-I uses a five-phased approach to transition current capabilities to the Iraqi government. In phases one and two, coalition forces manage the networks while the Iraqis observe and learn. In the

Iraqi Command and Control Network (ICN2)	C2 network utilized by the Iraqi police force for command and control. It includes VoIP phones and desktop computers with e-mail and Internet access	MoI
Advanced First Responder Network (AFRN)	Iraq's 911 network that facilitates Iraqi police and security forces responding to emergencies. AFRN includes handheld radios and centralized dispatch centers	MoI
Iraqi Defense Network (IDN)	IC2 network utilized by the Iraqi army, navy and air force for command and control. It includes VoIP phones and desktop computers with e-mail and Internet access	MoD

Figure 1. Networks of the ministries of the Interior and Defense.

third phase, coalition forces and the Iraqi government will work together to build and manage the networks.

In the fourth and vital transition phase, the Iraqi government takes over management of its networks while coalition forces observe and mentor.

Finally, in the fifth phase, the government of Iraq manages its networks independently. Each phase includes measurements to quantitatively and qualitatively measure the progress of the transition.

"The J6's goal is for all of the Iraqi security forces and their networks to reach the fifth phase," Henderson said.

Building Confidence

The Advanced First Responder Network (AFRN) is Iraq's equivalent to the American 911 system. The Interior Ministry has managed and funded AFRN since 2006.

"AFRN is close to phase five. [The] MoI has committed to maintaining this AFRN, and they are looking for ways to expand it effectively and efficiently," said Air Force Capt. Antonio McNutt, AFRN program manager for the coalition forces.

The Iraqi government is eager to be self-sufficient and pleased about its ability to provide public services to its citizens, according to Iraqi government officials.

"We take pride in ownership and accomplishing our missions on our own. We have an Iraqi-operated AFRN network operations center where we are able to respond to trouble tickets and monitor the network remotely.

"We were unable to accomplish this two years ago, but with the help of the coalition, we are now providing an invaluable service to our citizens," said Iraqi Brig. Gen. Ahmed, MoI AFRN program manager.

An effective communications capability is essential to Iraqi's defense forces and national self-sufficiency. The MNSTC-I J6 has an enormous responsibility to ensure the Iraqi government has an unassailable and battle-tested communication infrastructure that the Iraqis can manage and operate long after coalition forces depart from Iraq.

"We are not at the finish line yet, but we've made significant headway in getting the Iraqis to operate independently and professionalize their security forces," McNutt said.

The Multi-National Security Transition Command-Iraq was established June 28, 2004, building on previous efforts under the Coalition Provisional Authority. The command helps Iraq organize, train and equip its military and police forces.

In the past 15 months, working closely with the Iraqi ministries of Defense and Interior, the command assisted in forming more than 115 army and police combat battalions. There are now more than 600,000 trained and equipped members of the security forces, with more to come. These troops are in the field today, defending the Iraqi people. In the months ahead, the command will continue to assist in strengthening the Iraqi security forces as they take the fight to the enemy.

MNSTC-I's mission is to assist the Iraqi government in the development, organization, training, equipping and sustainment of Iraqi security forces and ministries so they can defeat terrorism and provide a stable environment in which representative government, individual freedom, the rule of law, and the free market economy can evolve and which, in time, will contribute to Iraq's external security and the security of the Gulf Region.

For more information about Multi-National Security Transition Command-Iraq, contact the public affairs officer at PAO@IRAQ.CENTCOM.MIL or go to the MNSTC-I Web site at www.mnstci.iraq.centcom.mil.

Iraqi students and instructors discuss the capabilities of the Iraqi Defense Network (IDN) to convey the need for continued program support during a visit by senior military leadership Sept. 22, 2008.

"This mission is more complex than simply building networks for sending and receiving data. It involves rebuilding a nation's confidence in their government, military and police …"

Air Force Maj. Daniel Steele
MNSTC-I J6 chief of strategic operations

Air Force Maj. Daniel Steele, MNSTC-I J6 chief of strategic operations, agreed with McNutt, but said that the program built more than networks for the Iraqis.

"This mission is more complex than simply building networks for sending and receiving data. It involves rebuilding a nation's confidence in their government, military and police. It involves developing long-term productive relationships inside and outside Iraq.

"It involves creating an atmosphere where the Iraqi people have the self-confidence to actively guide the evolution of their nation's future."

Lt. Damian R. Taylor is the C4 Capabilities Branch Chief/IC2N program manager MNSTC-I J6 for U.S. Central Command at Camp Phoenix.

There has been a lot of emphasis lately on computer security and the menace of cyber warfare. However, having surveyed the field and sifted through all the things that can go awry from an information security standpoint, I have come to the following conclusion: *We are the weakest link.*

And by "we" I mean, of course, all of us who form the sentient carbon-based portion of our IT systems. Yes, worms, viruses, botnets and other means of attack are legitimate threats. However, even these technology-based bad actors generally take advantage of human nature to inflict the most harm to our systems.

Information technology and business journals abound with stories of security breaches caused by careless, ignorant or optimistic users fooled by clever hackers. Reports on hardware compromises frequently mention that hackers used social engineering to extract key information from employees that helped them crack systems.

The "script kiddies" who download automated tools and use them to crack systems through purely technical means are at the low end of the hacker scale. As Bruce Schneier, my favorite security guru, observed, "Amateurs hack systems, professionals hack people."

For an example of a real pro, I offer Kevin Mitnick, arguably the most notorious hacker of modern times, who relied heavily on human vulnerabilities to get into the computer and phone systems of American government agencies, telecommunications carriers and technology companies. While he also used attacks like IP spoofing, he gained most of his illicit access simply by conning people. We will discuss why cons are successful later.

Therefore, we will look inside the human mind for therein may reside the answer to the eternal question: "Is this computer, network, e-mail — and the list goes on — safe?"

Playing the Confidence Game

Running a con, or confidence game, is fairly straightforward: gain the trust of your targets and persuade them to want to give you something you want, like money or information. There are two basic ways con artists put people in a giving mood: self-interest and reciprocity.

Self-interest can be illustrated by a classic con known as the *Pigeon Drop*. Here is an example of how it works. Our "pigeon" is a bartender. On a slow night a guy comes out of the men's room with a small black box and tells the bartender that he just found it in the men's room. Inside the box is an expensive-looking ring. Just then the bar's phone rings. On the other end of the line is a distraught gentleman asking if anyone found the ring he bought for his wife for their wedding anniversary and offering a $200 reward for its return. After hearing a description of the ring, the bartender tells him that a customer found it. The guy says, "Great, I'll be there in half an hour!" and hangs up.

Now the fun begins. When the bartender tells the "customer" about the reward, the guy holding the ring says he can't wait because he is in a hurry. He then offers to split the reward: *If the bartender will give him $100, he will leave the ring with the bartender.* At this point, if the bartender has been taken in by the scam, he hands over $100 and waits for the guy with the reward.

Unfortunately, 99 times out of 100, the ring, or cell phone, or purse, or necklace, is a fake. The only people splitting any money are the two guys with the bartender's $100.

Now, if we have the most advanced thinking devices on the planet, why does a con like this work? There are two factors at work here. The first, and most obvious, is simple greed. Free money? Great! Count me in!

The second factor, though, requires some understanding of neuroscience, specifically, a phenomenon called *The Human Oxytocin Mediated Attachment System*. THOMAS is, according to Dr. Paul Zak, author of The Moral Molecule blog, "a powerful brain circuit that releases the neurochemical oxytocin when we are trusted and induces a desire to reciprocate the trust we have been shown — even to strangers."

This reaction helps form the basis for a successful con. By appearing vulnerable, and even respectable, a con can trigger a response in us to be helpful. It is not that we trust the con, but that *we think he trusts us*. Con artists take advantage of the same biochemical reaction that is the basis of our attachments to friends and family and a reward for cooperative actions of all kinds.

So, aside from the desire for the reward money, THOMAS rewards us with a feel-good shot of oxytocin for wanting to help the poor guy who lost his wife's anniversary present. THOMAS is apparently very easy to stimulate in most people.

Our defense against this effect is our prefrontal cortex, the deliberative, decision-making region of our brain. Here is where we need to listen to that little voice of reason that says: *This is too good to be true.*

So how do we stimulate the prefrontal cortex? Any activity that engages logic or memory appears to help, like memorizing phone numbers or mentally calculating the tip on a restaurant bill. Perhaps we are, as a species, becoming more susceptible to being fooled because we do less of this type of thinking and offload these tasks to our personal digital assistants or calculators.

Do A Good Deed Daily

Taking advantage of THOMAS is not the only way to work a con. Let's look at a few examples of social engineering offered by uber-hacker Kevin Mitnick, in his book, *The Art of Deception*.

✓ To gain access to a computer system protected by a daily password change, wait for a snowstorm and call the network center posing as a snowed-in employee who wants to work from home and convince the operator to reveal the current password.

This one is less a trust issue than one of empathy or pity. To pull this off, the hacker must know the name of one or more employees and be capable of pulling off a convincing impersonation of a company employee. Those of us who live near the

Canadian border do tend to be pretty sympathetic to our friends and neighbors during blizzards.

✓ Gain proprietary information about a start-up company, then wait until the chief executive officer is out of town and show up at the company pretending to be a close friend of the CEO. Again, not a ploy that really takes advantage of the THOMAS phenomenon, but a common con all the same, particularly in any organization with a lot of new employees who do not know each other or their new boss well.

Here, the con man wants to give the impression that he will put in a good word for the helpful employee *(who has actually helped him infiltrate the company)* with the new boss.

✓ To gain access to a restricted area, approach the door carrying a large heavy-looking box and rely on a Good Samaritan to hold the door open for you. This one probably stimulates the THOMAS phenomenon because the target is helping a poor unfortunate staggering under the weight of a mighty load. Try this during a blizzard or other nasty weather to increase your chances for entry.

Let's face it, we are social creatures wired to help each other. Cooperative effort is how humans rose to the top of the food chain. Except for a very small percentage of the population who apparently lack THOMAS, which Dr. Zak estimates to be 2 percent, humans thrive on helping each other. The problem is that the other 2 percent are more than happy to take advantage of our helpful nature.

Chain Reactions

Isolated, single examples of social engineering may seem of limited harm. But good social hackers do not go for a big score all at once. They use a series of small exploits to score a big win.

Hackers approach social engineering through a psychological method. They attempt to create a perfect attack environment through impersonation, intimidation, ingratiation, conformity, diffusion of responsibility and friendliness. Their objective is to convince the person disclosing the information that they can be *trusted* with sensitive information.

The other important ingredient to their success is not to ask for too much information at one time so people do not become suspicious and are thus duped into providing valuable information bit by bit. By chaining related cons together, hackers can link these seemingly inconsequential pieces of information to gain access to an organization's systems — without launching a single piece of attack software.

Who Am I?

Social hackers often solicit information through impersonation. Impersonations generally fall into two categories: someone with a support job allegedly trying to provide help or someone with or close to authority. Common roles include: repairmen, IT techs, managers, trusted third parties (e.g., an executive assistant to a VIP), or fellow employees. The simple version of this attack is to call people pretending to be an employee and see what they will tell you. Here are some examples that have allegedly worked.

✓ A hacker calls unsuspecting targets and claims that he is from their telecommunications company's security division. He asks if a two-hour phone call has just been made to Israel. When the target vehemently denies this, the hacker says that he can remove the charges, but needs the target's calling card and PIN number. The target gratefully provides the information.

✓ A hacker calls the help desk and asks to be passed on to a supervisor. Once connected, the hacker expresses sympathy for the supervisor, who asks why. The hacker says that he is a system administrator and that from his console he can tell that systems are down. When the supervisor expresses surprise, he tells her to log in and out several times, each time claiming that he cannot see any activity at his end. Eventually, he tells her that the only way he will be able to isolate the problem is if she gives him her account login information. Since she believes, at least at this point, that he is legitimate, she does.

Here is a more complex exploit that has apparently been replicated more than once by security testers.

✓ The hacker starts by sending an e-mail to a target organization, that we will refer to here as "Acme Widgets," asking about upcoming jobs. With any luck the reply will contain Acme's e-mail signature, its title and address formats, and whatever e-mail confidentiality statement is included in its official message.

Then the hacker registers a domain similar to the company's domain name. If the actual domain is "acmewidgets.com," the hacker might try "acmewjdgets.com." The hacker then creates a mail server with the fake domain and sends an e-mail to Acme employees from an account named "Help Desk" with a compressed file attachment that contains a keyboard logger. If this spyware is unique, it will not likely be included in standard antivirus profiles and may not be discovered by most antivirus or anti-spyware software.

The bogus e-mail instructs employees to run the attached file as part of an antivirus upgrade. Since the message may look legitimate to some of the targeted employees, they will follow the instructions and install the hacker's spyware, which subsequently sends an e-mail, with possibly sensitive data, at the end of each day back to the hacker.

Who Are They?

Another common social engineering attack method is to obtain a complete list of an organization's IT personnel and their contact information. The goal is to determine the usernames of the people likely to have the greatest access to an organization's networks.

This hack takes the form of a phone call to the fictional Acme Widget's human resources department. The hacker says that he was there earlier in the week for a job interview and wants to send thank you notes to the people who interviewed him, for example, the chief information officer, IT director and two network administrators. However, curse his bad memory, he cannot-remember their names and has lost or misplaced their business cards.

In telling the HR person how embarrassed he is about this, he attempts to trigger THOMAS and get names and as much other information as he can — whatever he can con out of the sympa-

thetic person on the other end of the phone. If this attempt is successful, the hacker can now move on to trying to collect other information. He will probe various offices to find out how willing people are to share information. The next couple of questions could look something like this …

I have a meeting tomorrow with your IT engineering manager, Chad Thomas. Where is he located, please?

I am out of my office at the moment. What is our help desk number, please?

If he's been successful in all the previous intelligence gathering methods, our hacker now has enough information to try a more elaborate impersonation, particularly if he has established a relationship with some employees during earlier calls …

Hi! My name is Ron. I'm a co-op, and I work with Chad Thomas and Pete Harmon in the network engineering office on the third floor in our Taft Corners office in Williston. They told me to give you a call because we are making some changes to the network, and I need to get some information from you.

At this point, the hacker can try to solicit more detailed information by "helping" employees report the IP address of their computer, or even tricking IT personnel into sending a complete organizational list of employees and account names.

All these social hacks, by themselves, may seem relatively harmless or even improbable. However, security personnel will tell you that not only can they work, they have worked, and are likely occurring somewhere as you read this.

As a result, hackers get lists of employees, administrator user IDs, data from keyboard loggers, useful jargon and other unique data that they can use to pass themselves off as authentic employees. Once hackers establish a certain level of credibility, they go after the real prizes: passwords, root level access to systems, and financial or operational data.

User, Know Thyself

Virtually every organization, public or private, in the United States requires annual computer security training for employees. But much of the focus is on preventing potential threats to the computer and on the network — turn off macros, do not download strange files and lock down system configurations — all good advice.

But our overall approach should be education in all security disciplines — physical, operational, informational and technological, and should include a strong coordinated approach to recognizing and responding to social hacking as a universal threat not limited to one area of security.

Educating people to defend themselves against social engineering is not a new concept. I remember watching a film in Air Force Basic Training in 1981 warning about these types of tactics in the context of the Cold War.

In the training film, spies asked seemingly innocent questions about people and places at a base and gathered enough information to waylay a courier and steal the classified documents he was carrying.

If we are serious about defending ourselves against social engineering attacks, we need to educate users. In particular, we need to impress on personnel that they are the gatekeepers for organizational information and help them spot and report potential scams.

Our gatekeepers are secretaries, administrative employees, human resources employees, help desk technicians and other people in our organizations who answer the phones or respond to inquiries from the public.

Do we want them to be friendly and helpful? Of course, we do. But because they may be less sophisticated about security threats, they are the favorite targets of thieves and hackers.

We must teach employees how to identify the information they should protect and how to protect it. We must also teach employees how to recognize social engineering.

The Computer Security Institute provides tips to users that should trigger alarm when you are asked to provide information to unknown persons or from unsolicited e-mails. *If the caller or e-mailer …*

- ✓ *Refuses to provide contact information*
- ✓ *Exhibits undue haste for a response*
- ✓ *Name-drops VIPs within the organization*
- ✓ *Attempts to intimidate or ingratiate*
- ✓ *Makes mistakes such as misspellings or misnomers*
- ✓ *Asks odd questions or requests information that is for official use only*

alert your security staff at once!

The United States Computer Emergency Readiness Team, at www.us-cert.gov, offers training and guidance in spotting social engineering tactics and other computer security information.

We should establish and publicize procedures for reporting social engineering incidents to educate employees so they can avoid becoming targets too. I also suggest that some discussion of THOMAS should be part of every security training program. Maybe if people know how pleasure-inducing oxytocin rewards them for being helpful, they will be less likely to fall victim to hacker schemes.

Spies, con men and salesmen have been taking advantage of this mechanism for years, but it was only about four years ago that Zak demonstrated that this phenomenon exists and how it can be manipulated to scam innocent victims. Finally, we must recognize our social vulnerabilities and work to improve our behaviors, take time to think and use common sense. Don't let yourself or your network become a victim.

Until next time, Happy (Safe) Networking!

Long is a retired Air Force communications officer who has written regularly for CHIPS since 1993. He holds a master of science degree in information resources management from the Air Force Institute of Technology. He currently serves as a telecommunications manager in the Department of Homeland Security. CHIPS

Enterprise Software Agreements

Listed Below

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

Additionally, the ESI was incorporated into the Defense Federal Acquisition Regulation Supplement (DFARS) Section 208.74 on Oct. 25, 2002, and DoD Instruction 500.2 in May 2003.

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

For more information on the ESI or to obtain product information, visit the ESI Web site at http://www.esi.mil/.

Software Categories for ESI:

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://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-07-A-0005

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: 29 May 09

Web Link: https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-07-A-0006

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: 19 Nov 09

Web Link: https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-07-A-0004

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://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-07-A-0002

Patriot

BigFix Asset Management - Provides software, maintenance and services.

Contractor: ***Patriot Technologies Inc.*** (W91QUZ-07-A-0003)

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

Ordering Expires: 08 Sep 12

Web Link: https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-07-A-0003

Business and Modeling Tools

BPWin/ERWin

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

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

Ordering Expires: Upon depletion of Army Small Computer Program (ASCP) inventory

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

Business Intelligence

Business Objects

Business Objects - Provides software licenses and support for Business Objects, Crystal Reports, Crystal Enterprise and training and professional services. Volume discounts range from 5 to 20 percent for purchases of software licenses under a single delivery order.

Contractor: ***EC America, Inc.*** (SP4700-05-A-0003)

Ordering Expires: 04 May 10

Web Link: http://www.gsaweblink.com/esi-dod/boa/

Mercury

Mercury Software - Provides software licenses, training, technical support and maintenance for Mercury Performance Center, Mercury Quality Center, Mercury IT Governance Center and Mercury Availability Center.

Contractor: ***Spectrum Systems, Inc.*** (SP4700-05-A-0002)

Ordering Expires: 21 Feb 09

Web Link: http://www.spectrum-systems.com/contracts/esi-hp.htm

COTS Systems Integration Services

COTS Systems

COTS Systems Integration Services - Provides the configuration; integration; installation; data conversion; training; testing; object development; interface development; business process reengineering; project management; risk management; quality assurance; and other professional services for COTS software implementations. Ordering under the BPAs is decentralized and is open to all DoD activities. The BPAs offer GSA discounts from 10 to 20 percent. Firm-fixed prices and performance-based contracting approaches are provided to facilitate more efficient buying of systems integration services. Five BPAs were competitively established against the GSA schedule. Task orders must be competed among the five BPA holders in accordance with DFARS 208.404-70 and Section C.1.1 of the BPA. Acquisition strategies at the task order level should consider that Section 803 of the National Defense Authorization Act for 2002 requirements were satisfied by the BPA competition.

Contractors:

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

BearingPoint (N00104-04-A-ZF15); (703) 747-8854

Computer Sciences Corp. (N00104-04-A-ZF16); (856) 988-4505

Deloitte Consulting LLP (N00104-04-A-ZF17); (571) 480-7272

IBM Corp. (N00104-04-A-ZF18); (703) 424-7581

Ordering Expires: 03 May 09

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/erp_services/erp-esi.shtml

Database Management Tools

Microsoft Products

Microsoft Database Products - See information under Office Systems on page 50.

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); (757) 284-6570

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

Ordering Expires:

Oracle: 30 Sep 11
DLT: 1 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://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

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

Sybase (DEAL-S)

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

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

Ordering Expires: 30 Sep 09

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

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

Enterprise Application Integration

Sun Software - NEW!

Sun Products - Provides Sun Java Enterprise System (JES) and Sun StarOffice. Sun JES products supply integration and service-oriented architecture (SOA) software including: JES Identity Management Suite; JES Communications Suite; JES Availability Suite; JES Web Infrastructure Suite. 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; (301) 731-8105

Ordering Expires: 24 Sep 12

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/application_integration/SUN/index.shtml

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: 26 Mar 09

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

Enterprise Management

CA Enterprise Management Software (C-EMS2)

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

Contractor: ***Computer Associates International, Inc.*** (W91QUZ-04-A-0002); (800) 645-3042

Ordering Expires: 22 Sep 09

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

Citrix

Citrix - Provides a full range of Metaframe products including Secure Access Manager, Conferencing Manager, Password Manager, Access Suite & XP Presentation Server. Discounts range from 2 to 5 percent off GSA Schedule pricing plus spot discounts for volume purchases.

Contractor: ***Citrix Systems, Inc.*** (W91QUZ-04-A-0001); (772) 221-8606

Ordering Expires: 22 May 09

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

Microsoft Premier Support Services (MPS-1)

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

Contractor: ***Microsoft*** (DAAB15-02-D-1002); (980) 776-8283

Ordering Expires: 31 Jan 09 (Please call for information about follow-on contract.)

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

NetIQ

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

Contractors:

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

Northrop Grumman - authorized reseller

Federal Technology Solutions, Inc. - authorized reseller

Ordering Expires: 5 May 09

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

ProSight

ProSight - Provides software licenses, maintenance, training and installation services for enterprise portfolio management software. The software product provides the enterprise with a suite of solution specific applications for Capital Planning and Investment Control (CPIC) Budgeting (OMB 300/53); CPIC Process (Select/Control/Evaluate); IT Governance; FISMA (Federal Information Security Management Act) and Privacy Compliance; Project Portfolio Management; Application Rationalization; Research and Development (R&D) and Product Development; Asset Management; Grants Management; Vendor and Service Level Agreement Management; and Regulatory Compliance. ProSight products have been designated as a DoD ESI and GSA SmartBUY. The BPA award has been determined to be the best value to the government and; therefore, competition is not required for software purchases. Discount range for software is from 8 to 39 percent off GSA pricing, which is inclusive of software accumulation discounts. For maintenance, training and installation services, discount range is 3 to 10 percent off GSA pricing. Credit card orders are accepted.

Contractor: ***ProSight, Inc.*** (W91QUZ-05-A-0014); (503) 889-4813

Ordering Expires: 19 Sep 11

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

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) 709-7172

Ordering Expires:

Quest: 14 Aug 10

DLT: 01 Apr 13

Web Links:

Quest

https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-05-A-0023

DLT

https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-06-A-0004

Telelogic Products

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

Contractors:

Bay State Computers, Inc. (N00104-07-A-ZF48); Small Business Disadvantaged; (301) 352-7878, ext. 116

Spectrum Systems, Inc. (N00104-07-A-ZF46); Small Business ; (703) 591-7400

Ordering Expires:

Bay State Computers, Inc.: 4 Aug 10
Spectrum Systems, Inc.: 31 Jul 10

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/telelogic/telelogic.shtml

Enterprise Resource Planning

Digital Systems Group

Digital Systems Group - Provides Integrated Financial Management Information System (IFMIS) software that was designed specifically as federal financial management system software for government agencies and activities. The BPA also provides installation, maintenance, training and professional services.

Contractor: ***Digital Systems Group, Inc.*** (N00104-04-A-ZF19); (215) 443-5178

Ordering Expires: 31 Aug 10

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/erp_software/dsg/dsg.shtml

Oracle

Oracle - *See information provided under Database Management Tools on page 46.*

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); (609) 937-7628

Ordering Expires: Effective for term of the GSA FSS Schedule

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/erp_software/rwd/rwd.shtml

SAP- NEW Contractors!

SAP Products - Provides 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

Carasoft 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.it-umbrella.navy.mil/contract/enterprise/erp_software/sap_products/sap_hdr.shtml

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 currently 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 Department of the Navy, Army and Air Force will be releasing service-specific DAR guidance for their personnel to follow. Go to the ESI Web site at www.esi.mil for more information.

As of press time, DoD users are not authorized to purchase DAR software because service-specific guidance has not been issued. DON users are not authorized to purchase a DAR solution until the DON CIO has issued an enterprise solution for purchasing DAR software.

Mobile Armor – ***MTM Technologies, Inc.*** (FA8771-07-A-0301)
Safeboot/McAfee – ***Rocky Mountain Ram*** (FA8771-07-A-0302)
Information Security Corp - ***Carahsoft Technology Corp.*** (FA8771-07-A-0303)
Safeboot/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)
Credant Technologies – **GTSI Corp.** – (FA8771-07-A-0309)
WinMagic, Inc. – ***Govbuys, Inc.*** (FA8771-07-A-0310)
CREDANT Technologies – ***Intelligent Decisions*** (FA8771-07-A-0311)
GuardianEdge Technologies – ***Merlin International*** (FA8771-07-A-0312)
Ordering Expires: 14 Jun 12 (If extended by option exercise.)
Web Link: http://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: 12 Dec 09

Web Link: http://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 Web sites:

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

Securify

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

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

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

Web Link: http://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 over 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*** (FA8771-05-0301)

Ordering Expires: 12 Sep 10

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

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 Web sites:

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

Xacta

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

Contractor: ***Telos Corp.*** (F01620-03-A-8003); (703) 724-4555

Ordering Expires: 30 Mar 09

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 2005 and 2006; Six Sigma and iGrafx Flowcharter 2005 and 2006; iGrafx Process for Six Sigma 2007; iGrafx Flowcharter 2007; Enterprise Central; and Enterprise Modeler.

Contractors:

Softchoice (N00104-06-A-ZF40); (416) 588-9002 ext. 2072

Softmart (N00104-06-A-ZF39); (610) 518-4292

Software House International (N00104-06-A-ZF38); (732) 564-8333

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

Ordering Expires: 30 Jan 09 (Please call project manager for extension information.)

Web Links:

Softchoice
http://www.it-umbrella.navy.mil/contract/enterprise/iGrafx/softchoice/index.shtml
Softmart
http://www.it-umbrella.navy.mil/contract/enterprise/iGrafx/softmart/index.shtml
Software House International
http://www.it-umbrella.navy.mil/contract/enterprise/iGrafx/shi/index.shtml

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.it-umbrella.navy.mil/contract/minitab/minitab.shtml

PowerSteering - NEW!

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.it-umbrella.navy.mil/contract/PowerSteering/PowerSteering.shtml

Office Systems

Adobe Desktop Software

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; Cold Fusion and other Adobe desktop products.

Contractors:

ASAP (N00104-08-A-ZF33); Small Business; (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); (301) 261-6970

Ordering Expires: 30 Jun 13

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/adobe-esa/index.shtml

Four Blanket Purchase Agreements (BPAs) provide both new and upgrade software licenses for Adobe desktop products. These BPAs also provide Adobe software maintenance agreements. The BPAs also include software licenses formerly known under the Macromedia product brand.

Microsoft Products

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

Contractors:

ASAP (N00104-02-A-ZE78); Small Business; (800) 248-2727, ext. 5303

CDW-G (N00104-02-A-ZE85); (877) 890-1330

Dell (N00104-02-A-ZE83); (800) 727-1100 ext. 37010 or (512) 723-7010

GTSI (N00104-02-A-ZE79); Small Business; (800) 999-GTSI or (703) 502-2959

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

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

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

Software House International (N00104-02-A-ZE86); (732) 868-5926

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

Ordering Expires: 31 Mar 10

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

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 Web sites 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 Web sites 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.

GIG or GCCS users: Common Operating Environment Home Page
http://www.disa.mil/gccs-j/index.html

GCSS users: Global Combat Support System
http://www.disa.mil/main/prodsol/gcss.html

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

Download Site: http://redhat.augustschell.com

Ordering Expires: 14 Mar 09 (Contract options expire 15 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.

Contractor: ***DLT Solutions, Inc.*** (HC1013-04-A-5000)

Ordering Expires: 30 Apr 09

Web Link: http://www.dlt.com/

WinZip

WinZip - This is an IDIQ contract with Eyak Technology, LLC, an "8(a)" Small Disadvantaged Business (SDB)/Alaska Native Corp. for the purchase of WinZip Standard, a compression utility for Windows. Minimum quantity order via delivery order and via Government Purchase Card to Eyak Technology, LLC is 1,250 WinZip licenses.

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

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

Ordering Expires: 27 Sep 09

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

Operating Systems

Apple - NEW!

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: http://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: http://www.ditco.disa.mil/hq/contracts/sstewchar.asp

Research and Advisory BPA

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

Gartner Group (N00104-07-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.it-umbrella.navy.mil/contract/r&a/gartner/gartner.shtml

Section 508 Tools

HiSoftware 508 Tools

HiSoftware Section 508 Web Developer Correction Tools - Includes AccRepair (StandAlone Edition), AccRepair for Microsoft FrontPage, AccVerify for Microsoft FrontPage and AccVerify Server. Also includes consulting and training support services.

Contractor: ***HiSoftware, DLT Solutions, Inc.*** (N00104-01-A-Q570); Small Business; (888) 223-7083 or (703) 773-1194

Ordering Expires: 31 Aug 10

Web Link: http://www.it-umbrella.navy.mil/contract/508/dlt/dlt.shtml

Warranty: IAW GSA schedule. Additional warranty and maintenance options available. Acquisition, Contracting and Technical fee included in all BLINS.

The DON IT Umbrella Program offers great customer service

Go to the WEB sites listed below to learn more:

www.it-umbrella.navy.mil

www.itec-direct.navy.mil

www.esi.mil

DEPARTMENT OF THE NAVY
COMMANDING OFFICER
SPAWARSYSCEN ATLANTIC
CHIPS MAGAZINE
3606 FOURTH AVE
NORFOLK, VA 23511 - 2130
OFFICIAL BUSINESS

PERIODICAL POSTAGE AND
FEES PAID NORFOLK, VA AND
ADDITIONAL MAILING OFFICE
SSC CHARLESTON
CHIPS MAGAZINE
USPS 757-012
ISSN 1547-9585