Sharing Information - Technology - Experience

CHIPS

January - March 2011

STOLEN IDENTITY

How To Protect Their Data While They Protect Us

CHIPS

January – March 2011 | Volume XXIX Issue I

Department of the Navy
Chief Information Officer
Mr. Terry A. Halvorsen

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

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

Senior Editor
Sharon Anderson

Assistant Editor
Nancy Reasor

Layout and Design
Sharon Anderson

Web Support
Minh Quach, SPAWARSYSCEN Atlantic

Columnists
Sharon Anderson, Terry Halvorsen,
Mike Hernon, Tom Kidd, Steve Muck

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

CHIPS is sponsored by the Department of the Navy Chief Information Officer (DON CIO), the Enterprise Software Initiative and Space and Naval Warfare Systems Center Pacific.

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

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

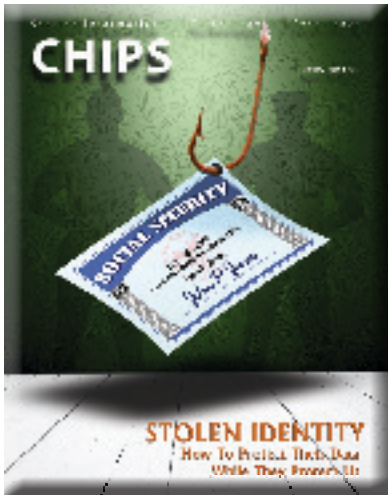
Requests for distribution changes or for other assistance should be directed to Editor, CHIPS, SSC Atlantic, 9456 Fourth Ave., Norfolk, VA 23511-2130, or call (757) 443-1775; DSN 646. E-mail: chips@navy.mil; Web: www.chips.navy.mil.

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

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

Online ISSN 2154-1779: www.chips.navy.mil

Cover



The Department of the Navy is working to eliminate the unnecessary collection of Social Security numbers to protect your personally identifiable information (PII). The SSN is involved in nearly 70 percent of DON data breaches. Educate yourself about identity theft and protect your personal information and the PII of your colleagues. The FBI's Internet Crime Complaint Center (IC3) (www.ic3.gov) offers the latest information about cyber scams and identity theft. For more information, visit the FBI's New E-Scams and Warnings Web page at www.fbi.gov/scams-safety/e-scams.

Contact the Federal Trade Commission to report identity theft using the online complaint form (www.ftc.gov/idtheft); or call the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261; or write Identity Theft Clearinghouse, FTC, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

DON CIO Privacy Lead Steve Muck discusses the history of the Social Security number, the proliferation of this unique personal identifier within the Defense Department, the Department of the Navy plan to reduce the use of the SSN, facts about identity theft, steps you can take to minimize identity theft and lessons learned from activities that have taken action to reduce the use of the SSN. Steve is the DON subject matter expert for privacy matters, advises the Senior Military Component Official for Privacy, develops privacy training and awareness and establishes privacy policy for the Department of the Navy.

Statement of Ownership, Management and Circulation

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

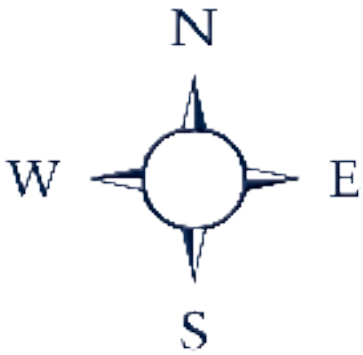
Date	1 July 2010
Title of Publication	CHIPS
Title of Publisher	U.S. Navy
USPS Publication Number	ISSN 1047-9988
Editor	Sharon Anderson
Frequency of Issue	Quarterly
Owner	U.S. Navy
Total No. of Copies Printed	30,500
No. Copies Distributed	30,420
No. Copies Not Distributed	80
Total Copies Distributed and Not Distributed	30,500
Issue Date for Circulation	July-September 2010
Location of Office of Publication	SPAWARSYSCEN Atlantic CHIPS Magazine 9456 Fourth Ave Norfolk, VA 23511-2130

Navigation

Feature Interviews with

Highlights

In Every Issue



From the DON CIO

Special Series on the Department of the Navy Social Security Number Reduction Plan

From Around the Fleet and Program Offices

Editor's Notebook

If you have any doubt that you could be the next victim of identity theft — think again — because new ways to beguile you into divulging your personally identifiable information (PII) spring up every day. The FBI's Internet Crime Complaint Center (IC3), at www.ic3.gov/, routinely reports on emerging scams. Since November 2010, the IC3 has reported identity theft and fraud related to payday loan telephone collection scams, e-mails promising sweepstakes or lottery prizes, and phishing and smishing schemes.

In phishing schemes, an identity thief poses as a legitimate entity and uses e-mails and scam websites to obtain victims' personal information, such as account numbers, user names, passwords, and more. Smishing is the act of sending fraudulent text messages to bait a victim into revealing personal information, like your Social Security number.

During the 2010 holiday shopping season, the FBI reminded consumers that cyber criminals create new, increasingly agressive ways to steal money and personal information. Identity thieves use many techniques to dupe potential victims, including conducting fraudulent auction sales, reshipping merchandise purchased with stolen credit cards, and selling fraudulent or stolen gift cards through auction sites at discounted prices. Identity thieves are not nice people and have been known to threaten victims with legal actions, arrests, and in some cases, physical violence, the FBI reported.

But the Department of the Navy is also aggressively working to educate its workforce about identity theft and properly control the use of your PII in the workplace. The DON is working to eliminate or reduce the collection, use, display and storage of the SSN through the DON Social Security Number Reduction Plan. By reading this issue of CHIPS, we hope to make you very skeptical and cautious about revealing your personal information — and very careful when handling the PII of others.

Another focus includes interviews with the brand new DON CIO, Terry Halvorsen, and an old friend and former DON CIO, Dave Wennergren, who is now the DoD assistant deputy chief management officer.

In November, CHIPS contributor Holly Quick and I exhibited CHIPS in the SPAWAR exhibit at MILCOM in San Jose, Calif. I also attended the fourth annual C5ISR Government and Industry Partnership Conference, cosponsored by the Charleston Defense Contractors Association and SPAWARSYSCEN Atlantic, in Charleston, S.C. The conference featured an eclectic mix of industry innovators and naval leadership speakers, and panel discussions led by subject matter experts.

A special thank you for the patience of CHIPS online readers who have experienced connectivity problems with the CHIPS website, www.chips.navy.mil, recently. The CHIPS website migrated to an enterprise solution, and we are working to make the CHIPS website better than ever. We are sorry for this temporary inconvenience to our readers. In the meantime, please do not hesitate to contact the CHIPS staff at chips@navy.mil for assistance.

Welcome new subscribers!

Sharon Anderson

Below, SPAWARSYSCEN Atlantic Technical Director Chris Miller and SPAWAR Commander Rear Adm. Patrick H. Brady address the audience at the C5ISR Government and Industry Partnership Conference. Other noted speakers included: SPAWARSYSCEN Atlantic Commanding Officer Capt. Bruce Urbon, NAVAIR Commander Vice Adm. David Architzel, Assistant Deputy Chief of Naval Operations for Information Dominance (OPNAV N2/N6) David W. Weddel and Director of Concepts, Strategies and Integration (OPNAV N2/N6) for Information Dominance Rear Adm. Kendall L. Card. Photos by Joe Bullinger/SPAWARSYSCEN Atlantic Photography and Video Services.

Above, the Space and Naval Warfare Systems Command exhibit at MILCOM in November 2010. Subject matter experts from SPAWAR activities led interactive panels and participated in discussion groups. Photo by Holly Quick.

A MESSAGE FROM THE

DON CIO

It is with great pleasure that I write my first CIO column for CHIPS magazine. I began serving as the DON CIO in late November, and my schedule has been full of activity. My first couple of months have been spent in fully understanding the functions and responsibilities of the position while establishing relationships with the Service Deputies, Assistant Secretaries of the Navy, operating commanders, functional area managers and echelon II command information officers.

Coming from the operational side of the house, I know from experience that the department's information technology (IT) infrastructure is strong and robust. We have more enterprise capability, the most secure enterprise network and a solid e-mail system. We also understand our cyber/IT workforce and have provided key input to congressional, federal, and DoD studies and plans on the current and future workforce. We know the kind of talent we need to build and maintain our network and have put enterprise processes in place to hire and train that talent.

We must continue our enterprise approach to IT and continue to build on our network capabilities, while improving effectiveness and realizing efficiencies in the way we do business. We will focus on actions that will make us more effective and efficient as an enterprise, including data center consolidation, network consolidation, and enterprise licensing to reduce the cost of the software applications we use. Recent direction from the Under Secretary of the Navy in a memo released on Dec. 3, 2010, spells out some immediate tasks related to our approach to IT and our information management (IM)/IT/cyberspace way forward *[Editor's Note: The memo is summarized on page 14]*.

As we apply an enterprise approach to DON IM/IT/cyberspace, we must examine all areas where enterprise processes can be applied for needed change. One of these areas is privacy. A strong and multifaceted enterprise privacy program will help ensure that commands/units consider privacy protections and controls when first making business decisions involving the collection, use, sharing, retention, disclosure, and destruction of personally identifiable information (PII). This isn't new and it needs to be part of our standard behavior. We need to look at how we deal with accountability in this area. Losing privacy information exposes us to risks similar to losing other government equipment and information.

This edition of CHIPS is dedicated to increasing awareness on the use of the Social Security number (SSN) across the DON enterprise. The SSN, when associated with a person's full name, is one of the key identifiers used to commit identity theft. A breach involving the SSN can result in financial or personal harm to an individual. It can also cause the accountable organization to suffer significant loss of reputation and public trust.

Safeguarding PII must be a priority at every level of the command/unit beginning with personnel who handle PII and leadership which must ensure that security controls, training and oversight are continually reinforced. A privacy program that reviews, justifies and strictly controls the use and handling of the SSN is a program that greatly diminishes the potential misuse and unauthorized disclosure of this unique personal identifier. The unauthorized disclosure of the SSN associated with a person's name may result in real consequences as commands hold personnel accountable for privacy violations. I still see too many forms requiring the full SSN when it is not required; we need to get better at this.

In this issue of CHIPS, you will find articles that describe the original purpose of the SSN and its expanded and widespread use today. There is an outline of the DON SSN Reduction Plan currently in progress and some lessons learned from DON activities that have taken steps to reduce and/or eliminate use of the SSN. I encourage you to visit the DON CIO website at www.doncio.navy.mil/privacy for more information about the DON Privacy Program. CHIPS

Terry A. Halvorsen

DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER
www.doncio.navy.mil

A Conversation with David M. Wennergren
DoD Assistant Deputy Chief Management Officer

David M. Wennergren

David Wennergren was selected to become the new Assistant Deputy Chief Management Officer (DCMO) for the Department of Defense in October 2010. He previously served for four years as the Deputy Assistant Secretary of Defense for Information Management and Technology/Deputy Chief Information Officer, providing top-level advocacy in creating a unified information management and technology vision for the Department of Defense and ensuring the delivery of the capabilities required to achieving the department's transformation to net-centric operations.

Prior to the Deputy DoD CIO job, Mr. Wennergren served for four years as the Department of the Navy Chief Information Officer (DON CIO), where he was responsible for the development and use of information management/information technology (IM/IT) for the Navy – Marine Corps team.

On Oct. 26, 2010, Defense Secretary Robert Gates named Teri Takai as the new DoD CIO. As a part of the Secretary's ongoing efficiency efforts, the position of Assistant Secretary of Defense for Networks and Information Integration will be eliminated, and so Takai will serve just as the DoD CIO. Joining her as the new DoD Deputy CIO is former Department of the Navy CIO, Robert J. Carey. Mr. Carey was named Deputy DoD CIO in October. In an interesting twist, this is the third time that Carey has succeeded Wennergren in a position. Carey took over as DON Deputy CIO when Wennergren became the DON CIO in 2002, and then again took Wennergren's place as DON CIO when Wennergren moved to the DoD position in 2006.

An optimist and change-leader, who advocates collaboration, teamwork and process transformation to enable successful IT change, Mr. Wennergren brings tremendous passion and vision to any undertaking. Wennergren was one of an inspired group of naval leadership who led the DON to "think like an enterprise" in IM/IT planning and management.

The Office of the Deputy Chief Management Officer is responsible for Defense Department business process change, strategic planning, performance management, IT acquisition reform and the successful deployment of the department's large business IT projects, such as Enterprise Resource Planning systems.

CHIPS talked with Mr. Wennergren in November as he prepared to move to his new job and asked him to discuss the role of the DoD CIO and his vision for the future as the DoD's Assistant Deputy Chief Management Officer.

CHIPS: Can you discuss some of the accomplishments of the DoD CIO organization? Some pundits said the organization was hampered in what it could accomplish by its limited authority and lack of resources.

Wennergren: It was a great ride, and the team accomplished a lot. And it went by so fast. I certainly don't think we were hampered by a lack of resources; but rather that we are a part of a huge and complex organization that has had a long history in information management of not always working together as a united enterprise. We're dealing with issues of significant cultural change, trust and the willingness to relinquish personal control. It's like the old saying: 'If these were easy changes, they would have already been done.'

There are a lot of things that we have accomplished in the last four years that I'm very excited about. We paved the way to be an integrated DoD information enterprise. First we aligned ourselves to a common mission and purpose to create an information advantage for our people and our mission partners. Galvanizing our team, we then developed the first-ever DoD-wide information enterprise strategic plan and roadmap, and are using these goals, objectives and measures to vet all the IM/IT work done by the DoD to see if it is aligned to the department's mission and vision. Because if it's not helping to accomplish our goal, why should we be expending our energy on it? Our strategic planning process is highly collaborative, using a wiki-based approach to ensure that all of the DoD components can collaborate on what the goals and objectives of the plan should be and what the roadmap should look like to accomplish those goals.

Today, it is much less about building another big IT system and much more about understanding how data can be exposed and Web services can be developed rapidly and reused across the organization. We have our net-centric data and services strategies in place, and through the work of our communities of interest, we have seen a number of functional areas that have adopted the idea that if you can expose your data, you can deliver new information capabilities much more rapidly than you would have done in the very recent past.

As you look across the organization, you will see examples of how that data strategy has been put into place. [For example,] in maritime domain awareness, I can get on any DoD computer and immediately see the status of commercial vessels, cargos and crews around the world. Similar advances have been made in Blue Force Tracking and in the ongoing work to find IEDs (improvised explosive devices). And now we have a service being made available to DoD military installations to help assess whether a visitor to a base is a good guy or bad guy before we grant them access — instantaneously and on-the-spot. These are just a few examples of people using the data strategy.

The power of a service-oriented world is that you don't have to automatically replace a legacy system with another big system that takes years to deliver and never delights anyone because it is trying to appease everyone. Instead, you could take advantage of a 'Web services world' where there are core enterprise services that are delivered at the corporate level, like smart cards, public key infrastructure, collaboration, messaging, and more. Local commands don't have to duplicate this work and can then focus their energies on using the enterprise services while they quickly build out the services and applications they need for their specific mission or functional area.

We put into place the first set of core enterprise services that are mandatory for use across the entire Department of Defense: collaboration service, content staging and content discovery. There is now a list of 10 or 12 enterprise services, like people directory services, attribute services, and machine-to-machine messaging services, that are going to be added to that list of core services that everyone has to use.

As individual organizations use these enterprise services, rather than try to duplicate them, they can focus their energy on bringing innovation and improvement to their areas of expertise. If you are the logistician, you can build logistics services, and if you are the meteorologist, you can develop weather services and you can post the services where they can be reused and improved by others.

I am thrilled with the work the Defense Information Systems Agency has done to help make this vision a reality. They have their first cloud computing offering called RACE, the Rapid Access Computing Environment. DISA also created Forge.mil, which is the common development environment where you can develop and test your applications in the environment in which they will have to operate, and then you can post the code for reuse.

There is a lot of work bringing us together to function as an enterprise rather than as individual stovepipes or as individual components. This year we had a great partnership with the intelligence community, who owns physical security policy for the Department of Defense, to create a Web service that will be available to every gate guard on military installations so that when somebody wants access and they swipe their identification [card], it will reveal whether or not there are outstanding warrants on them or if they are a suspected terrorist. These kinds of uses with data being available real time as a service anywhere are some of the things that I am really excited about that we have accomplished.

We have turned a corner on recognizing that the Web 2.0 phenomenon is the way business will be done and not just a quality of life issue or a way of keeping track of friends and family. It really is the way that work will get done in the future.

We published for the first time ever a policy on the use of Internet-based capabilities like social networking services so that we could both improve security and ensure that our people have access to the tools they need to get the mission accomplished. It was an effort that has helped our organization begin to embrace the idea that security in the 21st century can't be just reactive, we can't just block access to websites and assume that people will still be able to get their job done. Instead, we have to recognize that people need to have access to things like social media and social networking services and use them appropriately. Through a combination of educating and training our users, coupled with technology tools, like content filtering at our gateways, you can have an informed and protected workforce that can still watch a YouTube video or connect with somebody on Facebook to get the mission done.

"The power of a service-oriented world is that you don't have to automatically replace a legacy system with another big system that takes years to deliver and never delights anyone because it is trying to appease everyone. Instead, you could take advantage of a 'Web services world' where there are core enterprise services that are delivered at the corporate level."

We also published guidance to help people recognize that open source is a viable option and should be considered in new development work. In addition, the Enterprise Software Initiative, co-chaired by my office and the Department of the Navy CIO team, has been a huge success, and continues to pay big financial dividends for us. Through the use of enterprise licensing agreements, we are up to about $4 billion in cost avoidance for the department over the last decade.

We have done a lot of work with architecture so that for the first time ever we have a DoD Information Enterprise Architecture, a strategic-level architecture that all mission areas and all DoD components have to comport with, which allows users to comply to common business rules and then build reference architectures and solution architectures within their organizations. Likewise, we have done work to improve the DoD Architecture Framework so that people can have the right kind of architecture artifacts. If you are doing an Enterprise Resource Planning solution, you will need different architecture documentation than if you are developing a Web service.

Another thing that I am very excited about is the importance of the workforce of the future. The DoD CIO team was instrumental in putting together (on behalf of the whole Federal CIO Council) a Net Generation workforce report. If you haven't had a chance to look at it [www.cio.gov/pages.cfm/page/Recruiting-the-Net-Generation], I would commend it to you. I think it came out well. We had a partnership with Don Tapscott, the author of 'Wikinomics' ['Wikinomics: How Mass Collaboration Changes Everything'], 'Growing Up Digital' and a number of other books. I think it is valuable wherever you work, whether you are in government or industry, whether you are an IT leader or any federal manager, to understand the Net Generation, which is the primary workforce that we would like to attract and retain.

Baby boomers like me are getting ready to retire and Generation X, which comes after my generation, is a smaller population. In the Millennial Generation, or the Net Generation as Don Tapscott refers to them in his work, there is a larger population and they are going to fill leadership positions at a younger age as baby boomers leave the workforce. The good news is that the Net Generation has a desire for public service; the bad news may be that if you don't provide them with the tools and technologies they use to manage their lives, and you don't give them the right kind of leadership opportunities, and encourage and mentor them, they may not stay. I think it is a challenge that we all need to be thoughtful about. In the guide there's some good information to help you understand the values, norms and beliefs of the Net Generation, as well as showing you how you can use the federal system to be an employer of choice.

I do love change management, and that's why I am really excited about the Deputy Chief Management Officer team.

If you look at the traditional portfolio of many CIOs, a lot of the work that I have enjoyed most is the work that CMOs do. The DCMO team is responsible for business process change, business process reengineering, strategic planning, change performance management, and planning the future for business IT capabilities. It's a tremendous opportunity to look at the end-to-end processes of the department, and focus on process improvement first and then insert technology appropriately to deliver new capabilities much more rapidly.

CHIPS: In your time in the office of the DON CIO and as DON CIO you led the Department of the Navy through transformational IM/IT business processes and improvements such as the implementation of the Navy Marine Corps Intranet, the combination of Common Access Card/PKI use and partnership in the Enterprise Software Initiative. As you look back, have these changes met your expectations?

Wennergren: With any change management issue, particularly the ones that are big, you can always reflect back and see that there are a lot of things that you might do differently. The Common Access Card and public key infrastructure certificate use has been a very positive thing for the Department of Defense. Mary Dixon, the Director of the Defense Manpower Data Center and a true leader in the identity management field, called me the other day to remind me that Oct. 6, 2010, was the 10th anniversary of the issuance of the first Department of Defense Common Access Card. At that time, I was the DON Deputy CIO, Dan Porter, my mentor and great friend, was the CIO and Rob Carey, another great friend, was our e-business and smart card team leader. Look how far we have come!

We have 3.5 million people that use the CAC for cryptographic logon to the network, which has significantly reduced successful password cracking into the networks, which is a big deal. It costs a lot of money to clean up when people break into the network. Raising the bar on security with cryptographic access and helping to move away from a world where you have hundreds of websites, all with different user IDs and passwords, as well as being able to use the cards for legally binding digital signatures, are other key accomplishments. You can move away from all those labor-intensive paper processes. I can sign a travel claim and have money in my bank account 24 hours later, and this can only happen because of things like the Common Access Card and its PKI credentials.

"We have turned a corner on recognizing that the Web 2.0 phenomenon is the way business will be done and not just a quality of life issue or a way of keeping track of friends and family. It really is the way that work will get done in the future."

On the physical access front, aligning the use of the Common Access Card for access to military installations and coupling that with services that are available to let you know if someone is still a valid member of the community and eligible for access is another important use of the technology.

There is a fascinating dichotomy of change. Some change management efforts are best done locally in an evolutionary approach to change management where you can keep it small and agile with local people involved who have a strong sense of ownership. Whenever it is possible, change that starts locally is always a good thing because it has grassroots support.

But some of the fundamental changes that we have gone through can't happen if they are only done locally, one by one. While you can get people excited about building Web services instead of buying big IT systems locally, we would not have a single Common Access Card if we tried to implement this change locally. Sometimes you have to have a revolutionary change strategy where you just demand change of the entire organization. If you hadn't, you would have 100 different PKI solutions, they wouldn't be interoperable, you wouldn't be able to share signed e-mails and build interoperable systems that use digital signatures and do all the things that the CAC and PKI give you the power to do.

CHIPS: I read that the DoD may add multiple functions to the CAC to transform it into a debit card to reduce the number of cards personnel must carry. Do you forecast any other leaps in functionality in technologies that the department is using right now?

Wennergren: Yes, we are continuing to expand use of the CAC, which also has a contactless capability on it; we haven't used it a lot yet, but we will be using it more and more. You will be able to use the contactless capability on the CAC to access a building or ride the Metro if you live in the D.C. area instead of having a separate Metro card. We're also looking at using the CAC to replace the other cards we use for financial transactions aboard ships or on military bases. These are the kinds of things that can happen once you get an enterprise solution into place.

Can you continue to improve how you implement these efforts? Yes. Should you take time to learn from what has happened in the past? Absolutely, as long as you remember that the pace of change is relentless, and your learning about how to improve on the past is at a rate that keeps pace with the technological changes that surround us.

NMCI is another good example of learning from the deployment of an enterprise solution. I firmly believe that the Navy is better off by having implemented the Navy Marine Corps Intranet. There were hundreds, literally thousands of networks, 100,000 legacy applications, differing security models, and absurd tech refresh rates — horribly long for operational commands because operational commands did not have the money that well-funded RDT&E (research, development, test and evaluation) and Working Capital Fund activities had. And there are also lots of valuable lessons learned about how the program was implemented and how it could be improved.

I think the power of performance-based contracting, the power of doing things as an enterprise, like enterprise e-mail, the power of using NMCI as a forcing function to eliminate duplicative applications and networks, the power of moving away from fragmented security architectures on individual bases and moving away from local active directory forests are all things that the other military departments are working on now, and these are all things that NMCI helped bring to the Navy and Marine Corps team years ago.

So there is a lot of positive [change] that came out of NMCI. And it's also true that the world has changed a lot, and the Navy and Marine Corps team has also learned from the aspects of NMCI that didn't work as well in a very joint and fast moving world. And these lessons learned will help the team do even better as they [DON] move to the Next Generation Enterprise Network (NGEN) initiative.

In another example about how enterprise initiatives need to continue to change, in the early days of the Enterprise Software Initiative, the focus was on aggregating known buying demand. If you were going to buy 50 licenses from Oracle, I was going to buy 100 licenses, and someone else was going to buy another 100, we could aggregate demand and try to get a better deal. Then the licensing [model] began to evolve from only aggregating known demand to creating enterprise-wide licensing agreements for the Department of the Navy, recognizing that you could get an even better deal if you license your entire organization.

And now our strategy has matured even further, allowing us to do things like the Data at Rest Solutions enterprise licensing agreement [see page 50], where we also picked the products that best met our needs and put into place a vehicle where you can buy only those products. And by the way, we made that contract available to every federal, state and local government in the country so that everybody can benefit from this leveraging of our buying power.

In spite of some of the hype around service oriented architecture, Web 2.0 and cloud computing — they will be fundamental technology changes for the department — and we must take advantage of them. If we understand and use them effectively, we will deliver information capabilities much more rapidly, we will be more agile — and we will delight our customers.

Successful use of service oriented architecture allows you to build Web services and applications much more quickly than you can build big IT systems. If you think about maritime domain awareness, when we want to learn more about commercial vessels and their cargos and crews coming into harbors, we could have tried to replace all the legacy systems in the Navy, intelligence community, Department of Transportation and the Coast Guard with some big new system, but we recognized that it would take years. The right thing to do was to expose data so you could quickly mash things up, overlay it on something like Google Earth and have a result immediately.

"There is this democratization of technology taking place where a young Navy lieutenant or Air Force major can build a Web service, post it someplace like Forge.mil, where it can be reused in Apps for the Army or the DoD Storefront, and other people can use it, reuse it and build upon it. That kind of stuff happens overnight rather than in weeks or months."

So I can go on any DoD computer and stick my Common Access Card in and have situational awareness about maritime domain awareness from any workstation. That's powerful — and it doesn't have to take 80 months to do a big IT system. There is this democratization of technology taking place where a young Navy lieutenant or Air Force major can build a Web service, post it someplace like Forge.mil, where it can be reused in Apps for the Army or the DoD Storefront, and other people can use it, reuse it and build upon it. That kind of stuff happens overnight rather than in weeks or months.

Then if you explore the power of cloud computing, which eliminates a bunch of data centers that are underutilized, over cooled and fragmented, we will reduce costs. And if you could move your desktop into the cloud, use thin clients, where appropriate, be connected from anywhere, and be able to find the people and information that you need to get your job done whether you're on the road or at home, not only will it improve information sharing but it will also improve security. We spend a lot of money to secure the desktops and laptops that we put in offices. There is a sort of 'perfect storm' of technology around the power of cloud computing, the Web 2.0 phenomenon and using a service-oriented approach. If we sync those together we will come up with a world that allows us to go from years to getting new solutions into place to days and weeks.

CHIPS: Do you have a 90-day plan or any immediate priorities as you take on your new job? Does IT play a major role in your vision for improving business processes?

Wennergren: One of the big priorities for the DCMO team is optimizing the end-to-end business processes of the Department of Defense. This is an important shift from our traditional view of only looking at things within functional or organizational stovepipes. If you think about process change first, then you can decide how to insert technology at the right moment rather than what we have done in the past, which is to become enamored with building an IT system.

Rather than focusing first on building a system, we should look thoughtfully at what capability we want to deliver. There are a couple of things going on now that will be helpful in this regard, one is IT Acquisition Reform. Section 804 of the [National Defense] Authorization Act for Fiscal Year 2010 had a provision about reforming IT acquisition, which is another initiative that the DCMO team leads. It will be an end-to-end look about how you determine requirements, how you spend money, contracting, testing, program management and governance.

We are going to look at things differently in order to deliver information capabilities more rapidly. If you think about the result that you want to achieve, you might use a different process. If you decided that you wanted to build an ERP [system], the steps to do it would look significantly different with a lot more oversight and rigor because of the amount of money that you would spend and the complexity of the effort. Deploying a Web service or buying a managed service would have a quicker timeline and a different set of steps.

The IT Acquisition Reform work will be one of the big things we will be working on as well as the IT Consolidation Roadmap. Partnering with the CIO team, there are a number of consolidation and alignment actions that will create an integrated 'DoD Information Enterprise' that aligns the activities of all of our DoD components, as well as increasing effectiveness, improving security and reduc-

ing costs. There is clearly great synergy between CIOs and CMOs and information is at the heart of it.

I don't have a 90-day plan. I am going to jump on board and see how I can help Beth McGrath (Elizabeth A. McGrath, Deputy Chief Management Officer for the Department of Defense) with the big portfolio of work that she has. We are hoping to have the IT Consolidation Roadmap to the Secretary of Defense before the end of the calendar year. The IT Acquisition Reform Task Force work is ongoing and should have clear deliverables this fiscal year. We'll also be looking at some end-to-end processes for the department, like 'procure to pay' and 'hire to retire.'

While we have this vision of using more Web services and cloud computing, we still have some big IT systems that are still in the process of delivering. Every one of the military departments has ERPs, and we'll be helping to make sure those initiatives deliver value and deliver quickly.

In addition, there are some opportunities in aligning strategic planning efforts of the department and focusing efforts on performance management with outcome-based measures to assess the progress of our plans.

CHIPS: Because of DoD's stringent security requirements, the department traditionally has had to delay in deploying new technologies. Are there any emerging technologies that you are watching for possible implementation in the department?

Wennergren: The pace of technology changes so fast, there is always something new going on. We are already taking advantage of the Web 2.0 world, the powers of mass-collaboration and social networking, and the ability to expose data and do mashups overnight rather than spending months or years to build an IT system. This is a radical change, and it affects every aspect of the way we do our business.

And yet we still spend a lot of time talking about building IT 'systems,' we still talk about 'systems views' of architectures and 'systems certification and accreditation,' and so we are a long way yet from fully recognizing the power of a Web 2.0 service-oriented world. The use of Web services and cloud computing are technology shifts that we are going to have to stay on top of, not only if we want to deliver information capabilities more rapidly and more cost effectively, but also if we expect to be an employer of choice for the Net Generation workforce, a workforce that expects to be able to use these tools and techniques.

We will also need to be open-minded about the technology that we use to get our job done. A decade or so ago, I used to have better computing capabilities in my office than I did at my home. I wonder how many of your readers feel that way today. They probably have more computing power at home than they do in their office. Droids, iPads, iPhones, BlackBerries, and the like, are powerful channels that allow users to get work done from anywhere, so we better be thinking about a future that allows users to get on any computing device, whether it is government provided or not, to get the job done. We will have to work through security issues so users will be able to use the best technologies at their disposal.

We need to understand that we have a highly mobile workforce. We can't talk out of both sides of our mouth. We can't demand a culture that demands self-service, but then not be able to provide every reservist or National Guardsman a laptop and also say, 'Oh by the way, you can't use your own device to get your work done.'

We must be a highly functioning information-age organization, ready to embrace and effectively leverage the tools and technologies that are available to us today. And, you know, so much of this comes down to people issues. The technology is out there to allow you to never again have to take eight to 10 years to field a big IT system, to never again be thwarted by the fact that you can't be connected anywhere, anytime to get the job done. It's a world full of change, but one brimming over with tremendous opportunity, and we must seize this opportunity.

CHIPS: One more question, I've always enjoyed hearing about your reading list. What are you reading right now?

Wennergren: I am a huge believer in the power of continuous learning and the importance of leading by example. We did a thing with my CIO team called 'Expanding Horizons,' where I have a wonderful team in Barry and Jeanne Frew, who helped me when I was at DON CIO and have continued to help me at the DoD CIO team. We get the team together five times a year and read a book. And then we talk about how that book has practical applications for leadership, management and information technology for the future. The sessions help align the team, and help us to keep looking outside of ourselves for new ideas and approaches.

There are so many good books to read; let me offer you a couple that get at the heart of some of the issues facing us today. I believe that across the Department of Defense, just like across a lot of large private sector firms, we operate in a low trust environment, and that low trust environment creates a huge tax that you pay in terms of how much it costs to get things done and how long it takes to get things done. There is an interesting book by Stephen M.R. Covey Jr. called 'The Speed of Trust: The One Thing that Changes Everything.' It discusses how you can create high trust organizations.

Another issue that we face across DoD is maintaining a true sense of urgency. For that topic, I'd recommend the John P. Kotter book, 'A Sense of Urgency.' Years ago, Kotter wrote 'Leading Change.' In that book, he talked about the eight steps of change, and the first step was to 'create a sense of urgency.'

Since that time he has realized that this is the key step, and he offers a lot of sound advice on how to create and maintain a true sense of urgency.

There is also an interesting book by Robert Quinn called 'Building the Bridge As You Walk On It: A Guide for Leading Change' which is a powerful book about how to live with change successfully and address change in your personal and your professional life.

There are so many good books out there that there is no excuse not to grab one and take it for a ride. You will not only be expanding your own horizons, but you'll be setting the right example for your teammates too. CHIPS

For more information about the DoD Deputy Chief Management Officer (DCMO), go to http://dcmo.defense.gov/. For information about the enterprise licensing agreements mentioned by Mr. Wennergren, go to page 45 for Enterprise Software Initiative (ESI) agreements or visit www.esi.mil.

AN INTERVIEW WITH MR. TERRY A. HALVORSEN
Department of the Navy Chief Information Officer

As the DON CIO, Mr. Halvorsen heads the Office of the DON CIO and is the DON's senior official and adviser on matters related to information management (IM), information technology (IT)/cyberspace (including National Security Systems) and information resources management (IRM). Mr. Halvorsen has oversight for the IM function within the Office of the Secretary of the Navy, Chief of Naval Operations, and Headquarters Marine Corps. He develops strategies, policies, plans, architectures, standards and guidance, and provides process transformation support for the entire Department of the Navy. Additionally, he ensures that the development and acquisition of IT systems are interoperable and consistent with the department's objectives and vision. Mr. Halvorsen also serves as the department's Cyber/IT Workforce Community Leader, Critical Infrastructure Assurance Officer and the Senior Military Component Official for Privacy.

Prior to becoming the DON CIO, Mr. Halvorsen was the Deputy Commander, Navy Cyber Forces. He began serving in this position in January 2010 as part of the Navy cyber reorganization. Previous to this, Mr. Halvorsen served as the Deputy Commander, Naval Network Warfare Command. He was responsible for providing leadership for more than 16,000 military and civilian personnel and supporting over 300 ships and approximately 800,000 computer network users, all globally dispersed. In this position he was responsible for the business performance of Navy network operations, space operations, information operations and knowledge management. Mr. Halvorsen was directly involved in establishing governance structure, processes and mechanisms to optimize more than $8 billion in Navy resources.

CHIPS asked Mr. Halvorsen to talk about his experience and job as the new DON CIO.


Mr. Terry Halvorsen

CHIPS: Your responsibilities as the deputy commander of Navy Cyber Forces, U.S. Fleet Forces deputy ACOS, and deputy commander for NETWARCOM hold similarities with your new responsibilities as DON CIO. You are also a Reserve Army officer, so you have experience as an operational commander. Can you talk about the unique insights and experience you bring to the DON CIO position?

HALVORSEN: The insight and experience I bring to the position is that I am familiar with the challenges encountered in the operational world outside the Beltway. I know that some of the applications we give our Sailors and Marines to use don't quite do the job, especially in their bandwidth-constrained environments. It is really challenging in the afloat and expeditionary environments.

As deputy commander at Navy Cyber Forces and Naval Network Warfare Command, I was directly involved in initiatives to improve cybersecurity by eliminating or moving systems onto better protected networks. So I also bring to the table an understanding of the operational challenges of ensuring cybersecurity in the DON.

CHIPS: What are your thoughts as you move from an operational environment to a largely policy and guidance role as the DON CIO?

HALVORSEN: Before answering this question, I want to emphasize that the role of the DON CIO is more than 'policy and guidance.' A key function of the DON CIO is to operationalize (not to operate) the IM/IT/Cyber Strategy for the department and then to use policy, guidance, and other mechanisms to guide the department toward achieving the goals and objectives associated with these strategies. As the DON CIO, my focus is on the 'DON Enterprise.' We have to keep the entire enterprise in mind in all we do, while also keeping in mind the realities of our limited resources.

From my experience in moving from the operational environment to the DON CIO, I realize we have to keep the warfighter in mind as we write policy. I just mentioned some of the challenges faced by our warfighters. Our IT policies and strategies must consider all of these challenges, and we must write them to be understood and implemented at the operational level.

One of the things I told my team of DON CIO directors during our first meeting together was that I would ask two questions when writing new policy: how is it helping the customers at all levels and how do you operationalize it?

CHIPS: The DON CIO has a broad portfolio of responsibilities: assuring DON access to the electromagnetic spectrum; enterprise architecture; Clinger-Cohen Act Compliance; the IT investment strategy; critical infrastructure protection; and DON privacy and civil liberties officer, to just name a few. Have you developed a 90-day plan or do you have any immediate concerns for quick resolution — and a long-term vision?

HALVORSEN: Yes, we have a broad portfolio, but we must narrow our focus for some quick wins. We are working on a 100-day plan while we are in the process of strategic planning with the Navy and Marine Corps Deputy CIOs and the service operational commanders. We are in the early stages of planning, but I can tell you that we will focus on DON IT efficiencies — becoming more effective and efficient as a department in information management and IT/cyberspace procurement and business processes. The Office of the Secretary of Defense and the SECNAV are serious about becoming more efficient in the way we do business, and we have identified some key tasks related to IT efficiencies within the department. We will also focus on the IT workforce and of course, our networks. We will not stop working the other initiatives we are responsible for, but I believe we should focus our effort on these areas in the near term to bring long-term results that benefit the entire department.

CHIPS: You have held numerous positions in the training and education community, and you were one of the principal architects of the Navy's reengineering efforts that resulted in the pivotal Revolution in Training. What opportunities exist for the cyber/IT workforce in training, education and development and for those looking to enter into government service in the DON?

HALVORSEN: There are a multitude of training and education opportunities and many of them revolve around e-learning. Within the government, e-learning systems are available to our workforce, there are approximately 3,000 training courses. Topics range from engineering to business to IT and technical management courses. While the department must continue to embrace e-learning, it must also be improved to better support our customers. E-learning, supplemented by sound exercises and simulations, is a critical element to the training of our cyber/IT workforce.

Within the last three years both the Navy and Marine Corps Information Systems Technician and command, control, computers and communications schoolhouses have revamped their curriculum. They now include Information Assurance and commercial IT-related certifications — some of the same certifications that are sought after in commercial industry. We are standardizing our military, civilian and contractor training through baseline commercial certifications.

We have training and education initiatives underway to strengthen and broaden the cybersecurity workforce. For those looking to enter the government, the Navy and Marine Corps have instituted recruiting incentives for highly skilled individuals, scholarship programs and internships. For example, Schedule A hiring authority was put into effect through December 2012 (www.public.navy.mil/donhr/Employment/CivJobOpps/Pages/CyberSecuritySchedA.aspx) to allow the department to quickly hire more than 1,000 cybersecurity professionals. The Information Assurance Scholarship Program pays for master's and doctorate degrees in IA-related fields, and there are internships available for college students. All of these training, education and development initiatives have been developed to make our IT workforce capable of handling the challenges of supporting our warfighting mission, and we want those interested in government service to know about them.

CHIPS: What do you see as the DON's biggest cybersecurity challenges right now?

HALVORSEN: The threat to our networks is sophisticated, organized and dynamic, and our resources are limited. Since there is a greater demand today for information sharing, our biggest challenge is to maintain the security and effectiveness of our networks while enabling appropriate access. And we must do this while reducing cost. We must have qualified people and clear, well-coordinated priorities. Everyone who touches a computer is part of the cybersecurity workforce. Knowing the basics of how to operate safely in the Web environment is everyone's responsibility. Doing the basics: keeping virus scan updated, not connecting unauthorized devices, reporting when you get a suspicious e-mail; all of these can make us more secure but it requires all of us to participate.

Our Navy Marine Corps Intranet has served us well in the area of cybersecurity. Many of us have short memories, but I remember the cyber attacks that affected

DON CIO RESPONSIBILITIES

- ❑ Reports directly to the Secretary of the Navy (SECNAV).
- ❑ Heads the office of the DON CIO.
- ❑ Is the DON's senior information management, information technology (including National Security Systems), and information resources management (IRM) official.
- ❑ Serves as the department's principal adviser on IM/IT and IRM matters.
- ❑ Is responsible for IM/IT and IRM matters.
- ❑ Has oversight for the IM function within the Office of the SECNAV, the Chief of Naval Operations and Headquarters Marine Corps.
- ❑ Carries out the IM/IT responsibilities and duties set forth in Title 10, 40 and 44, U.S. Code.
- ❑ Provides oversight of strategic planning for all information and IT management functions.
- ❑ Provides oversight for IT capital planning and investment management.
- ❑ Provides oversight of compliance for protecting information and systems.
- ❑ Provides oversight of the process of developing and maintaining the DON enterprise architecture and assesses compliance with DoD and federal interoperability standards.
- ❑ Develops DON-wide IM/IT policy, standards and guidance.
- ❑ Provides oversight of DON IM/IT compliance with applicable statutes, regulations, policy and guidance.
- ❑ Ensures that DON IT complies with government and DoD standards and is interoperable with other relevant IT systems.
- ❑ Serves as the DON Critical Infrastructure Assurance Officer (CIAO), responsible for all aspects of the Department's Critical Infrastructure Protection program, including both physical and cyber assets.
- ❑ Serves as the Senior Military Component Official for Privacy.
- ❑ Promotes the effective and efficient design and operation of all major IRM processes, including improvement to DON work processes.
- ❑ Serves as the Community Leader for the DON Cyber/IT Workforce and develops Cyber/IT workforce policies, plans and guidance, in coordination with the Assistant Secretary of the Navy (Manpower and Reserve Affairs), as appropriate, to ensure that the DON has sufficiently trained personnel in IM/IT competencies.

our networks before NMCI. Since deploying NMCI across our shore-based users in the United States, Japan and Hawaii, successful cyber attacks that disrupt our networks have dropped to zero. NMCI is the largest intranet in the world serving 700,000 users and supporting 124,000,000 browser transactions per day. NMCI is second in size only to the Internet.

NMCI made our network more robust and able to withstand attacks, and we will continue to make that a requirement as we focus on advancing the Next Generation Enterprise Network and Naval Networking Environment. Our goal is to provide an interoperable enterprise environment that is standardized and enables secure access to data and services across the DON. *[Editor's Note: In this issue, Capt. Timothy Holland (NGEN program manager) and Capt. Scott Weller (NMCI program manager) report on the NMCI continuity of services contract and NGEN. See page 29.]*

CHIPS: One of your roles as the DON CIO is the Senior Military Component Official for Privacy. You are responsible for privacy program oversight and policy. What are your thoughts about this program remaining under the DON CIO?

HALVORSEN: The DON CIO was appointed the Senior Military Component Official for Privacy for the DON in October 2009. The visibility and challenges of this function are significant and well suited to remain within the DON CIO. Making the CIO responsible for privacy seems to be the inclination across the federal government because in 17 of the 27 federal agencies, the CIO has oversight of the privacy function.

The bulk of personally identifiable information (PII), which is the number one privacy concern, is collected, displayed, transmitted and stored via electronic means vice hard copy, and that trend is growing. The DON CIO has been aggressive in implementing the means to protect PII. Last year the DON CIO took initiatives to protect the broader category of 'sensitive' information on our mobile devices by employing encryption of data at rest (DAR). This has significantly improved the protection of that privacy sensitive data. The DON CIO has also taken numerous steps to drive down both the number of incidents and the number of personnel impacted over the past year, and we will continue implementing corrective action through policy changes. We will be emphasizing accountability. This isn't new to anyone; the education and training are in place. We need to raise the level of personal accountability in this area.

CHIPS: At Naval Network Warfare Command, you led the Navy's Cyber Asset Reduction and Security initiative, which identified more than 1,200 networks as vulnerable to cyber attack. As a result, 828 of the networks were eliminated to save $20 million and significantly improve security. The CARS effort is part of the Navy's larger effort to implement the Naval Networking Environment. Can you talk about NNE progress?

HALVORSEN: We are on pace with the Secretary's timeline of publishing an overarching NNE strategy document to align the governance, administration, operation, investment and acquisition of DON IM, IT/cyberspace and IRM resources and assets. Additionally, the services are on pace to align with NNE efforts.

The Navy's Convergence to a Single Network (CSN) initiative supports its Information Dominance Vision (published May 2010) of a single unified information environment. The Marine Corps Enterprise Network (MCEN) remains the Corps' general service, common user network environment enabling MAGTF C2 (Marine Air-Ground Task Force command and control), business, intelligence, and enterprise services systems, applications and users.

Together, the NNE shall become the Department of the Navy's net-centric environment that securely, effectively and efficiently leverages the full range of information resources. Once the NNE strategy is published, we will begin development of supporting strategies that will leverage Navy, Marine Corps and Secretariat level stakeholder participation to achieve the necessary changes and desired outcomes.

CHIPS: SECDEF has proposed significant changes to the DoD organizational structure and processes to reduce redundancies and ensure that essential national security programs are sustained. Do you have any plans to revamp processes or realign resources within the office of the DON CIO?

HALVORSEN: I don't know yet; we are going to look at everything we do in the DON CIO, and we will make changes and realign resources where necessary. For example, I think some teams that are operating separately would be more effective if they came together under one team. Their work crosses over into each other's areas, so I hope to leverage that and help them work together better.

Coming in as an 'outsider' to the DON CIO, I realize that people don't quite understand our organization chart and the functions of each team. I hope to improve communications about the organization so that people outside will know who to go to for help in different areas. I also want to establish measures and metrics that ensure the DON CIO is providing value to the department and the services.

CHIPS: Decision speed is more important than ever. What are your thoughts about the delicate balance between the need to share information and collaborate with the need for security?

HALVORSEN: The reality is that we live in an environment where we have to be able to collaborate within and outside DoD, and do so securely. So it's not one or the other — the need to share or the need for security — it is a need for secure, balanced information sharing. A great example of this that we've been involved in is the North Chicago Veterans Affairs Medical Center. It will be the first fully integrated federal health care center between VA and DoD.

So, we are working with them to achieve interoperability of all our IT systems in the area. A VA employee should be able to securely access the Navy system when needed, and likewise, Navy personnel should be able to securely access the VA system when needed. They are working together so we are making sure they can truly work together — sharing the information needed in their IT systems. In the DoD we go places that are dangerous, we take prudent risks, establish standard operating procedures, and we execute. Cyberspace is another environment we must operate in to be successful.

CHIPS: Do you see the value in social media or Web 2.0 tools, and do you plan to blog?

HALVORSEN: I see the value in social media/Web 2.0 tools and I encourage the department to continue to leverage technologies associated with them where it makes sense to do so. These tools enable effective collaboration, at a low or no cost to implement, across a broad spectrum of individuals from the DON, DoD and federal government. That being said, I do not plan to blog. There are many ways for me to get my message out, CHIPS magazine being one of them.

For those who liked the back and forth exchange that the blog allowed, we have a site that was set up to encourage this type of exchange but in a secure environment that is behind the DON firewall. There are many people in the DON with good ideas and information to share. And this site, called the Pulse, is a place where they can do that. I caution that in using social media, we must be mindful of the inherent security risks they may pose. There are some applications where, with careful use, social media is the right media for communication and collaboration. For more in-depth information exchange about the work we are focusing on, I prefer that the DON CIO err on the side of caution and use social media applications that are protected by the DoD public key infrastructure. I am [also] looking at other ways to communicate more directly with the public. CHIPS

DON IT/Cyberspace Efficiency Initiatives and Realignment

By Lynda Pierce

The Under Secretary of the Navy, The Honorable Robert O. Work, signed a memo, dated Dec. 3, 2010, addressing information technology (IT)/cyberspace efficiency initiatives and realignment in the Department of the Navy. The memo underscores the challenge from Secretary of Defense (SECDEF) Robert Gates to think about the DON's approach to IT initiatives and to centralize and consolidate efforts where it makes sense. Mr. Work and Department of the Navy Secretary Ray Mabus view SECDEF's challenge as an opportunity to become efficient in the DON's IT procurement and business processes and to define a department strategy to shape the way forward in information management (IM), IT and cyberspace. The memo directs the DON Chief Information Officer to take the lead for the department for this endeavor, noting that it is a team effort and no one organization can do it alone.

The memo designates Mr. Terry A. Halvorsen, DON CIO, as the DON's IT/Cyberspace Efficiency Lead. It directs him to partner with several Secretariat level offices, the Chief of Naval Operations and Commandant of the Marine Corps to ensure the Department's IM, IT/cyberspace and Information Resources Management (IRM) goals are clearly articulated and met. The memo directs these offices to review their current processes and procedures to ensure their organizations are aware and actively included in all IM, IT/cyberspace and IRM activities. Additionally, to ensure a common, enterprise approach to IM, IT/cyberspace and IRM activities, the memo tasks the DON CIO to provide updates to the memos of August 2005 and November 2006 designating the DON Deputy Chief Information Officers.

Mr. Work writes that the IT/cyberspace efficiencies efforts must ensure operational integrity, maintain sufficient levels of defense-in-depth and fail-over capabilities, and be supportive of Department of Defense IT consolidation and efficiency efforts. They must also address the costs and risks associated with any proposed changes and be based on solid business case analysis. Mr. Halvorsen is tasked to collaborate with relevant DON IM, IT/cyberspace and IRM stakeholders to accomplish the following by the due dates noted:

- Create a process to become advocates and active participants in the development and review of the Services and DON's IM, IT/cyberspace and IRM portions of the annual Program Objective Memorandum (POM) build (Dec. 30, 2011).
- Charter and chair a DON IT policy/governance board to function as the Department's single senior governance forum in which IM, IT/cyberspace and IRM matters are reviewed and approved or disapproved (Jan. 14, 2011).
- Publish an overarching Naval Networking Environment (NNE) strategy document to which the governance, administration, operation, investment and acquisition of DON IM, IT/cyberspace and IRM resource assets will be predicated (Feb. 14, 2011).
- Identify opportunities for consolidation and centralization of IM, IT/cyberspace and IRM services, applications and operations across the Department (Feb. 28, 2011). Then submit an aggressive high-level Plan of Action & Milestones that spans the Future Year Defense Plan (FYDP) to migrate to cohesive, defendable and resilient DON enterprise solutions (Mar. 30, 2011).
- Develop, publish and implement a new Secretary of the Navy instruction to articulate roles, responsibilities and relationships of all key stakeholder entities within the IM, IT/cyberspace and IRM domains (May 1, 2011). CHIPS

– For the full text of the memo, go to: www.doncio.navy.mil/PolicyView.aspx?ID=2061.

Lynda Pierce is the DON CIO strategic communications team leader.

By Steve Muck

DON SSN REDUCTION PLAN

The Social Security number (SSN) has evolved beyond its intended purpose to become the identifier of choice for many of the business processes within the Department of the Navy. While use of the SSN has become the enabler to identify and authenticate individuals, it is one of the key elements used for identity theft and fraud. Widespread use of the SSN has reached unacceptable levels and requires a department-wide effort to eliminate or reduce the collection, use, display and storage of this sensitive data element.

The SSN reduction plan will consist of two phases. Phase One is currently in progress. Phase Two will be implemented when Department of Defense guidance has been released. Details are provided below.

PHASE ONE – CURRENTLY IN PROGRESS:

- Justify continued use and collection of SSNs in all official Navy and Marine Corps forms.
- Catalog all official DON forms using Naval Forms Online: https://navalforms.daps.dla.mil.
- Eliminate all unofficial forms in use; either stop using or validate for official use. DON forms management officers, consulting with the Privacy Official, draft justifications using Secretary of the Navy Forms Management Manual (SECNAV M-5213.1) of January 2010 for all forms that fall within their area of responsibility. This includes: DD/SD forms, component-wide forms, command forms and installation forms. All reviews must include:
  - » Copy of Privacy Act Statement;
  - » Copy of official form;
  - » Acceptable use (from list of 12). If you use "Other Cases," you must describe;
  - » Actions taken to truncate, hide or mask SSN;
  - » Statement regarding impact to business process if SSN were to be eliminated;
  - » Potential for SSN to be replaced with another unique identifier;
  - » Justify continued use and collection of SSNs in all information technology (IT) systems registered in the DoD Information Technology Portfolio Repository (DITPR)-DON;
  - » DON Chief Information Officer will submit changes to the program manager that mirror the forms review process in April 2011 to eliminate the need for a data call; and
  - » Data fields in DITPR-DON for IT systems with personally identifiable information (PII) must be verified for accuracy.

PHASE TWO – AWAITING DEPARTMENT OF DEFENSE GUIDANCE:

- Where continued use of SSNs is required, substitute another unique identifier for the SSN.

CHALLENGES:

- Without controls in place, the substitute for the SSN could become sensitive PII.
- Despite the current SSN Reduction Plan, human error will still result in the loss and compromise of the SSN.
- The DON does not control many of the forms requiring use of the SSN.
- Elimination of the SSN or substituting the SSN for another identifier will incur unfunded program costs especially with IT systems. CHIPS

By Steve Muck

THE NUMBERS GAME

MORE THAN 420 MILLION SSNs HAVE BEEN ISSUED

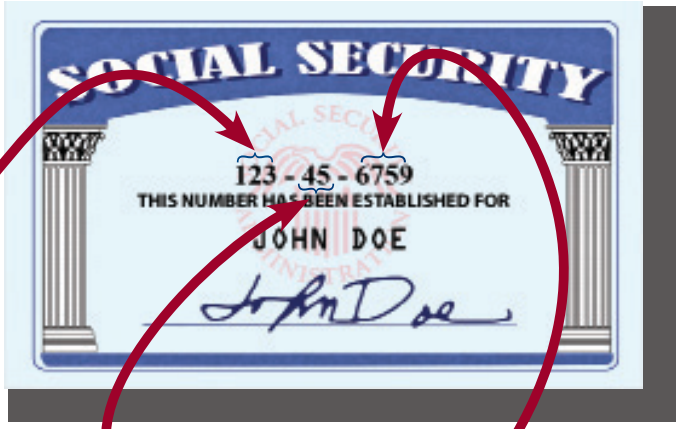
THE SSN IS NOT REASSIGNED AFTER THE NUMBER HOLDER'S DEATH

THE CURRENT NUMBERING SYSTEM WILL PROVIDE ENOUGH NEW NUMBERS FOR SEVERAL FUTURE GENERATIONS

APPROXIMATELY 5.5 MILLION NEW NUMBERS ARE ASSIGNED EACH YEAR

The nine-digit Social Security number has been used since 1936 to track a person's wages for the purpose of accruing benefits within the Social Security Administration. Since it's inception, the SSN has become the unique identifier for a wide range of business processes. For example, the SSN is required for parents to claim their children as dependents for federal income tax purposes; the Internal Revenue Service requires all employers to obtain SSNs (or alternative identifying numbers) from their employees; the Navy and Marine Corps use the SSN on all military ID cards; and the SSN is used to access a variety of information technology system applications. CHIPS

THE SSN IS COMPOSED OF THREE SECTIONS



1 The first three digits of the SSN are called area numbers. This is because they originally corresponded to the state that a person lived in at the time he or she was issued a SSN. Beginning in 1972, area numbers were assigned based upon the zip code in the mailing address to which the individual requested his or her card be sent. In 2011, the geographical significance of the first three digits of the SSN will be eliminated.

2 Digits four and five in the SSN are referred to as group numbers. They are used to identify the block of numbers currently issued. As an example, the SSNs 123-01-0001 through 123-01-9999 would be issued before moving to the next group numbers.

3 Digits six through nine are known as serial numbers. They are issued consecutively from 0001 to 9999.

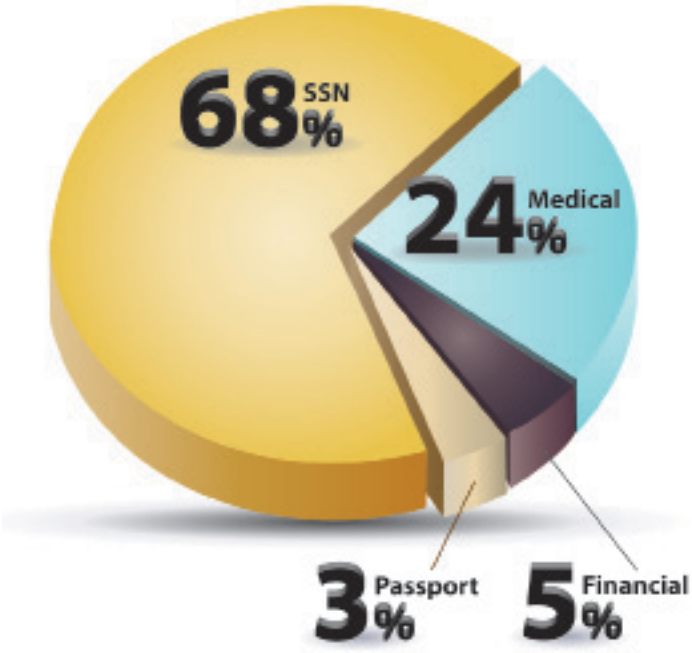
By Steve Muck

TO ERR IS HUMAN

Human error is the cause of 80 percent of the DON's PII breaches. Not knowing or not following guidance, or just being careless can result in the unintended disclosure of privacy sensitive information and potentially adversely affect many personnel.

The Social Security number is the most frequently lost, stolen, or compromised PII data element. The SSN is involved in almost 70 percent of DON breaches. This sensitive identifier must be closely safeguarded or eliminated from use. SSNs are improperly disclosed by: sending SSNs in an e-mail or in attachments, creating recall rosters with SSNs, or posting names with associated SSNs to Web portals or shared drives.

In these examples, SSNs were either transmitted without encryption, not properly marked, or sent to recipients that did not have a need to know.



TYPES OF PII LOST, STOLEN, OR COMPROMISED

PII BREACH CAUSES

DOD DIRECTIVE 5400.11 DEFINITIONS

5400.11 Para E2.2: Personally Identifiable Information (PII)

Personal Information. "Information about an individual that identifies, links, relates, or is unique to, or describes him or her (e.g., a Social Security number; age; military rank; civilian grade; marital status; race; salary; home or office phone numbers; other demographic, biometric, personnel, medical, and financial information, etc.). Such information also is known as personally identifiable information (e.g., information which can be used to distinguish or trace an individual's identity, such as his or her name; Social Security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information which is linked or linkable to a specified individual.)"

5400.11-R: PII Breach

"Actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for an other than authorized purposes where one or more individuals will be adversely affected." CHIPS

COMPILED FROM INFORMATION SUPPLIED BY THE FEDERAL TRADE COMMISSION
WWW.FTC.GOV/BCP/EDU/MICROSITES/IDTHEFT

Compiled By Steve Muck

FACTS ABOUT IDENTITY THEFT

How do thieves steal an identity? Identity theft starts with the misuse of an individual's personally identifiable information (PII), such as name and Social Security number (SSN), date of birth, mother's maiden name, credit card numbers or other financial account information. For identity thieves, this information is as good as gold.

Skilled Identity Thieves May Use a Variety of Methods to Obtain Personal Information, including:

- Dumpster Diving: They rummage through trash looking for bills or paper with personal information on it.
- Skimming: They steal credit/debit card numbers by using a special storage device when processing a card.
- Phishing: They pretend to represent financial institutions or companies and send spam or pop-up messages to trick people into revealing their personal information.
- Changing Addresses: They divert billing statements to another location by completing a change of address form.
- Old-Fashioned Stealing: They steal wallets and purses; mail, including bank and credit card statements; pre-approved credit card or loan offers; and new checks or tax information. They steal personnel records or bribe employees who have access to PII. CHIPS

USEFUL IDENTITY THEFT INFORMATION:

- The Federal Trade Commission (FTC) reports that approximately 3.6 percent of the U.S. adult population has experienced identity theft. Identity theft of children and the deceased are on the rise. Additionally, medical identity theft is a growing concern.
- The most common forms of identity theft are the fraudulent use of PII to open a new line of credit and the use of credit/debit card account numbers to make purchases.
- The full SSN, linked to a name, is a key element to committing identity theft.
- Crimes occur more often offline than online.
- A significant amount of PII, including Social Security numbers, can be found in public records.
- Risk is greatest when information is stolen by someone targeting the data, e.g., by a hacker or a burglar.
- Most victims find out about identity theft through an adverse action such as a creditor demanding payment on a delinquent bill.
- Half of known identity thieves are known by their victims; one-fourth are dishonest employees.
- The President's Identity Theft Task Force recommended that federal agencies reduce the unnecessary use of Social Security numbers, which it calls "the most valuable commodity for an identity thief."
- Phishing attacks aimed at identity theft affect one in four individuals per month.
- Two-thirds of attacks appear to be from legitimate companies.
- Consumer credit card liability is $50.
- Consumer debit card liability is $50 if reported within 48 hours, $500 if reported within 60 days. After 60 days the victim may lose all the money in the account — in addition to the overdraft amount.
- The Identity Theft Enforcement and Restitution Act of 2008 makes it easier to prosecute thieves and compensate victims for time and trouble.

WHAT DO THIEVES DO WITH A STOLEN IDENTITY?

Once they have your personal information, identity thieves use it in a variety of ways.

Credit Card Fraud:

- They may open new credit card accounts in their victim's name. When they use the cards and do not pay the bills, the delinquent accounts appear on their victim's credit report.
- They may change the billing address for a credit card so that the victim no longer receives bills, and then run up charges on the account. It may be some time before the victim realizes there is a problem because the bills are sent to a different address.

Bank/Finance Fraud:

- They may create counterfeit checks using their victim's name or account number.
- They may open a bank account in their victim's name and write bad checks.
- They may clone their victim's ATM or debit card and make electronic withdrawals in their victim's name, draining the accounts.
- They may take out a loan in their victim's name.

Government Documents Fraud:

- They may obtain a driver's license or other government-issued ID card in the victim's name but with their photo.
- They may use their victim's name and SSN to get government benefits.
- They may file a fraudulent tax return using their victim's information.

Other Fraud:

- They may get a job using their victim's SSN.
- They may rent a house or get medical services using their victim's name.
- They may give their victim's personal information to police during an arrest. If they do not appear for the court date, a warrant for arrest is issued in their victim's name.

Phone or Utilities Fraud:

- They may open a new phone or wireless account in their victim's name or run up charges on an existing account.
- They may use their victim's name to get utility services, like electricity, heating or cable television.

Compiled by Steve Muck

GUARD AGAINST IDENTITY THEFT

The Department of Justice provides information about how to prevent identity theft, as well as what to do if you become a victim of identity theft. The information below summarizes these preventive measures and actions. Additional information can be found at www.justice.gov.

What Can I Do About Identity Theft and Fraud?

To victims of identity theft and fraud, the task of correcting erroneous information about their financial or personal status, and trying to restore their good credit standing and reputations, may seem as daunting as trying to solve a puzzle in which some of the pieces are missing and other pieces no longer fit as they once did. Unfortunately, the damage that criminals inflict in stealing another person's identity to commit fraud often takes far longer to rectify than it took the criminal to commit the crimes.

What Should I Do to Avoid Becoming a Victim of Identity Theft?

To reduce or mitigate the risk of becoming a victim of identity theft or fraud, there are some basic steps to take.

First, be cautious about giving your personal information to others unless you have a very good reason to trust them, regardless of where you are.

When You're at Home

Start by adopting a "need to know" approach to safeguarding your personal data. Your credit card company may need to know your mother's maiden name, so that it can verify your identity, but be suspicious of a phone call from your bank asking for personal information that is already on file with your bank. The only purpose of such a call is to acquire your personal information for identity fraud. Another consideration is to be careful with the information you have printed on your bank checks, such as your Social Security number or home telephone number; you may be routinely sharing your personal information needlessly.

If someone you don't know phones and offers you the chance to receive a "premium" credit card, prize or other valuable item, but asks for personal data, such as your Social Security number, credit card number and expiration date, or mother's maiden name, ask for an application form by mail. If they decline, terminate the call. If you do receive an application, carefully review the information and make sure it is from a company or financial institution that's well-known and reputable. Contact the Better Business Bureau for additional information if you are not familiar with the company or financial institution making the offer.

Check your bank statements and other financial information regularly to ensure that the data is correct.

If you are not receiving monthly financial statements for your accounts, call the financial institution or credit card company immediately and ask for your statement. If you are told that your statements are being mailed to another address that you have not authorized, tell the financial institution or credit card representative immediately that you did not authorize the change of address and that someone may be improperly using your accounts. In this situation, you should also ask for copies of all statements and debit or charge transactions that have occurred since the last statement you received. Obtaining those copies will help you to work with the financial institution or credit card company in determining whether transactions were fraudulently conducted.

Ask periodically for a copy of your credit report. It should list all bank and financial accounts under your name and will provide other indications of whether someone has wrongfully opened or used any accounts in your name. See the information on the next page to contact one of the major credit reporting agencies to order a report.

Maintain careful records of your banking and financial accounts. Even though financial institutions are required to maintain copies of your checks, debit transactions and similar transactions for five years, you should retain your monthly statements and checks for at least one year, if not more. If you need to dispute a check or transaction, especially if they purport to bear your signatures, your original records will be more immediately accessible and useful to the institutions that you have contacted for resolution of a disputed charge.

While You're on Travel

When traveling, never place your government or personal laptop into your checked baggage. Thieves commonly target checked luggage and may benefit from accessible per-

sonally identifiable information (PII), as well as the monetary value of the devices.

Put your mail on hold with your local post office or ask someone you know well and trust, such as a family member, friend or neighbor, to collect and hold your mail while you are away.

If you must share PII over the phone, do not do it in a public area where passers-by may hear your conversation. Similarly, protect data transmissions from laptops and cell phones using only secure Wi-Fi connections.

What Should I Do If I've Become A Victim Of Identity Theft?

If you think you have become a victim of identity theft or fraud, act immediately to minimize the damage. Contact the **Federal Trade Commission (FTC)** to report the theft: www.ftc.gov; 1-877-ID THEFT (1-877-438-4338); TTY: 1-866-653-4261; or by mail to Identity Theft Clearinghouse, FTC, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580.

Per the Identity Theft and Assumption Deterrence Act, the FTC is responsible for receiving and processing identity theft complaints, providing informational materials, and referring complaints to the appropriate entities, including the major credit reporting agencies and law enforcement agencies. For further information, check the FTC's identity theft Web pages. You may also call your local FBI office or the U.S. Secret Service to report crimes relating to identity theft and fraud. If you believe your information was stolen or compromised from a Department of the Navy activity, contact your chain of command so the Naval Criminal Investigative Service (NCIS) can be alerted if criminal intent is suspected.

You may also need to contact other agencies for other types of identity theft:

- Your local office of the **Postal Inspection Service** if you suspect that an identity thief has submitted a change of address form with the Post Office to redirect your mail or has used the mail to commit frauds involving your identity.
- The **Social Security Administration** if you suspect that your Social Security number is being fraudulently used. Call 1-800-269-0271 to report the fraud.
- The **Internal Revenue Service** if you suspect the improper use of identification information in connection with tax violations. Call 1-800-829-0433 to report the violations.

Report the Theft to the Fraud Units of the Three Principal Credit Reporting Companies:

- **Equifax**: Phone 1-800-525-6285 or write to P.O. Box 740250, Atlanta, GA 30374-0250. To order a copy of your credit report ($8 in most states), write to P.O. Box 740241, Atlanta, GA 30374-0241, or call 1-800-685-1111. To dispute information in your report, call the phone number provided on your credit report. To opt out of pre-approved offers of credit, call 1-888-567-8688 or write to Equifax Options, P.O. Box 740123, Atlanta, GA 30374-0123.
- **Experian** (formerly TRW): Phone 1-888-EXPERIAN or 1-888-397-3742, fax to 1-800-301-7196, or write to P.O. Box 1017, Allen, TX 75013. To order a copy of your credit report ($8 in most states) write to P.O. Box 2104, Allen, TX 75013 or call 1-888-EXPERIAN. To dispute information in your report, call the phone number provided on your credit report. To opt out of pre-approved offers of credit and marketing lists, call 1-800-353-0809 or 1-888-5OPTOUT or write to P.O. Box 919, Allen, TX 75013.
- **TransUnion:** Phone 1-800-680-7289 or write to P.O. Box 6790, Fullerton, CA 92634. To order a copy of your credit report ($8 in most states), write to P.O. Box 390, Springfield, PA 19064 or call 1-800-888-4213. To dispute information in your report, call the phone number provided on your credit report. To opt out of pre-approved offers of credit and marketing lists, call 1-800-680-7293 or 1-888-5OPTOUT or write to P.O Box 97328, Jackson, MS 39238.

Other Places to Report the Theft:

Contact all creditors with whom your name or identifying data has been fraudulently used. For example, you may need to contact your long-distance telephone company if your long-distance calling card has been stolen or you find fraudulent charges on your bill.

Contact all the financial institutions where you have accounts to report that an identity thief has fraudulently created accounts in your name but without your knowledge. You may need to cancel the accounts, place stop-payment orders on any outstanding checks that may not have cleared, and change your automated teller machine card, account and personal identification numbers.

Contact the major check verification companies (listed below) if you have had checks stolen or bank accounts set up by an identity thief. If you know that a particular merchant has received a check stolen from you, contact the verification company that the merchant uses. CHIPS

- **CheckRite** 1-800-766-2748
- **ChexSystems** 1-800-428-9623
- **CrossCheck** 1-800-552-1900
- **Equifax** 1-800-437-5120
- **SCAN** 1-800-262-7771
- **TeleCheck** 1-800-710-9898
- **NPC** 1-800-526-5380

Compiled by Steve Muck

UNIQUE DOD ID REPLACES SSN

A memo from the Under Secretary of Defense issued Nov. 23, 2010, (DTM 13798-10, "Social Security Numbers (SSN) Exposed on Public Facing and Open Government Websites"), addresses concerns about the potential for adverse consequences if the Social Security number (SSN) is truncated or removed as previously planned.

Primary concerns are the potential impacts to existing business practices associated with the identification of Defense Department personnel overseas, especially in theater, as well as the administration of TRICARE benefits for DoD beneficiaries. Both of these mission critical business practices rely heavily on the presence of a visual, numeric identifier on ID cards.

The updated plan includes the use of two alternative identifiers, the DoD identification number and the DoD benefits number, which will help support the broadest array of business practices while still reducing the department's reliance on the SSN. When the new plan is fully implemented, all individuals with a direct relationship to DoD will use a new identifier called the Electronic Data Interchange-Person Identifier (EDI-PI), hereafter referred to as the DoD identification (ID) number, to be printed on all DoD ID cards. All individuals eligible to receive DoD benefits, such as commissary; exchange; and morale, welfare and recreation, or TRICARE purchased care, will receive a DoD benefits number in addition to the DoD ID number. CHIPS

THE TIMELINE FOR THIS PLAN TO REMOVE SSNs FROM DOD ID CARDS IS AS FOLLOWS:

2008 – 2012
Removal of printed family member SSNs from all family member ID cards.

2010
Begin replacing the SSN with the DoD Identifier and DoD Benefits Number.

2012
Begin removal of the SSN from barcodes.

By Steve Muck

DONCAF REDUCES SSN USE

The Department of the Navy Central Adjudication Facility (DONCAF), a Naval Criminal Investigative Service (NCIS) organization, is responsible for determining who within the Department of the Navy is eligible to hold a security clearance, have access to Sensitive Compartmented Information (SCI), and be assigned to sensitive duties.

DON personnel consist of active duty and Reserve components of the United States Navy and Marine Corps, as well as civilians and contractors. DONCAF makes SCI eligibility determinations for select contractor personnel.

DONCAF also maintains an extensive database of its security decisions and provides overall operational support to the Navy's personnel security program.

Adjudication is the review and consideration of all available information to ensure an individual's loyalty, reliability and trustworthiness are such that entrusting an individual with national security information or assigning an individual to sensitive duties is clearly in the best interest of national security. DONCAF's mission is to provide excellent customer service, and accurate and timely adjudication. DONCAF implements innovative strategies for the DON Personnel Security Program.

A recent breach of personally identifiable information resulted when an adjudication package containing an individual's PII was lost in the mail. Considering the amount of PII that is commonly found in these packages, the DONCAF organization reviewed its procedures and came up with a new policy which either eliminates the Social Security number from correspondence or greatly mitigates the risk of a breach of PII by using only the last four digits of the SSN. The DONCAF policy is shown at right. CHIPS

1. Effective immediately, this applies to everyone and supersedes any previously disseminated guidance. In accordance with the Under Secretary of Defense memorandum of March 28, 2008, "DoD Social Security Number (SSN) Reduction Plan": "Due to recent Privacy Act concerns and potential compromises, a subject's full Social Security number (SSN) will not be included on any correspondence, including shell letters and forms. Only the last four digits of the subject's SSN will be included in all outgoing correspondence. Whenever feasible, the subject's case identification number will be used as the subject identifier for internal correspondence."
2. The following format for all external correspondence should be used: XXX-XX-1234.
3. All current shell and form letter variables have been updated to accommodate this change.
4. These changes are approved by Director, DONCAF and will be incorporated throughout the next revision of the SOP (standard operating procedure).

By Jim Hoskins

COMBATING IDENTITY THEFT

Marine Corps Base Camp Pendleton, located in Southern California, is the largest Marine Corps installation on the West Coast. Camp Pendleton has an active duty military population of more than 46,000 inhabitants and a daytime population of more than 70,000, which includes the 1,150 Marines, 3,500 civilian Marines and supporting government contractors employed to accomplish its assigned mission.

To comply with Department of Defense (DoD) and Department of the Navy (DON) policies, Camp Pendleton began the revitalization of its privacy program in 2008. Using such references as Directive-Type Memorandum 07-15-USD (P&R), DoD Social Security Number (SSN) Reduction Plan; DoD Directive 5400.11, DoD Privacy Program; Combating Identify Theft: A Strategic Plan from the President's Identity Theft Task Force; and other guidance issued by the DON and Headquarters Marine Corps, Camp Pendleton began its efforts to reduce the usage of Social Security numbers for identification by consolidating reference materials, analyzing current procedures and identifying key stakeholders.

The consolidation and validation process was not an easy task during the 2008 and early 2009 time period. Some of the contributing factors making the process difficult were: changing requirements, lack of a primary reference, compliance ownership, and personnel availability and/or opportunities for training and idea sharing which were further constrained by budget limitations. Additionally, the use of the Social Security number for identification was and still is ubiquitous. Too many of our processes, many that are beyond Marine Corps control, rely on the use of the SSN. But by 2009, dramatic, positive change began in Camp Pendleton's privacy program.

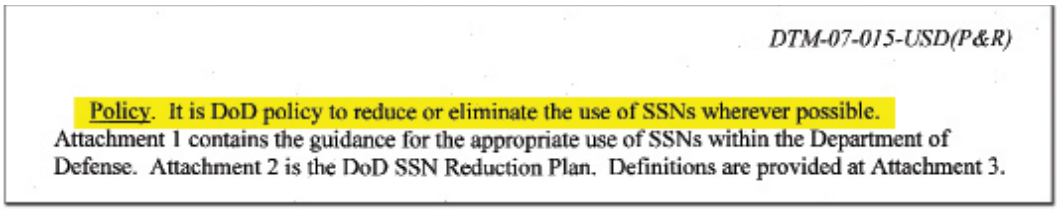
The tipping point was the issuance of the Marine Corps Enterprise Information Assurance Directive (EIAD) 011, Personally Identifiable Information (PII), of April 9, 2009. This document consolidated various directives into a single source reference and detailed requirements. EIAD 011 outlined cross-functional (Privacy Act and information technology) action items and melded together requirements from previously bifurcated functions.

Implementation of EIAD 011 laid the foundation of a manageable Privacy Act Program that includes the requirements of both electronic and manual systems of records. Action taken for Phase One of the DON's SSN Reduction Plan was an easy fit into the oversight structure developed as a result of EIAD 011. A good fit for action officers, compliance for Phase One was substantial.

The following actions were completed as a result of Phase One.

- All locally generated forms for Camp Pendleton were thoroughly reviewed.
- SSN use was validated, eliminated when possible, or justified for continued use.
- Privacy Act statements and systems of record numbers were assigned to each form where required.

- Purchased and distributed the DON PII training class on compact disc and distributed CDs to all special staff sections for internal training.
- Local form numbers and local stock numbers were assigned to each form.
- Forms not submitted for review and approval were no longer authorized.
- Electronic versions of all forms were entered into the Marine Corps forms processes link.
- Of 200 local forms, only 17 required the continued use of the SSN. This number will be further reduced when a substitute unique identifier is authorized for DON use.
- A PII training class based on the required annual PII training syllabus was developed. This class is given quarterly at the base theater and is open to anyone on the base who does not have access to online training.
- Developed and instituted self-inspections for PII compliance.
- Field assist visits are offered and occur on a regular basis. Best practices are discussed and shared.



DTM-07-015-USD(P&R)

Policy. It is DoD policy to reduce or eliminate the use of SSNs wherever possible. Attachment 1 contains the guidance for the appropriate use of SSNs within the Department of Defense. Attachment 2 is the DoD SSN Reduction Plan. Definitions are provided at Attachment 3.

Camp Pendleton's privacy program significantly reduces the risk of loss or compromise of warfighters' personal information by eliminating, masking or truncating the SSN wherever possible. Reducing exposure of this sensitive privacy element reduces the likelihood that the Marines and civilian workforce will fall victim to identity theft.

Even though Camp Pendleton has a revitalized Privacy Act Program, there is always the risk of compromise or loss. The best case scenario is to mitigate that risk to the extent possible. The following suggestions may further enhance efficiencies and mitigation.

- Mandate that Privacy Act responsibilities are a primary duty for assigned personnel. Currently, Privacy Act duties are collateral duties at the major command level.
- Require professional training prior to assignment of Privacy Act duties and semiannual refresher training thereafter. Currently, training is not required and learning occurs on the job.
- Establish one agency office with responsibility for compliance with all phases of the Privacy Act. Currently, several offices may be issuing directives that have an impact on the Privacy Act Program.
- Establish a venue for privacy professionals to meet semiannually and discuss best practices, challenges and accomplishments.

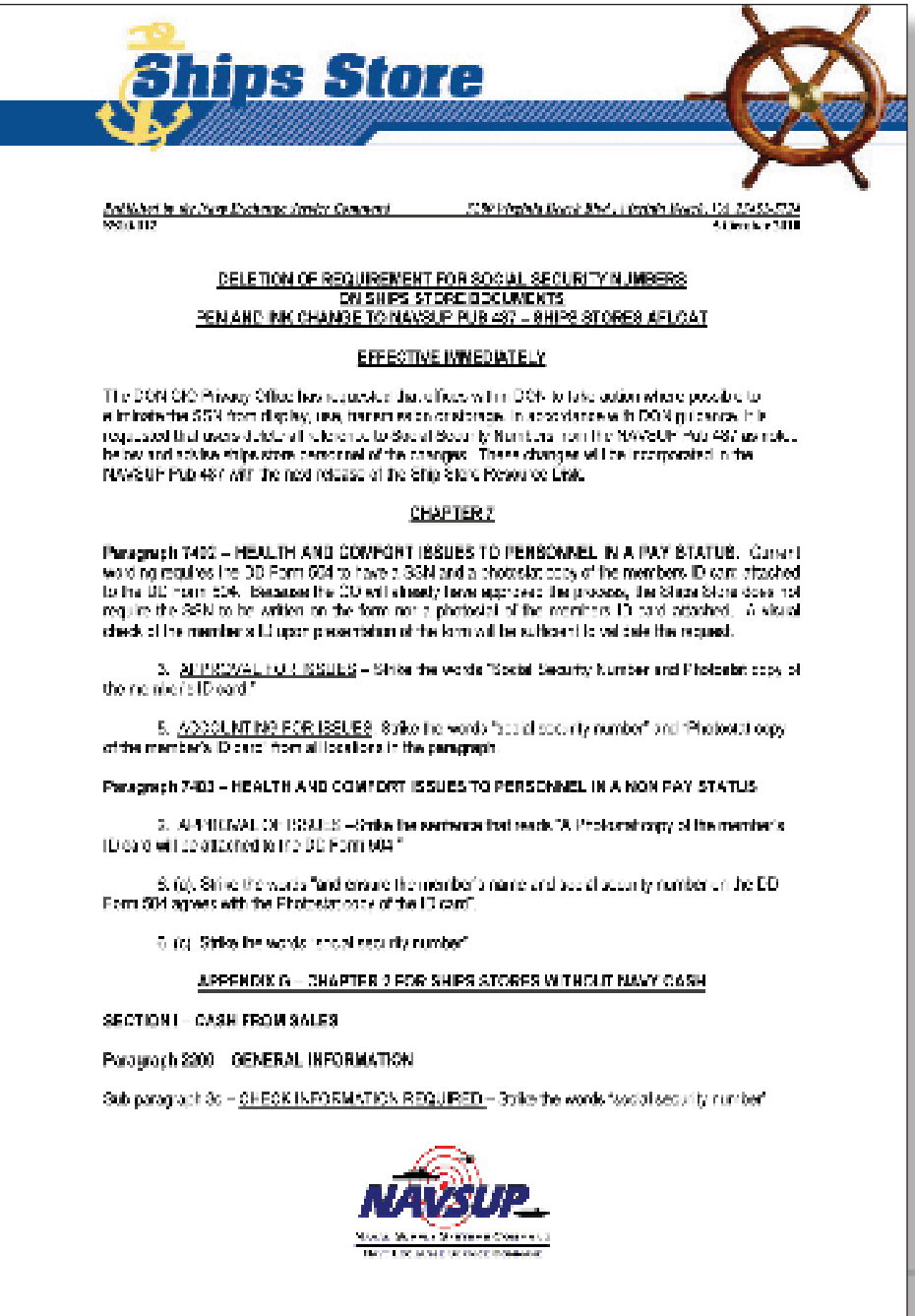
Camp Pendleton is very proud of the collaborative efforts of its team members and looks forward to the continual improvement of its privacy processes. CHIPS

Jim Hoskins is the MCB Camp Pendleton adjutant.

By Charles H. Vaughan

COMPLAINT LEADS TO POLICY CHANGE

The Navy Exchange Service Command Ships Store Program, a Naval Supply Systems Command organization, is responsible for oversight of the Navy's Ships Stores.



Ships Store

DELETION OF REQUIREMENT FOR SOCIAL SECURITY NUMBERS
ON SHIPS STORE DOCUMENTS
PEN AND INK CHANGE TO NAVSUP PUB 487 – SHIPS STORES AFLOAT

EFFECTIVE IMMEDIATELY

The DON CIO Privacy Office has mandated that effective from 2004 to take action where possible to eliminate the SSN from display, use, transmission or maintenance. In accordance with DON guidance it is required that words pertaining to Social Security Numbers from the NAVSUP Pub 487 are stricken below and notice ships store personnel of the changes. These changes will be incorporated in the NAVSUP Pub 487 ARF the next release of the Ship Store Program Desk Guide.

CHAPTER 7

Paragraph 7402 – HEALTH AND COMFORT ISSUES TO PERSONNEL IN A PAY STATUS. Current wording requires the DD Form 504 to have a SSN and a photostat copy of the members ID card attached to the DD Form 504. Because the CO will already have approved the process, the Ships Store does not require the SSN to be written on the form nor a photostat of the members ID card attached. A visual check of the member's ID upon presentation of the form will be sufficient to validate the request.

3. APPROVAL OF ISSUES – Strike the words "Social Security Number and Photostat copy of the member's ID card."

5. ACCOUNTING FOR ISSUES. Strike the words "social security number" and "Photostat copy of the member's ID card" from all locations in the paragraph.

Paragraph 7403 – HEALTH AND COMFORT ISSUES TO PERSONNEL IN A NON PAY STATUS

3. APPROVAL OF ISSUES – Strike the sentence that reads "A Photostat copy of the member's ID card will be attached to the DD Form 504."

5. (c). Strike the words "and ensure the member's name and social security number on the DD Form 504 agrees with the Photostat copy of the ID card".

7. (c). Strike the words "social security number"

APPENDIX G – CHAPTER 3 FOR SHIPS STORES WITHOUT NAVY CASH

SECTION I – CASH FROM SALES

Paragraph 3000 – GENERAL INFORMATION

Sub paragraph 3c – CHECK INFORMATION REQUIRED – Strike the words "social security number"

NAVSUP

The program is expeditionary, sea-based and provides essential quality of life services to Sailors and Marines serving on fleet ships around the world. Since Congress authorized the Ships Store operation in 1909, the program has taken care of Sailors and Marines whenever they are called to sea. The tempo of fleet operations remains high, and the Ships Store goes where our customers go. More than 50 percent of Navy ships are at sea and approximately 30 percent are forward deployed. The Ships Store program provides retail stores, vending machines, barbershops and laundry facilities to make seagoing life better.

Ships Stores are operated using appropriated funds and generate dividends to support shipboard morale, welfare and recreation (MWR) programs that are vital to enhancing the well-being and readiness of Sailors at sea. The afloat telecommunications program, which provides that vital underway phone link home for deployed Sailors and Marines, continues to be one of the biggest shipboard morale boosters.

A recent question sent to the Department of the Navy Chief Information Officer (DON CIO) Privacy Office via its website addressed a concern from a chief petty officer about the requirement for writing his full Social Security number on the back of a personal check for payment in a ships store. His question led to a major policy change within the Ships Store Program. Since the CPO did not have a Navy Cash debit card established, he wrote a personal check. To respond to the chief, the DON CIO Privacy Office contacted the Vice President of Afloat Operations/Ships Store Program and received immediate and positive results.

The old Ships Store Program policy required that service members writing a check for ships store merchandise include their SSN on the back of the check. Additionally, the old policy required personnel who receive health and comfort items while in a non-pay status to write their SSN on their Request and Receipt for Health and Comfort Supplies, DD Form 504.

The new policy, effective Nov. 1, 2010, eliminates the requirement to place the SSN on the DD Form 504 and the requirement to have SSNs on personal checks. By the end of 2010, guidance will be published which will eliminate all policy requirements by the Ships Store Program to require a SSN for identification. CHIPS

By Lani Gordon

TAKE NO PRISONERS

SPAWAR safeguards SSNs through decisive action and strict controls on SSN use.

The White House's Office of Management and Budget Memorandum (M-07-16), issued May 22, 2007, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," required that Executive Department officials safeguard personally identifiable information, also known as PII, maintained by the government and prevent its breach to ensure the government retains the trust of the American public. The term "PII" refers to information which can be used to distinguish or trace individuals' identity, such as their Social Security number (SSN).

The Space and Naval Warfare Systems Command (SPAWAR) takes this responsibility seriously. In recent months, SPAWAR has successfully contained two separate breach incidents involving loss of control, unauthorized disclosure, and unauthorized acquisition of documents containing SSNs.

SPAWAR prevented spillage of the SSNs through prompt investigation, thoughtful analysis, required reporting and coordinated action. These incidents prompted SPAWAR to conduct command training for safeguarding PII and eliminating the unnecessary collection and use of SSNs. A summary of the two incidents follows.

1 The first incident involved an electronic breach regarding the Personalized Recruiting for Immediate and Delayed Enlistment (PRIDE) electronic information system. A contractor employee sent an e-mail with an Excel spreadsheet attachment containing full SSNs to recipients. It was real data taken from the PRIDE recruit master repository to be used for testing. The e-mail and the Excel spreadsheet were sent unencrypted. Each recipient had a need to know some of the information but not all of the information. Further, the attachment containing PII did not have the proper privacy marking.

LESSONS LEARNED

Before sending an e-mail that contains PII, ask: Do the recipient(s) have a need to know all of the information? Are the means of transmission secure? Is it essential to include the SSN or could it be eliminated?

Other preventive actions include:

- Establish procedures for proper maintenance, storage and dissemination of the PRIDE recruit master repository;
- Provide PII training to ensure civilian, military and contractor personnel follow established procedures;
- Limit PII elements to individual organizations. Send only the information that is necessary to perform the required tasks;
- Establish strict controls so that only those personnel with a need to know have access to files containing SSNs;
- Ensure procedures are in place so that all electronic or hard copy documents and attachments containing PII are marked: FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE: Any misuse or unauthorized disclosure of this information may result in both criminal and civil penalties;
- Ensure that compliance spot checks include data collections, surveys and spreadsheets; and
- Foster compliance of Secretary of the Navy Instruction (SECNAVINST) 5211.5E, "Department of the Navy (DON) Privacy Program."

2 The second incident involved a breach concerning a key SPAWAR satellite program. An employee of a prime contractor in support of the program inadvertently posted paper copies of access lists, which displayed full names and full SSNs, near the entrances of two secured areas at the contractor's facility. A requirement to include the SSN on the access lists did not exist. Internal security procedures were not followed.

LESSONS LEARNED

Before posting access lists that display SSNs ask: Who are the recipients of this information? What is the need to post an individual's SSN to verify access? Can the requirement for including the SSN be eliminated?

Other preventive actions include:

- Establish procedures for proper maintenance, storage and dissemination of access lists;
- Ensure security basics are understood through training;
- Review the feasibility of eliminating the SSN on access lists;
- Limit PII elements on access lists;
- Ensure that compliance spot checks include access lists; and
- Foster compliance of SECNAVINST 5211.5E.

In conclusion, SPAWAR works diligently to safeguard personally identifiable information and eliminates the collection and use of the SSN when it is not required to accomplish its mission. CHIPS

By Barbara Figueroa

BUPERS REDUCES SSN USE

The Department of the Navy (DON) is currently involved in a top-down approach to eliminate the unnecessary collection of Social Security numbers (SSNs).

Official DON forms, sponsored by all echelons, have been identified as a leading source of SSN collection and were a good starting point to review and either justify continued SSN use or eliminate its unnecessary use. The goal of this effort is to greatly reduce the collection, display, storage and/or transmission of SSNs where possible.

A formal review process was created in response to Directive-Type Memorandum (DTM) 07-015-USD(P&R) of March 28, 2008, "DoD Social Security Number Reduction Plan" and DON CIO MSG DTG: 192101Z of July 2010, "DON Social Security Number Reduction Plan for Forms Phase One."

In collaboration with the Privacy Act Program Manager (DNS-36), the DON Forms Manager (DNS-51) and all Navy echelon forms managers, significant progress continues to be made to reduce the use of the SSN across the Navy and Secretariat. The Marine Corps has implemented a similar review process to make this a DON-wide initiative.

Like many of the commands that conducted the DON SSN Reduction Plan for Forms Phase One, the Bureau of Naval Personnel (BUPERS-01F) dramatically decreased the requirement to collect the SSN on many Navy Personnel Command/Bureau of Naval Personnel forms. Because so many of their processes involve the collection of privacy sensitive data, BUPERS is a great example of how an aggressive review process can work across the DON.

During the recent review and justification process, 146 forms were identified that collect the SSN. From that group, the SSN field was eliminated on 48 forms, 40 forms were canceled, and 58 received justifications for continued SSN use. The results of the BUPERS-01F review have been consistent with other Navy and Marine Corps components. CHIPS

Articles written and compiled by the following

CONTRIBUTORS

Barbara Figueroa
Director, Navy Staff 51
CNO, SECNAV & Navy Forms Mgr.

Lani Gordon
SPAWAR
Associate Counsel

Jim Hoskins
MCB Camp Pendleton
Adjutant

Steve Muck
DON CIO
Privacy Lead

Charles H. Vaughan
Navy Exchange Service Command
V.P. Afloat Operations/
Ships Store Program

From stovepiped silos to NMCI, the Department of the Navy's integrated enterprise network

NMCI transitions to NGEN by 2014

By Michelle Ku

The Navy Marine Corps Intranet (NMCI) began as a revolutionary idea more than 10 years ago when the question was posed: What if the Department of the Navy (DON) consolidated all of its disparate information technology (IT) networks into one secure, fully functional enterprise network on a single technological platform with standardized hardware and software and integrated voice, video and data communications?

The idea further evolved into one of the most ambitious and transformational contracting initiatives ever undertaken when the DON competitively sourced a single industry partner to build, manage and maintain an entire intranet infrastructure, as well as software maintenance and deployment, and all at a lower cost than managing an enterprise network in-house.

Today, that network built by Hewlett-Packard (HP) Enterprise Services, formerly Electronic Data Systems, is the largest corporate intranet in the world with more than 700,000 users utilizing 384,000 workstations. The NMCI is second in size only to the Internet itself!

After 10 years of overseeing the NMCI, the DON is poised to take the next step — transitioning the innovative NMCI to the Next Generation Enterprise Network (NGEN) with full government ownership, including increased management and control.

The start of the transition began Oct. 1, 2010, when the NMCI Continuity of Services Contract (CoSC) took effect. Over the next four years, NMCI CoSC — the follow-on contract to the NMCI contract that ended Sept. 30 — will enable the DON to purchase the infrastructure, assets and the rights to use the intellectual property of the NMCI while increasing command and control (C2) of the network.

As the DON assumes enhanced visibility into the network, the NMCI will transition to NGEN, which will be acquired in a segmented approach allowing for the possibility of multiple vendors. The NMCI has been operated by a single prime contractor since it was stood up in 2000. During this fiscal year, Requests for Proposals (RFPs) for several NGEN segments will be issued to support migration of the first seats to NGEN in FY 2012; the full transition will be completed by 2014.

"NMCI was a hugely successful program for the DON in consolidating disparate, stove-piped networks into a single, modern, cost-effective enterprise network with a high level of service that meets mission critical needs," said Capt. Scott N. Weller, NMCI program manager.

With the end of the 10-year NMCI contract, the DON decided to change the way the network operates, Weller said. "For NMCI, the DON chose to have the prime vendor supply the infrastructure; under NMCI CoSC, we want the ability to purchase it. The NMCI CoSC vehicle provides the ability to transition pieces of NMCI services to multiple contracts, instead of a single contract."

The NMCI CoSC will enable the transition to NGEN, the next step in the evolution of the DON's secure, net-centric enterprise network. This strategy is illustrated in Figure 1. NGEN will continue the capabilities that are currently available in the NMCI while providing an increased level of government control, thus maintaining information security and remaining within budget.

The NGEN Acquisition Strategy

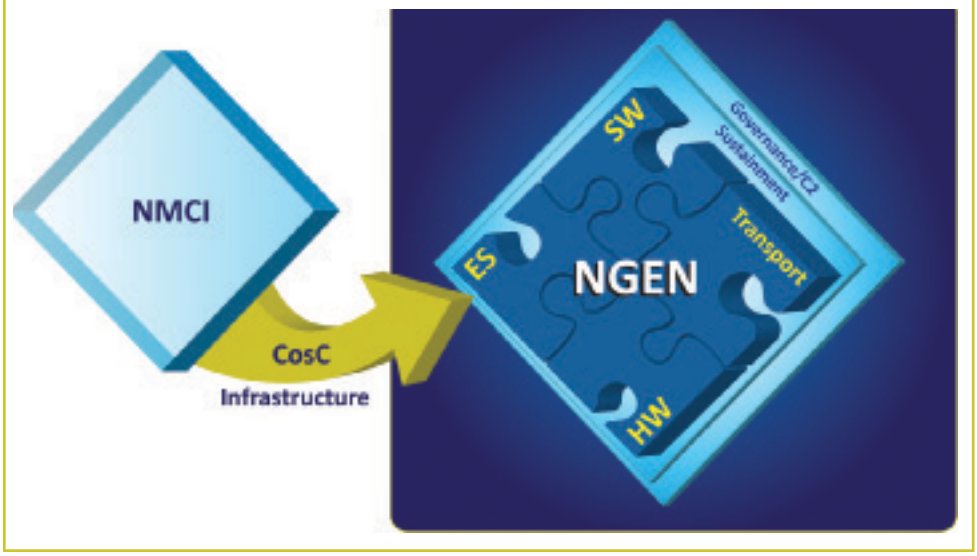


Figure 1.

NMCI Consolidates Assets

Not only was the decision to consolidate the naval networks revolutionary, the contracting vehicle used was also precedent setting. Prior to NMCI, a model did not exist in the Department of Defense (DoD) in which a private company was hired to build, manage and maintain an entire intranet.

Despite some early growing pains, NMCI quickly proved to be hugely successful, cost effective and reliable; it provided an unprecedented level of service and security for the DON and ensured a rich user experience, forever changing network security and IT management for the department.

The move to NMCI required users to change behaviors and eliminate poor security habits, such as loading unlicensed or unauthorized software onto government computers and using commercial e-mail accounts to conduct department business.

"The biggest change management obstacle we had was going from a

world where people felt that they had complete control, and they had a lot of autonomy in how they built, maintained and operated their networks. It may be a nice world to be in, but it is completely unsecure; there is no discipline from a spending perspective, and it doesn't meet any enterprise goals. That is the reason we transitioned to NMCI," Weller said. "Anytime you transition from where you have a high degree of localized control to a high degree of centralized control, which was by design and by definition exactly what we intended, there is going to be a natural tendency to resist the change."

NMCI standardized everything from network operations and data security to technical support and real-time communications across every level of command in the Navy and Marine Corps. Standardization achieved a number of goals, including increased productivity, interoperability and security within the DON through the use of common hardware, software and operating systems and decreased costs through the elimination of redundant IT solutions and a reduction in the number of routers, switches, servers and legacy applications.

Cost savings were also achieved through centralized technical and help desk support which replaced local technical support centers.

NMCI is not a static network; it is continuously evolving with the introduction of new technologies, improved service delivery and enhanced security which included the use of authentication services — the combination of the Common Access Card/public key infrastructure logon and user credentials — to ensure authorized use of government equipment and information.

"NMCI is not a 10-year-old network," Weller said. "The NMCI program is 10 years-old, but NMCI is a completely modern, five-minute-old network. We have upgraded and maintained NMCI with cutting-edge technology deployed on it since the beginning. All aspects of NMCI are state-of-the-art and state-of-the-shelf today."

The focus on security has made NMCI the most secure network in the DoD and beyond, said Capt. Timothy A. Holland, NGEN program manager. "If NMCI is not the most secure network in the world, it is certainly close. There is no shortfall that we have to address [in transitioning to NGEN]."

Today, NMCI is a mature, secure enterprise network that has transformed from a business system to a battlespace enabler that meets the needs of warfighters, supports information dominance and responds quickly to emerging needs.

Moving Toward NGEN

As the NMCI contract drew to a close, the DON decided the government should own the infrastructure and assets of the network as it evolves to its next iteration, NGEN. To transition between NMCI and NGEN, the DON signed the NMCI CoSC, a 43-month service contract with HP, on July 8, 2010.

The NMCI CoSC fulfills multiple requirements. It allows for the uninterrupted continuity of NMCI's level of service and performance, the government's purchase of the network infrastructure and assets in a phased approach and increased governmental flexibility. That flexibility included the government's purchase of the right to use NMCI's intellectual property as the technical data, processes and procedures necessary to operate and manage the network and implement NGEN. It also included the ability to purchase segments of the network's services through multiple vendors instead of the current model of a single vendor for all services.

Many people view NGEN as a "new" network, but it isn't, Holland said. Rather, NGEN is a new acquisition model rooted in industry best practices and proven methodology, such as the Information Technology Infrastructure Library (ITIL) v3, a set of concepts and practices for information technology service management.

"What NGEN brings to the table, is modeling the acquisition after Fortune 500 CIO best practices, and I am not talking about technology providers, I am talking about the users of the technology. This industry best practice allows an individual organization, specifically the Department of the Navy, to manage its core competencies where it needs to manage them. Ultimately under NGEN, we want the ability to move rapidly toward other technologies if they make sense, where they make sense, for the right price," Holland said. "While NGEN begins with the NMCI solution or architecture, it won't end there."

A critical milestone in the transition to NGEN was achieved in early October 2010 when the DON purchased the "Government Purpose Rights" (GPR) to the network's intellectual property. Those rights allow the government to share HP's NMCI and NMCI CoSC intellectual property with potential third-party

"NMCI is not a 10-year-old network. The NMCI program is 10 years-old, but NMCI is a completely modern, five-minute-old network. We have upgraded and maintained NMCI with cutting-edge technology deployed on it since the beginning. All aspects of NMCI are state-of-the-art and state-of-the-shelf today."

– NMCI Program Manager Capt. Scott N. Weller

"This industry best practice allows an individual organization, specifically the Department of the Navy, to manage its core competencies where it needs to manage them. Ultimately under NGEN, we want the ability to move rapidly toward other technologies if they make sense, where they make sense, for the right price. While NGEN begins with the NMCI solution or architecture, it won't end there."

– NGEN Program Manager Capt. Timothy A. Holland

successor contractors and the rest of the Defense Department.

Currently, NGEN acquisition is divided into several segments explained below.

- The Local Transport Services segment includes network, Information Assurance security and testing services and infrastructure sustainment.
- The End User Hardware segment includes computers, monitors and keyboards. End user hardware will be introduced as government furnished equipment via the technology refresh cycle.
- The Enterprise Software License segment includes software for end users, such as operating systems and office tools, and a requirement to support on-demand purchasing.
- The Enterprise Services segment includes seat services, such as desk side support and voice, video and data services, and non-seat services, such as e-mail and messaging, application integration and hosting services, portal services and data storage services.

At NGEN's October 2010 Industry Day held to discuss the local transport services segment, Holland challenged industry participants to use new technologies to provide the same capabilities as NMCI does now at a lower price or more capabilities at the same price.

"I want industry to be able to tell me that segments of the network can be done better, with improved performance for the same price or the same performance for a lower price," Holland said. "If a vendor can provide the same or better experience than the end user expects, NGEN will incentivize [the vendor] for that new technical solution."

A Look Ahead

As the transition to NGEN progresses, the majority of the changes will be internal, in a behind-the-scenes capacity, as the government takes over complete oversight, leadership and ownership of the network. With more than two years of preparation work already completed, the changeover from NMCI to NGEN will be seamless. CHIPS

Michelle Ku is a contractor who supports public affairs for the NMCI program.

The Department of the Navy's Program Executive Office for Enterprise Information Systems oversees a portfolio of enterprise-wide information technology programs designed to enable common business processes and provide standard information technology capabilities to Sailors at sea and Marines in the field, and for their support systems. The PEO ensures that these programs maximize value to warfighters by balancing cost with the capability delivered to the end user.

PEO EIS Programs

- (PMW 200) Navy Marine Corps Intranet (NMCI); BLII/ONE-NET provides secure, seamless and global computer connectivity for the Department of the Navy.
- (PMW 210) Next Generation Enterprise Network (NGEN) serves as the program office for the planned follow-on to NMCI.
- (PMW 220) Navy Enterprise Resource Planning (ERP) provides an integrated set of management tools that facilitate business process reengineering and interoperable data.
- (PMW 230) Global Combat Support Systems-Marine Corps (GCSS-MC) modernizes the Marine Corps' logistics systems.
- (PMW 240) Sea Warrior Program fields integrated and improved IT solutions across the enterprise that will enable the Navy's active duty enlisted and Reserve force to direct their own professional development while supporting a fleet readiness assessment.
- (PMW 270) Enterprise IT Services streamlines the acquisition and management of enterprise IT solutions and services and aligns the development, acquisition and deployment of enterprise IT solutions and capabilities to span across the U.S. Navy's enterprise networks, systems and programs of record.

Follow PEO EIS on Twitter
@PEOEIS
@PMNGEN
@NMCIEnterprise
@NavyERP
@NavySeaWarrior

We Live In A Radiant World

By Thomas Kidd

Our atmosphere is filled with electromagnetic energy from many sources. These include manmade emissions from sensors and communications equipment, electrical power lines and generators, as well as natural emissions from lightning, the sun, cosmic radiation and other sources. The electromagnetic environment is all around us every day. For example, electromagnetic energy from the sun reflects off the moon and refracts through the atmosphere to create the illusion of the harvest moon, the effect that makes the moon appear larger soon after the autumnal equinox.

Light is electromagnetic radiation. Energy arriving from the sun as infrared light warms the atmosphere, oceans and land. And when we sit in front of a campfire, we feel electromagnetic radiation, also in the form of infrared energy, warming our fingers and toes. Radio waves from the sun and distant stars can be heard as AM radio static, and on a stormy night that radio will crackle from the electromagnetic radiation released by lightning. We live in a radiant world with a very active electromagnetic environment.

Technology both impacts the electromagnetic environment and is susceptible to its negative effects. Electromagnetic energy can significantly affect Navy and Marine Corps capabilities and affect operations, training and safety. We all experience some of these effects when noise from our cell phones interferes with our music player. Those pulsating beeps and buzzing sounds are electromagnetic interference. But while cell phone noise may be a nuisance in our personal lives, electromagnetic interference to and from military systems can have significant effects on their operations.

It is critical that the Department of the Navy effectively manages and mitigates these negative effects during the planning, management and operation of installations, and during the construction and maintenance of their utilities infrastructure. In the future, as wires are replaced by wireless technology and our Sailors and Marines become more integrated into the Naval Networking Environment, the electromagnetic environment and its effects on systems must be associated with the performance attributes of emerging technology that are necessary to provide the operational capabilities required by the warfighter.

Negative electromagnetic environmental effects can not only degrade the performance of systems, but they can also place personnel at risk, damage equipment, or even trigger catastrophic events such as the unintended detonation of ordnance or the ignition of fuels. Unless the electromagnetic environment is considered during research, development and acquisition, these effects can also increase the life cycle costs of weapons systems, automated information systems, and other systems that are instrumental to the success of the Sailors and Marines who are carrying out the DON's mission.

The Department of the Navy continually strives to identify, understand, address and mitigate electromagnetic environmental effects to accomplish its warfighting missions. Because we live in a radiant world, we must all strive to minimize our impact on the electromagnetic environment and its impact on us. CHIPS

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

Necessary actions associated with the acquisition of spectrum equipment are identified in Department of Defense (DoD) Instruction 3222.3: "DoD Electromagnetic Environmental Effects (E3) Program." The instruction states that it is DoD policy that:

➔ *All electrical and electronic systems, subsystems, and equipment, including ordnance containing electrically initiated devices, shall be mutually compatible in their intended electromagnetic environment (EME) without causing or suffering unacceptable mission degradation due to E3.*

➔ *Identification of requirements for E3 control shall be initiated early during the concept refinement and technology development phases, fully defined prior to Milestone C, and verified throughout the acquisition process. Pertinent documents such as Capability Development Documents (CDDs), Capability Production Documents (CPDs), equipment specifications, Information Support Plans (ISPs), and Test and Evaluation Master Plans (TEMPs) shall specify, define, and verify E3 control requirements, as appropriate.*

➔ *Operational effectiveness and suitability of all DoD weapons, command, control, communications, intelligence, surveillance, reconnaissance, and information systems in the intended operational EME shall be demonstrated.*

➔ *E3 issues shall be identified and assessed prior to entering the Systems Demonstration and Production and Deployment phases and shall be addressed during critical design reviews. TEMPs shall include within the scope of critical operational issues and sub-issues, the requirement to demonstrate the effective E3 control of systems, subsystems, and equipment.*

➔ *The operational electromagnetic compatibility disposition of systems, subsystems, and equipment shall be reported in the ISP or in other management/support plans.*

➔ *Hazards of Electromagnetic Radiation to Ordnance (HERO), Hazards of Electromagnetic Radiation to Personnel, and Hazards of Electromagnetic Radiation to Fuel shall be mitigated prior to the conduct of all military exercises, operations, and activities.*

Department of the Navy Enterprise Architecture: Providing Value to Stakeholders

By Victor Ecarma and Fumie Wingo

The Department of the Navy Enterprise Architecture (DON EA) continues to provide stakeholder value and support DON transformation. Since its initial release in July 2009, the DON EA has been focused on two overarching goals:

- Guiding the department's Information Technology, including National Security Systems (IT/NSS), investments toward achieving departmental goals and objectives. This is done by including actionable content in the DON EA, such as those artifacts associated with data at rest (DAR) encryption, fielding only supported commercial off-the-shelf software, and DON NIPRNET public key enablement (PKE).
- Assisting DON program managers in the development of "solution architectures," as mandated by the Joint Capabilities and Integration Development System and Defense Acquisition System processes. This is done by providing program managers "plug-and-play" DON EA products to be used as a foundation for their architectures.

All DON IT/NSS systems are assessed on an annual basis for compliance with the DON EA. The need to perform an assessment is triggered by one of the following events:

- A DON Information Management/ Information Technology (IM/IT) Investment Annual Review. As of Oct. 1, 2010, the IM/IT Investment Annual Review process was expanded to include all four mission areas: Business Mission Area (BMA), Enterprise Information Environment Mission Area (EIEMA), Warfighting Mission Area (WMA) and Defense Intelligence Mission Area (DIMA).
- A Title 40/Clinger-Cohen Act (CCA) Confirmation. Title 40/CCA Confirmations are required for all Information Technology/National Security Systems, prior to each formal acquisition milestone, contract award and deployment and fielding decision.
- A DON NIPRNET public key enablement (PKE) waiver request.

The DON EA is an integrated architecture, as depicted in Figure 1, which is made up of enterprise-level architecture content, as well as the solution architectures of the DON. The enterprise-level content provides program managers with foundational information to be used in the development of their program-specific solution architectures. It helps to minimize the need for solution architects to recreate portions of the enterprise architecture that are not specific to their individual program. In addition, the solution architectures, developed by individual DON programs, are one of the key mechanisms used to expand and mature the DON EA content. The DON EA enterprise-level content also provides authoritative requirements, which program managers must comply with, to ensure their particular solution is aligned with achieving departmental goals and objectives.

With the release of DON EA v2.0.000 in July 2010, the architecture content was expanded to include traditional DoD Architecture Framework (DoDAF) products such as the Capability Taxonomies (CV-2), Organizational Hierarchies (OV-4), Operational Activities (OV-5), Technical Standards (StdV-1), Technical Standards Forecast (StdV-2), and architecture common element lists. DON EA v2.0.000 requires acquisition category (ACAT) programs to document their solution architectures in a particular way and/or to make use of DON EA artifacts as their starting point. In addition, DON EA v2.0.000 included new and updated laws, regulations, policies and guidance (LRPG) artifacts, which are based on existing DoD and DON policy and strategy, such as requirements associated with Navy conditioned based maintenance.

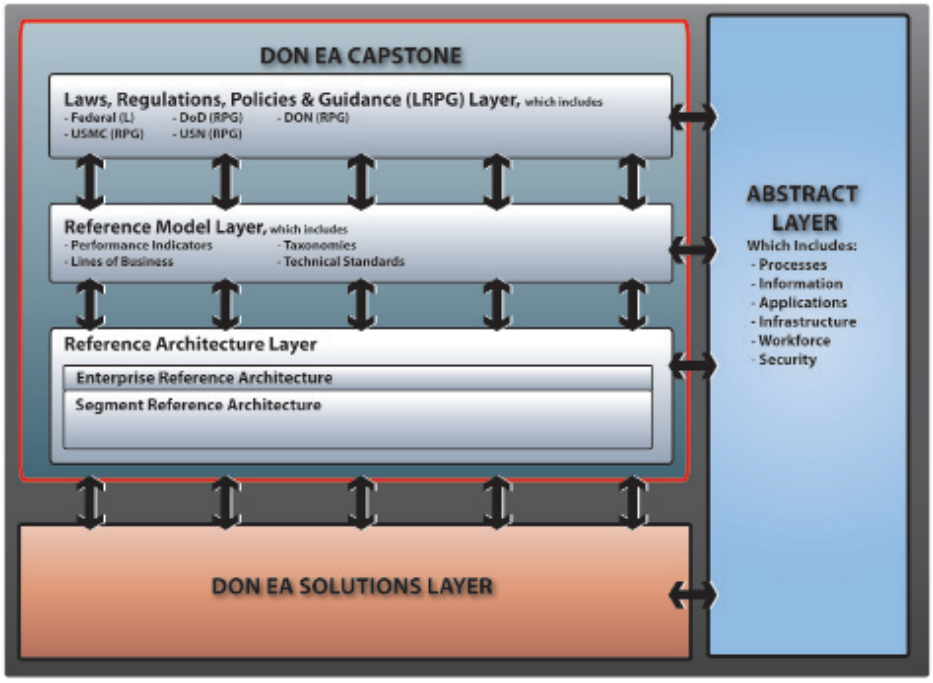


Figure 1.

The DON EA compliance and waiver processes are the mechanisms used to ensure that existing policy and strategy (i.e., LRPG), and other contents of DON EA, are properly executed by DON programs. Effective Oct. 1, 2010, compliance assertion, waiver requests and review processes have been fully automated in the DON variant of the DoD Information Technology Portfolio Repository (DITPR)-DON.

Each DON EA waiver requested represents an individual DON program or project that has been made aware of departmental goals and objectives, which they were not adequately aligned to achieve. Granted waivers include identification of specific expectations of how and when the program or project needs to become compliant with the requirements of the DON EA, thereby aligning the program or project with achieving the associated departmental goals and objectives.

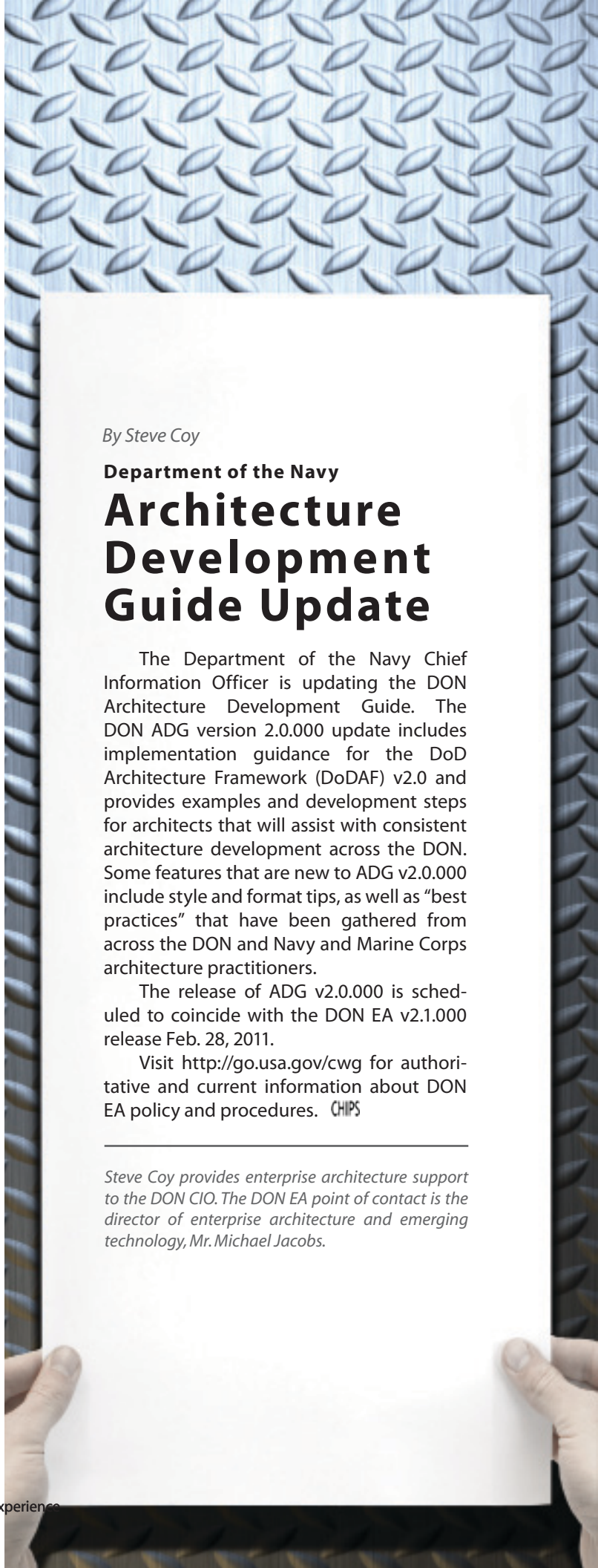
On Sept. 15, 2010, the DON EA Governance and Configuration Management Plans were officially released. The DON EA Governance Plan formalizes the roles, responsibilities and standard operating procedures of the DON EA Approval Board, DON EA Working Group, and DON EA Independent Verification and Validation (IV&V) Board. The DON EA Configuration Management Plan establishes standard procedures for management and maintenance of DON EA content, policy and procedures.

Moving forward, the DON Chief Information Officer (CIO), in partnership with the DON EA Approval Board member organizations, DON Deputy CIO (Navy), DON Deputy CIO (Marine Corps), Deputy Chief Management Officer, and Assistant Secretary of the Navy for Research, Development and Acquisition Chief Systems Engineer, are working toward accomplishing the following major initiatives associated with upcoming DON releases:

- Incorporating DON EA content and compliance into the Systems Engineering Technical Review process which will ensure alignment with the DON EA of DON solution architectures and system designs early in the program's acquisition life cycle.
- Establishing pilot Segment Reference Architecture (SRA) communities of practice (COPs) to develop Logistics, Net-Centric and Force Support SRAs, as well as to prove the processes and procedures necessary to successfully run DON EA COPs.
- Developing a robust DON EA Repository strategy that will provide functional capabilities of content management, architecture development support, the DON EA compliance assessment process and executive dashboards.
- Providing DON EA training and communications to increase DON EA awareness and alignment across the DON.

The DON CIO is planning to release DON EA v2.1.000 in February 2011 and v3.0.000 in July 2011. As the DON EA continues to grow, stakeholders are strongly encouraged to provide recommendations about how the DON EA may better support their business needs. Comments or recommendations may be submitted at http://go.usa.gov/1bG. All authoritative DON EA content, policy, procedures and guidance may be accessed at http://go.usa.gov/1bf. CHIPS

Victor Ecarma and Fumie Wingo provide support to the DON CIO enterprise architecture and emerging technology team. The DON EA point of contact is the director of enterprise architecture and emerging technology, Mr. Michael Jacobs.



By Steve Coy

Department of the Navy

Architecture Development Guide Update

The Department of the Navy Chief Information Officer is updating the DON Architecture Development Guide. The DON ADG version 2.0.000 update includes implementation guidance for the DoD Architecture Framework (DoDAF) v2.0 and provides examples and development steps for architects that will assist with consistent architecture development across the DON. Some features that are new to ADG v2.0.000 include style and format tips, as well as "best practices" that have been gathered from across the DON and Navy and Marine Corps architecture practitioners.

The release of ADG v2.0.000 is scheduled to coincide with the DON EA v2.1.000 release Feb. 28, 2011.

Visit http://go.usa.gov/cwg for authoritative and current information about DON EA policy and procedures. CHIPS

Steve Coy provides enterprise architecture support to the DON CIO. The DON EA point of contact is the director of enterprise architecture and emerging technology, Mr. Michael Jacobs.

Wikis, Portals and Bandwidth Considerations in the Fleet

Designing portals to optimize bandwidth and usability

Using open standards allows greater interoperability with mission partners

By Lt. Cmdr. Pablo C. Breuer

Collaborative Sites

The Navy has long had a requirement for units to share information at great distances to collaborate on mission essential tasks. Whether called wikis, portals or collaboration sites, these tools allow large groups to share information in near real-time. For the sake of simplicity, these types of sites will be referred to as wikis for the remainder of this article. If you have used Navy Knowledge Online (NKO), All Partners Access Network (APAN), the Non-Classified Enclave (NCE), a Microsoft SharePoint portal, Collaboration at Sea (CAS), or Wikipedia, you have used a wiki.

Since the use of these sites is new to the fleet, there are understandably some growing pains. One of the greatest challenges to using current tools is the bandwidth required to support them. While many of these sites are shore-based, it is important to remember that often customers are not. A page that loads instantaneously on a shore network may load slowly on a carrier — and be completely unusable on a frigate. Fortunately, great gains in bandwidth management can be had if we break a little "cultural china" and teach users to properly use the tools as intended. Ensuring a wiki is properly designed will take us the rest of the way.

Wikis, portals and collaboration sites all refer to the same set of tools. While it's true that wikis provide voice and desktop sharing functionality, the largest savings in bandwidth usage and tool usability lie in the format used to share information via text (including documents) and chat. Sharing documents via a wiki requires a fundamental paradigm shift for users.

Wikis allow the content of the document (picture and text) to be placed directly on the page or for a document to be uploaded for users to download. Wikis are not shared/global drives; thus, attaching a Microsoft Word document not only negates the advantages of using a wiki (collaborative editing and search), but also drastically increases the amount of bandwidth required to share the information.

Content Generation

Decreasing the size of content files dramatically reduces required bandwidth; and therefore, drastically increases the amount of service that can be provided by a given bandwidth. Very simple changes can have an enormous effect on data size. For example, the operation order (OPORD) for the Navy's exercise, PANAMAX 2010, is 5.1 megabytes, but the text content is a mere 53 kilobytes — 100 times smaller!

The OPORD also contained two maps that were reduced in file size to less than 50 kilobytes each by reducing the image resolution and changing file type. Doing the math, even these results are 33 times smaller than the original OPORD!

Cosponsored by U.S. Southern Command and the Panamanian government, the 12-day PANAMAX exercise held in August brought together sea, air and land forces in a joint, combined operation. To understand the scope of planning for PANAMAX, it is important to note that the exercise consisted of participation from 2,000 personnel and 18 nations.

Undercutting Search

In adopting an information sharing solution, there are many options to consider: How will the wiki be used? Do users need to download a Microsoft document or do they simply want to reference the information inside the document?

Have you ever searched in vain for a document following these steps?

- Go to a folder/directory/Web page;
- Click on a document that *might* be what you are searching for;
- Wait for the document to download;
- Wait for the application to open;
- Wait for the document to be opened by the application;
- Scan the document and determine it is not what you are looking for; and
- Return to step one and repeat until the appropriate document is found!

This process can be maddening! Now consider that every time you click on a link it takes 30 to 60 seconds to see a result (much longer on a frigate). Luckily, most wikis have a search feature; unfortunately, the search feature will search the text content of the wiki, but it will not typically search inside attached Microsoft Office documents.

At this point, if users are attaching Microsoft Office documents, they are not only downloading large documents — much larger than necessary — but also downloading documents that will not be used because users can't determine if they contain the information they need.

Here is a recent scenario from Operation Unified Response in Haiti to illustrate the point. Non-governmental organization (NGO) doctors at mobile field hospitals had a need to know when medical evacuation helicopters would deliver patients to their facility; their only communication tool was a smart phone. Is it more reasonable to expect them to download and open/view a Microsoft Excel document or view a "lite" version of a Web page to find this information?

Undercutting Version Control and Collaboration

It is rare that a document is written, beginning-to-end, by a single person. Quite often, different people are required to work on different sections of the same document. Additionally, that document is often submitted for approval and editing by the chain-of-command in an organization. Microsoft Office allows changes to be tracked via the "Track Changes" feature. Using this feature, you can see who made changes and why.

What Microsoft Office does not allow, however, is for multiple persons to edit the same document at the same time. This invariably leads to multiple copies of the same document spread throughout the network, none of which are completely up-to-date.

Consider the process for updating an OPORD for an exercise. The N3 (operations) needs to update Annex R,

MAYPORT, Fla., (Aug. 25, 2010) U.S. Air Force Gen. Douglas Fraser, Commander, U.S. Southern Command, U.S. Navy Rear Adm. Vic Guillory, PANAMAX 2010 Combined Force Maritime Component Commander, and Panamanian navy Cmdr. Osvaldo Urenas, PANAMAX 2010 Deputy Combined Force Maritime Component Commander, are briefed by Ecuadorian navy Cmdr. Juan Pablo Tascon during PANAMAX 2010. PANAMAX exercises a variety of responses to requests from the Government of Panama to protect and guarantee safe passage of traffic through the Panama Canal, ensure its neutrality, and respect national sovereignty. U.S. Navy photo by Mass Communication Specialist 2nd Class Robert A. Wood Sr.

while the N6 (communications) needs to update Annex K. In this scenario one of three things will happen:

- Annexes K and R will have to be separate documents that will need to be merged by someone.
- Annexes K and R are contained within the same file and either N3 or N6 will have to wait for the other to finish making updates before starting work.
- N3 and N6 will each make a copy of the OPORD, neither of which will contain updates made by the other, and someone will have to figure out what changes were made and merge the documents.

To date, we've tried to mitigate this challenge by either placing "last updated" on the document or using version numbers. Unfortunately, in time-critical operational situations, this is less than ideal. What if the N3 decides to update from version 1 to version 2, while N6 decides to update from version 1 to version 1.1?

What if both of these updates happen on the same date rendering the last modified date useless for tracking purposes? But placing the content of a document on a wiki, allows multiple persons to update content simultaneously and still see incremental changes being made by other personnel in near real-time.

Additionally, many wikis have the capability to track changes much like Microsoft Office, so it's easy to determine who made changes, where, when and why. This allows real-time version control and ensures that all personnel have access to the most up-to-date document.

Wiki Architecture and Features

Information professionals and system administrators must keep in mind their target audience, expected use and future requirements when acquiring and setting up a wiki. Target audiences may be strictly U.S. Navy shore commands, but can also include U.S. naval ships, foreign navies or NGOs. Some users may only need to view the information while others may need to view and edit.

Stick to Open Standards

Keep in mind that not everyone uses Microsoft products. Whatever product is used, it should have vendor agnostic standards. HyperText Markup Language (HTML) is an open standard; Active Server Pages (ASP), Lotus Domino and Adobe Flash are not. While Microsoft SharePoint has good integration with Office 2010, U.S. Navy ships use the Common PC Operating System Environment (COMPOSE), which does not currently support Office 2010.

During Operation Unified Response, the primary method of information access was via cell phones which do not support Active Server Pages. Another consideration is that some of our partner nations and NGOs do not use Microsoft products, so sticking to open standards and using HTML for display and Standard Query Language (SQL) for database backends will ensure maximum compatibility for future growth and ease of data migration into the future.

For best results for information sharing, no custom software client or fly-away kits should be required; they will certainly not be part of the baseline for partner nations or NGOs. Additionally, custom clients are costly in terms of time and money. Fly-away kits are also difficult to incorporate into the networked environment because there will never be enough of them for all users, and it will always be a challenge to get the kits to the right deploying unit on time.

Further, what happens when a component on a fly-away kit has a casualty? Are there enough kits left in reserve for replacement? At this point, the equipment that was considered a fly-away kit is now organic to the ship, and there is no flying away anymore.

Mobile and Reduced Bandwidth Versions

Users need content, although some will want it to be aesthetically pleasing. Separate mission need from user want. In the June 2010 edition of the Information Professional (IP) newsletter, I wrote an article on how bandwidth-restricted commands could direct users to mobile, "lite" versions of websites through user agent strings.

One brave IP implemented this temporarily on a carrier strike group for the entire Facebook website. The mobile version of Facebook allowed the crew to communicate with friends and family, but did not allow access to FarmVille or some of the other games.

While the primary mission of allowing Sailors to communicate via social networks was accomplished, many complained about the lack of access to unauthorized, bandwidth-hogging information assurance risks. This is a clear example of a user want versus a mission need. Mobile or lite versions of Web pages provide vast savings in bandwidth

usage while providing 90 to 100 percent of the functionality that users need.

Security

The security of any network-enabled tool is critical. There are some very basic administrative steps that should be taken to secure these network tools. The first obviously is to be cognizant of who is authorized to view information and who is authorized to edit information. Fortunately, wikis keep logs of user updates.

It is equally important to have a good authentication scheme. User names and passwords are usually sufficient, but the password requirements should include both complexity and expiration requirements. Likewise, user accounts that have become dormant or which belong to personnel that no longer require access should be deleted.

Active content is a necessary evil when it comes to wikis. A scripting language, such as Java and SQL, for access to the back-end database will be required. This could open up the wiki and its users to a litany of attacks from cross-site scripting (XSS) to SQL injection attacks. Commands fielding these technologies should keep up-to-date on all Information Assurance Vulnerability Alerts (IAVAs) and periodically test their wiki with an automated tool that tests for vulnerabilities.

Consider the Layout

There is no right or wrong way on how to design a layout for a wiki, but there are some best practices. Two things that are of paramount importance to users are determining what content has changed since they last logged in and helping them find the content they're looking for. Streamlining these tasks will save users from tremendous frustration, and it will also save the unit's bandwidth.

After the initial login screen, the next page to load should be useful to the user. This seems intuitive, but I've seen so many wikis where this is not the case. Upon logging in, a user should be presented with a page that contains three things: a "What's Hot" list of important documents/links/content; any system-wide announcements; and any changes to content to which the user subscribes.

For NKO, What's Hot might be changes to uniform policy; system-wide announcements might be upgrades to NKO servers; and user subscribed content might be changes to the IP officer page. Additionally, pages should have Really Simple Syndication (RSS) feeds. An RSS feed includes summarized text and metadata with a published date and eliminates the need to click into the actual content. More importantly, RSS feeds can be updated without explicitly visiting a site and, in many cases, RSS feeds can be accessed without even opening a Web browser.

Sites should be designed so that it takes no more than five clicks to get to any content on a wiki. Remember that every time a user selects a link, there will be a waiting period for the page to load. Tree views, which present a hierarchical view of information, are great for navigating directly to content. It's also important to provide a "map" to show users where they are currently located on the wiki.

Mobile or lite versions of Web pages provide vast savings in bandwidth usage while providing 90 to 100 percent of the functionality that users need.

Knowledge management is key to the success of your wiki. If your wiki supports a staff, the organization of the wiki should probably mirror the staff organizational chart. Remember to archive outdated content. Note that I wrote "archive" and not "delete." Depending on the content, it may be beneficial, or legally required, to keep old documentation. Create an archive section that is also easy to navigate. Congratulations, you are now a wiki wizard!

Continuity of Operations

This tongue-in-cheek expression often holds true: "Why buy one when you can buy two at twice the price?" We often work in adverse conditions. Things break. No plan survives enemy contact, so we need a secondary location for our files in case of a downed communications link. A possible single point of failure *will* become the single point of failure; thus, wikis and their content must be backed up regularly.

One area in which wikis are currently lacking is in the area of replication. The latest high-tech buzzword is "the cloud." What does it mean? It means that if the server that holds all of my data dies right now, none of my users are the wiser because another server *magically* makes itself available. It means that if I can't reach the U.S. Naval Forces Southern Command, U.S. Fourth Fleet (C4F) portal, my network automatically presents me with an exact replica that is mirrored on my ship. This idea of replication is an area ripe for development.

Chat

Chat offers a completely different functionality than a traditional wiki; however, chat is often supported in conjunction with the use of a collaboration portal. Most of the best practices for selecting a chat product are the same for selecting a wiki. Stick to open standards and reduced bandwidth variants when possible. The two most common chat protocol standards are Internet Relay Chat (IRC) and Jabber/XMPP (Extensible Messaging and Presence Protocol).

The advantage of using IRC or XMPP is that clients exist for virtually any and all operating systems including cellular phones. Additionally, if installing custom software is not an option, Web-enabled clients exist that require nothing except a Web browser and Java. While shore-based commands have the advantage of using Web-enabled clients, bandwidth restricted units may want to install standard software clients. Most modern chat clients support multiple standards. It is recommended, however, that unneeded and bandwidth-intensive features, such as file transfer and video chat, be disabled by default.

Create and Collaborate

Wikis hold tremendous promise for collaboration and can be tremendously successful tools if selected, administered and used correctly. We must find ways to create and collaborate with each other, with our partners, and with NGOs in near real-time. Wikis hold the promise of letting us do just that. CHIPS

Lt. Cmdr. Pablo C. Breuer is the staff communicator for Commander, Destroyer Squadron 40.

GOING MOBILE

500,000 Apps (and Nothin' On) Will Mobile Apps Get Serious in 2011?

By Mike Hernon

Most of the buzz in the mobility world these days is about apps, apps and more apps. The growth in the number and variety of mobile applications over the last 18 months has been dramatic. This has been the result of the owners of mobile operating systems promoting their platform to the application developer community and providing free or low-cost development tools. Mobile devices now compete in the marketplace on the strength and size of their application libraries as much as, if not more than, their voice and data services.

Many Defense Department and Department of the Navy mobile users feel left behind in the app wars. Due to, among other reasons, the need to maintain information assurance, DoD and federal government users typically have access to a more limited range of devices and operating systems than the standard consumer. Also, systems development on mobile platforms within the DoD has not grown as fast as in the consumer market.

The promise of the app explosion was to deliver highly functional mobile apps that would allow the mobile workforce to be as productive on their smart phone as if they were sitting in front of their office desktop computer. Is there any evidence that this is indeed happening?

An analysis of the state of mobile apps shows that, to date, they have not fulfilled the promises made. With enhanced connectivity increasingly becoming available, the opportunity exists for both the consumer and government mobile app environments to better support the mobile workforce with rich and robust productivity tools.

Apps Analysis

As of this writing the Apple Apps Store has 300,000 mobile applications available for downloading to iPhone, iPod or iPad. There were 85,000 apps for Android-based devices, and a little more than 15,000 listed in the BlackBerry App World online catalog. Thousands of apps are also available for the Palm webOS platform, Windows Mobile, and more. These numbers will almost certainly be out of date by the time you read this article.

Recent analyses of the way apps are actually used present some intriguing, if not depressing, insights, according to a Nielsen study (see http://blog.nielsen.com/nielsenwire/online_mobile/the-state-of-mobile-apps/). Twenty-one percent of American wireless subscribers have a smart phone, 59 percent of those have downloaded an app in the last 30 days, and the average number of apps on their phone is 22. However, another study of iPhone and Android apps shows that more than half of the people who downloaded an app abandoned it in the first month and after three months more than 90 percent of users abandoned the app (see http://blog.flurry.com/bid/30548/Flurry-Smartphone-Industry-Pulse-January-2010). For those of you who engage in the *"My phone is a better platform for apps than your phone"* debates, be aware that the retention rates for both operating systems were nearly identical.

These statistics indicate a significantly high level of churn — users are downloading apps and then abandoning them at incredible rates. Why are people seemingly so fickle with the apps they took the time to download, and in many cases, paid for? The Nielsen study shows that a large majority, some 61 percent of app use, was for games. Perhaps once you have mastered Breakout or the latest fad game on your phone you're not likely to go back to it.

Also, some apps are relevant for a limited time, for example, the Apps Store carries no less than a dozen vuvuzela soccer horn apps months after the World Cup has ended. Are people blowing their virtual vuvuzelas at National Football League games? Not likely.

And the productivity apps that were to lead the mobile revolution? They landed in a distant 11th place, representing only 22 percent of apps used.

In 1992 Bruce Springsteen wrote "57 Channels (And Nothin' On)" as a plaint about the state of television. It is hard to escape the conclusion that much the same could be said about the state of mobile apps (not to mention TV) in the year 2011.

Toward a DoD App World

While DoD may be behind in the app game, the above suggests that, at least so far, we really haven't missed much. Delivering on the vision of an enterprise mobility capability that better enables our warfighters and those who support them to accomplish their missions untethered from the network remains a priority. Enhanced mobile capabilities can also cut down on desktop phone and computer expenditures, support ad hoc operations, such as continuity of operations and disaster relief efforts, and will no doubt play an increasingly critical role in tactical settings.

Bringing a robust, practical DoD mobile app capability into fruition will require steps from both industry and the DoD information management/information technology (IM/IT) community, including:

- Connectivity enhancements. The commercial cellular providers are now rolling out their 4G networks, which deliver significantly higher data transmission speeds than today's networks. The 4G will be a critical enabler for app support in general, and allow some applications, such as mobile video conferencing, to operate in a wider variety of settings without Wi-Fi.

Within DoD installations, Wi-Fi and WiMAX capabilities will need to expand dramatically. In addition to providing broader signal coverage, keeping the traffic within DoD domains as much as possible will increase functionality and security.

- Application and Architecture Integration. All new application development efforts should consider how to best integrate the mobile user from the ground up, instead of later as a "bolt-on" capability. Today's mobile clients are more than powerful enough to run apps from the cloud, and in many ways are more powerful platforms than a desktop thin client computer. Likewise, as DoD and its components build their transport infrastructure to deliver unified capabilities (the delivery of voice, video and data on an all Internet Protocol (IP) converged network), mobile networks and users must be part of the planning and deployment process.
- DoD App Store. Because of the federal government and DoD's unique security requirements, an app store dedicated to DoD developed or approved apps will probably be necessary. This will ensure that the only applications that touch the Global Information Grid have been properly vetted and reviewed. A common DoD repository for mobile apps will also promote sharing of apps across the community and will better leverage the investments made in developing them.
- Enhanced Security. The encryption algorithm that protects many of today's cellular transmissions has been broken and can be easily exploited with minimal investment or technical expertise. Industry must continue its efforts to respond to, and hopefully, avert such breakdowns.
- End User Insights. Many of the apps available in the commercial marketplace are duplicative, have a limited life span, or otherwise provide little value to the end user. DoD must develop the mobile apps that people need and will use. Soliciting input from the warfighter and other communities of interest will facilitate the delivery of apps that are both functional and relevant to the DoD mission.
- Policy. Maintaining a balance between information assurance and increased wireless use for official business will remain a challenge as technology continues to advance and consumer experiences continue to expand. Wireless policy must be robust enough to meet user expectations while protecting the information stored and transmitted by mobile devices. In some cases, existing policy may need to be relaxed.

Groundbreaking Future DoD Apps

Apps developed within DoD on mobile platforms so far have primarily been stand-alone applications. These apps store content on the mobile device for reference later and no active wireless connection is required. Examples include MobiAFG, developed by the Naval Postgraduate School, which provides a trove of content related to Afghanistan for deployed troops, and the Individual Augmentee mobile app developed by U.S. Fleet Forces Command to support deployed Sailors performing duties outside of traditional Navy billets. For connected devices, the Marine Corps Marathon developed a feature rich app delivering real-time race updates and results.

Future mobile apps are envisioned to support a broad range of DoD and DON activities from the back office to the battlefield. By learning from the current state of the commercial app environment, a more focused and relevant DoD app environment can be developed. CHIPS

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

Bold Alligator 2011 - *the Blue-Green Team Together Again*

By Sharon Anderson

On a blustery day on the Norfolk Naval Base, Commander, Expeditionary Strike Group Two (ESG 2), and Commander, 2nd Marine Expeditionary Brigade (2nd MEB), in coordination with ships assigned to the U.S. Second Fleet, were hotly engaged in Bold Alligator 2011, the largest joint fleet simulated amphibious exercise in the last 10 years.

But don't let the word "simulated" fool you — the exercise included a total of 29 participating commands, including eight ships, 14 ESG/2nd MEB reporting units and seven training centers. While about 500 Sailors and Marines took part in the exercise, the scenarios were built for more than 10,000 notional forces operating within a highly volatile concept of operations.

The scenario for the exercise consisted of a forcible entry operation conducted to enable a non-combatant evacuation in the midst of a violent sectarian conflict. This complex but realistic mission required the ability to respond rapidly, project a credible force ashore, and organize and execute the evacuation of thousands of non-combatants. "In many cases, these capabilities can only be provided by amphibious forces," said Brig. Gen. Chris Owens, the commanding general of 2nd MEB, a few days before the exercise began.

Running Dec. 11 through 17, the exercise was designed to focus on the fundamental aspects and roles of amphibious operations to improve amphibious force readiness and proficiency for executing the six core capabilities of the Maritime Strategy: forward presence, deterrence, sea control, power projection, maritime security and humanitarian assistance/disaster response. Bold Alligator 2011 is the first of many planned Bold Alligator exercises; the next one, a live exercise, is scheduled for February 2012.

Media representatives gathered on the multipurpose amphibious assault ship USS Bataan (LHD 5) Dec. 13 to speak with exercise participants and view some of the hardware used in the exercise, including a 38-foot Nighthawk unmanned patrol boat, the intelligence gathering, unmanned vehicle Scan Eagle and a Sea Knight helicopter.

"We want to show you this because all of these assets play a part into that amphibious capability. When I talk about amphibious capability, I am talking about the ability to go from ship to shore and the ability to project that combat power to shore. No one else in the world has this kind of capability and the combination of services that we [Navy and Marine Corps] can provide. When we look at these different assets, each one of them plays a little part in the bigger picture," said Marine Corps Capt. Timothy Patrick, the public affairs officer for the 2nd MEB.

Rear Adm. Kevin Scott, commander of Expeditionary Strike Group (ESG) 2 emphasized the importance of "staff training and integration" within Bold Alligator. Although the U.S. Marines are legendary for conducting large-scale amphibious landings, for the past 10 years they have been landlocked in Iraq and Afghanistan. "Sailors and Marines who are in the services now do not have the training and experience in working together in amphibious operations. We will be building proficiency and interoperability," Scott said.

But Marines were aboard the Bataan to assist with humanitarian relief in response to the catastrophic earthquake which crippled Haiti in January 2010. Operating three miles from shore and equipped with heavy-lifting and earth-moving equipment, medical support facilities, a complement of Navy and Marine helicopters, as well as air cushion landing crafts, the combined Navy-Marine Corps team transported relief supplies and conducted medical evacuations.

"It is a misnomer that we haven't been doing amphibious operations over the last 10 years. Just because we are not going across a beach Normandy-style doesn't mean that we haven't been doing amphibious. In the last 10 years, we have probably had 12 or 13 different amphibious operations, most recently down in Haiti," said Chief Warrant Officer 3 Tony Siciliano, the systems planning engineering officer for Bold Alligator. "What this exercise really brings to the table, is getting that larger staff, larger than a MEU, that MEB staff integrated with the PHIBRONS and integrated with the Expeditionary Strike Group. It really builds the teamwork that you can honestly say has been lacking in the last few years with the land-based focus of Iraq and Afghanistan."

The exercise also gives the Navy and Marine Corps the opportunity to test their communications systems interoperability. To say that technology has changed a lot in the last 10 years would be an understatement.

"I have been doing this for about two years and I have seen changes since I have been onboard," said Lt. Cmdr. Andy Lucas with the ESG 2 C5I Department (N6). "We have had computer networks since I started doing this. I know, obviously years ago, the Marines and Navy staff never had computer networks onboard."

Cmdr. Eugene Bailey, the head of N6 for ESG 2, discussed the incompatibilities he has already discovered between Navy and Marine Corps systems since the exercise began.

"Some of the things that we are finding is that ships, especially the amphibious fleet, because of the dynamic nature [of operations], we have the advances of the Marine Corps [technology] which are outpacing the Navy amphibious baseline. We are seeing the disparity between things like Microsoft Office products interoperability between different communications systems because Marines have purchased more advanced equipment, or in some cases, have had their servers loaded with different things than what we currently have on ships because the ships are tied to the SHIPMAIN process [for modernization]. One of the things that concerns me as the C5I officer for the strike group, looking across the spectrum of amphib ships, is that I don't think in this arena we are agile enough to respond to a dynamic threat and be able to keep up with the Marine Corps' pace of advancement [in technology] if we don't do something quickly."

But Bailey quickly pointed out that the purpose of Bold Alligator is to do just that — to bring the incompatibilities between equipment to the attention of higher leadership for quick action. The chain of leadership goes all the way to the Chief of Naval Operations and Commandant of the Marine Corps, who have ordered the blue-green team to get back to its amphibious roots.

"My team has done a great job of turning all of our challenges into wins. From my perspective, the biggest advantage it gives for me is training because it opens up the aperture and gives a greater depth of experience to my Sailors … Because of the synthetic na-

Bold Alligator participants included: ESG 2, 2nd MEB, 6th Marine Regiment, Marine Aircraft Group (MAG) 29, Combat Logistics Regiment (CLR) 25, Amphibious Squadron (PHIBRON) 6, PHIBRON 8, Tactical Air Control Group (TACGRU) 1, Tactical Air Control Squadron (TACRON) 21, TACRON 22, Commander Naval Beach Group (CNBG) 2, Beach Master Unit (BMU) 2, Assault Craft Unit (ACU) 2, Assault Craft Unit (ACU) 4, USS Bataan (LHD 5) and USS Iwo Jima (LHD 7).

Response cells with supporting roles included: USS Mesa Verde (LPD 19), USS Fort McHenry (LSD 43), USS Ashland (LSD 48), USS Anzio (CG 68), USS Cole (DDG 67) and USS Elrod (FFG 55).

Training centers included: Commander Strike Force Training Atlantic Norfolk, Tactical Training Group, Atlantic Dam Neck, Expeditionary Warfare Training Group Atlantic, Commander Navy Expeditionary Combat Command, Commander Afloat Training Group Norfolk & Mayport, Marine Air Ground; 2nd MEB Simulation Center, and the Marine Air Ground Task Force Staff Training Program.

ESG 2's N6, Cmdr. Eugene Bailey with Lt. Cmdr. James Carsner (seated) during Bold Alligator 2011 aboard the USS Bataan (LHD 5).

ture of the exercise, we had to become experts on a lot of different systems. From my perspective that is a win because now my folks understand the operational flow of information: how it goes from weapons systems and radar to the watchstanders and to the leadership to be able to make decisions," Bailey said.

CWO3 Siciliano explained the communications that create situational awareness and commanders rely on for decisive action. "The ISR piece is huge now, where a few years ago it was a 'nice to have.' It was that 'sexy' technology that only the special operations folks had. Now, much like VTCs, commanders can't live without it."

Communications during the exercise were conducted primarily via Voice over IP because of the radio frequency conflicts of operating in port, but radios play a large role in Marine Corps communications, Siciliano said.

"Ten years ago, the Marine platoon would have a VHF radio like the 119 (SINCGARS Tactical Radio, AN/PRC-119 Manpack) and SINCGARS was king. Ten short years later, we have individual radios for each Marine. There is constant communication from the fire team level and all the way up to the company level. We have the 117Golf (AN/PRC-117G), which is being fielded now, which has data networking capabilities. In the Marines now, something as small as a fire team can create these ad hoc networks on the battlefield and exchange vast amounts of information via the radios," Siciliano explained. "The 117G is the newest piece of gear that we have been issued and with its networking capabilities and the 117Fox (117F), which is larger and can do SATCOM. As a planner, that is something that I always have to consider, what the satellite systems can support, and if that is really the best way for the Marines on the ground to go."

Operating together is important but the Navy-Marine Corps team must communicate with allies, coalition partners and non-governmental organizations, as well.

"Ten years ago it was rare that we would communicate or have any information exchange requirements with foreign allies or coalition partners. Today I can't think of an exercise or operation that we conduct that we don't have a coalition or allied partner involved. That brings its own issues, and there are things that we need to consider about security of classified information and how we want to be able to interact appropriately with our allies. It is not so much technology advancement as it is a procedural and security mindset change," Siciliano said.

The technological challenges can be mind-boggling to prepare an ESG's communications for a quick deployment, and Bailey said he has already begun a list of action items that will reduce the time to assemble the communications for a large amphibious force.

"One of the things that I am taking away from this exercise is a training plan for my team and a ship's ability to flex a rapid embarkation. I have to make some purchases for additional computers to be ready to go and match up schedules with the 'big decks' that we would embark on — to match it up with whoever is the ready duty ARG (amphibious ready group) if we had to respond to something of this size. So coming this quarter, my folks will start doing a rapid embarkation two-day exercise that is strictly focused within the ESG. On the administrative side, I have some guidance to put out to each of the ships to have pre-staged support items for the flag staff as they come aboard," Bailey said.

Not only is Bailey and his staff responsible for systems interoperability within the amphibious group, the N6 is also responsible for the integration of ISR assets and systems — anything with bits and bytes.

"Each of those systems comes with different technical capabilities and requirements. One of my jobs as the senior IP, the Information Professional for the strike group and the N6, is to ensure that we have at least met minimum capabilities to support advanced warfighter needs. For each of those new technologies that give the commander a more focused picture, I try to bring those things together to give them that fused picture in a consolidated format that is easily digestible," Bailey said.

"It becomes incumbent on me to coordinate with the ships and those system owners to make sure that we can integrate those products into the ship's networks and systems seamlessly, or if there are technical challenges that I have the ability to reach out to SPAWAR (Space and Naval Warfare Systems Command) and the other program offices to find out the technical solution to make all those systems integrate properly."

Still, undaunted by the technical challenges, Bailey said he could have fly-away kits with laptop computers, printers and information stores ready for the embarked staff in four days if the amphibious group had to respond to a crisis. Remarking on the communications needs of a large amphibious force, Bailey said, "It keeps me running every day." CHIPS

For more news from Expeditionary Strike Group 2, visit www.navy.mil/local/ESG2/.

SPAWAR Responds to Fleet Needs, Develops Data Sharing Capability

SAILOR 2.0 provides the fleet with self-help capability

By Andrea Houck

The Space and Naval Warfare Systems Command (SPAWAR) provided a solution for fleet users that increases product data availability, accuracy and accessibility for fleet systems by launching a website repository Nov. 30, 2010. The SPAWAR Acquisition Integrated Logistics Online Repository, known as SAILOR 2.0, was developed in response to feedback from fleet users about their inability to access hardware and software configurations. Further, users said their relevant product support documents were difficult to find and even acquire after new systems had been installed.

"The SAILOR 2.0 team designed and created an easy to use command, control, communications, computers and intelligence (C4I) enterprise tool that addresses the core issues in helping the fleet gain access to critical documents and configuration files for their C4I products on demand," said Margaret Fellenbaum, SPAWAR's technical director for product data management.

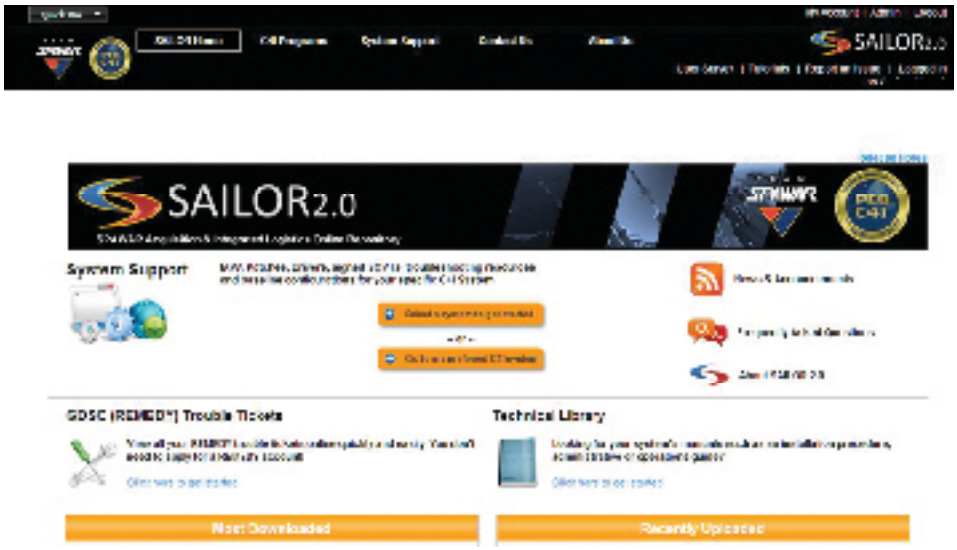
SAILOR 2.0 also allows fleet users to exchange technical knowledge with subject matter experts (SMEs) through its blogs and technical exchange forum, which increases response time and transparency, Fellenbaum said.

"SAILOR 2.0 is a critical and invaluable tool for the fleet," said Chief Warrant Officer 4 Michael Bush, from the Commander, Naval Air Forces/N6, Network Requirements office.

"The fact that it offers one-stop shopping, tailored specifically for each ship, is a major breakthrough, and it will do more than just benefit the ships, but [it] will [also] make the type commander's job easier," Bush said.

SPAWAR's Fleet and Logistics Readiness competency worked with the Program Executive Office (PEO) C4I to architect a solution to deploy critical logistics, configuration files and technical documentation enterprise-wide and provide a single point of entry to retrieve system support information for nearly 40 programs of record.

As part of this critical tool, SAILOR 2.0 provides all the documentation tools necessary to properly operate and maintain equipment and software so the fleet can improve system performance and support. This translates to increased fleet readiness, reduces total ownership costs and improves information sharing.



Previously, critical documents and configuration files were stored in disparate locations, which often led to decreased efficiency and user frustration. But now, SAILOR 2.0 eliminates stovepipe systems making all data secure and accessible across all domains in a collaborative, joint environment. SAILOR 2.0 makes it easier for the fleet to meet its mission and achieve operational excellence.

SAILOR 2.0 improves effectiveness by delivering the following requirements:

- Provides the fleet with a self-help capability reducing distance support and on-site support requirements;
- Delivers real-time access and updates for system-specific configuration, final issue technical and logistics documents, the latest security updates and baseline templates;
- Deploys interactive electronic technical manuals in their native XML format, significantly reducing distribution time and reducing the cost of compact disc production and postage;
- Minimizes system downtime and troubleshooting for support agents by providing the fleet a mechanism to exchange technical knowledge with SMEs through its blogs and technical exchange forum;
- Reduces the need for on-site technical visits;
- Diminishes technical documentation hard copy production and delivery to shipboard users; and
- Decreases help desk infrastructure support for technical documentation issues.

Last September, Capt. Pat Leary, Assistant Chief of Staff for C5I (N6), Commander, Naval Air Forces, received a demonstration from the SAILOR development team. To Leary, it was very informative, and he reported back that SPAWAR is on track to provide a capability to the fleet that has been needed for years.

"In particular, the quick links section for documentation will help the afloat Sailors," Leary said. "Bottom line: Please press on with SAILOR 2.0."

And that's exactly what the team did.

Team SPAWAR's SAILOR 2.0 deployment team will continue to provide the most technologically advanced data sharing capabilities to the fleet.

To learn more about SAILOR 2.0, visit https://sailor.nmci.navy.mil or e-mail sailor@spawar.navy.mil. CHIPS

Andrea Houck is a former communications specialist with the SPAWAR corporate communications office.

By JPEO JTRS Strategic Communications

JPEO JTRS Releases the Software Communications Architecture Next Draft Specification

The Joint Program Executive Office for the Joint Tactical Radio System (JPEO JTRS) has released the SCA Next Draft Specification. The new radio standard provides a technical refresh which will enable improved radios and extends the usability of the radio standard to other radios, including public safety, space and commercial applications.

A joint team of JPEO JTRS, commercial, and international system and software developers collaborated to produce the SCA new radio standard which defines a common framework for the deployment, management, interconnection and intercommunication of waveforms components in embedded, multiprocessor radios.

"The release of SCA Next is very important because expectations of radios have changed since the original draft SCA was released in 1999," said Jeff Mercer, director of Strategic Communications for JPEO JTRS. "Networking, small radio size, and long battery life are expected not only from personal mobile phones but also from tactical DoD radios."

The SCA separates the waveform from the radio's operating environment allowing waveform portability across various radio types. It also allows radio developers to interchange and upgrade existing radio services and hardware without major system revisions.

"The draft specification will be reviewed and prototyped over the next year and if determined mature and ready for deployment, it would formally become a new version of the SCA," Mercer explained.

SCA Next is more scalable, lightweight and flexible than SCA 2.2.2. It is compatible with radio sizes ranging from small, single channel radios to prime-power, multichannel sets.

As a technology refresh, it incorporates advances in portability for digital signal processor (DSP) and field-programmable gate array (FPGA) processors and new design patterns for its application program interfaces (APIs).

Common Object Request Broker Architecture (CORBA) is no longer required, permitting radio-specific middleware similar to the Android's remote procedure call (RPC) for communication between software components and hardware devices.

Registration of components and devices has been redesigned, incorporating a "push" model that substantially reduces communication. This enhancement facilitates dynamic or static configurations and reduces startup times.

A flexible specification for the application environment profile (AEP) defines the minimum operating system features required for a specific radio platform. Units of functionality permit a radio supplier to independently define optional services such as log, event, CORBA, multichannel, and more.

The specification is available for download from the JPEO JTRS Software Communications Architecture (SCA) website at http://sca.jpeojtrs.mil/scanext.asp.

Recent MIDS-LVT Follow-On Contract Awards

The Multifunctional Information Distribution System (MIDS) International Program Office has completed additional contract actions in pursuit of its mission to develop, field and support interoperable, affordable and secure MIDS tactical data link and programmable networking technologies and capabilities for the joint, coalition and international warfighter. The follow-on contracts, which are worth a combined total of about $64,670,000 were awarded to BAE, Data Link Solutions and ViaSat in September 2010.

The $34,500,000 follow-on contract awarded to BAE Systems Information and Electronic Systems Integration Inc. calls for the maintenance of MIDS-Low Volume Terminal (MIDS-LVT) software. About 98 percent of the work will be performed in Wayne, N.J., with 2 percent of the work performed in Paris, France.

The $24,629,000 follow-on contract awarded to Data Link Solutions calls for the delivery of MIDS-LVTs to the United States, Finland, Pakistan and Hungary. About 50 percent of the work will be performed in Wayne, N.J., and another 50 percent will be performed in Cedar Rapids, Iowa.

The $5,521,000 follow-on contract awarded to ViaSat calls for the delivery of MIDS-LVTs to the United States and Australia. About 30 percent of the work will be performed in Carlsbad, Calif., with about 70 percent performed at various sites worldwide.

MIDS-LVTs provide secure, high-capacity, jam resistant, digital data and voice communications capability for joint, coalition and international warfighters. The MIDS-LVT is procured through the MIDS International Program Office based in San Diego, Calif. The MIDS partner nations are Germany, France, Italy, Spain and the United States. Thirty countries around the world have already received MIDS-LVTs and an additional 11 countries have been approved to acquire them at a future date. CHIPS

http://jpeojtrs.mil

SAVE THE DATE

JTRS Science and Technology Forum 2011, March 14-17, 2011

JPEO JTRS will sponsor its annual JTRS Science and Technology Forum (JSTeF), March 14-17, 2011, on the campus of the University of California, San Diego, in La Jolla, Calif. Cosponsors include the Wireless Innovation Forum (WINNF) and the California Institute for Telecommunications and Information Technology (Calit2). The event will feature keynote addresses and interactive panel discussions by influential military, political, industry and academic leaders, discussing the importance of innovative wireless communications and networking within the Defense Department, emerging technologies of interest to defense planners, and the roles of industry and academia in developing future software-defined radio capabilities. Registration is available via the WINNF website at www.wirelessinnovation.org/page/NextMeeting.

JMAPS Star Catalog to Improve Satellite and Weapon Systems Accuracy

By Nicole Collins

The Joint Milli-Arcsecond Pathfinder Survey (JMAPS) will update the bright star astrometric catalog. In the future, the JMAPS star catalog and star tracker will be used to enable new capabilities for advanced missions and improve products delivered by space to the warfighter.

The stars will align with the launch of the Space and Naval Warfare Systems Command (SPAWAR) Joint Milli-Arcsecond Pathfinder Survey (JMAPS) spacecraft. The program recently transitioned from an Office of Naval Research (ONR) science and technology (S&T) program to a Program Executive Office (PEO) Space Systems acquisition category (ACAT) II program within SPAWAR.

The JMAPS mission is to produce a star catalog that will enhance military operations both terrestrially and in space by improving the output and accuracy of satellites along with many of the U. S. military's strategic weapons systems. JMAPS satisfies emerging requirements to meet future needs for high accuracy sensors and weapons systems by enabling the nation to conduct operations from space that are not technically feasible with current levels of accuracy.

"Space assets and many weapons systems use star catalogs, but the data they use is steadily degrading. By re-baselining the catalog, JMAPS will improve current performance and pave the way for a host of new technologies," said Lt. Cmdr. Sam Messer, JMAPS program manager for PEO Space Systems.

Whether using imagery to plan precision strikes or monitoring developing storms to assist in humanitarian relief, U.S. military forces rely on space as an enabler. Satellites and weapons across the spectrum of warfare utilize key satellite technologies like star catalogs to ensure accuracy and position. End-users ultimately benefit from improvements in the products and capabilities JMAPS provides that are critical to today's warfighting needs.

A team of space acquisition and technical experts build the spacecraft, develop the ground processing system and manage the program. PEO Space Systems, under the guidance of Rear Adm. Liz Young, is continuing to lead and foster the unique partnership established with the United States Naval Research Laboratory (NRL) and United States Naval Observatory (USNO). Both NRL and USNO are experts in their respective fields. NRL has a proud heritage of spacecraft development dating back to 1960 when it launched GRAB I, the nation's first operational intelligence satellite. USNO traces its renowned history in the fields of timing, navigation and astronomy to the 1830s. Together, NRL and USNO have assembled the best team of managers, scientists and engineers to execute the JMAPS mission.

"NRL works hand-in-hand with PEO Space Systems, the program manager, and USNO, the principal investigator. The exciting part of this program is that the three organizations all bring complementary capabilities," said Mr. Paul DeLaHunt, project manager for JMAPS at NRL.

NRL's primary responsibility for the JMAPS program is to construct the satellite that has two major elements designed to support the overall mission of collecting pertinent star data. One element is the design architecture of the spacecraft bus. The second element is the lightweight, high performance, and state-of-the-art instrument constructed with silicon carbide power optics, silicon mirrors, and a silicon carbide structure to minimize mass and maximize performance. The instrument utilizes hybrid complementary metal oxide semiconductor detectors to support the necessary performance and readout capability for JMAPS. The satellite's configuration while stowed for launch measures approximately 1 meter in each dimension and weighs approximately 220 kilograms.

"Without the agility, precision attitude knowledge, precision attitude control and jitter capability created by the tightly coupled spacecraft bus and instrument, the mission would not be possible," DeLaHunt said.

Upon launch, the spacecraft JMAPS will observe stars for the next 37 months. Data are collected and processed on board the spacecraft and transmitted to the mission operations center located at the NRL Blossom Point Tracking Facility several times a day.

After the data is collected at Blossom Point, the information is transferred to the U.S. Naval Observatory's Science Operation Center, located at its Washington, D.C. facility. The Naval Observatory is responsible to the Department of Defense for the maintenance and upgrade of the nation's reference frames, including the celestial reference frame. As data arrive at USNO, mission scientists monitor the instrument, and process and analyze the data providing mission planning information back to NRL. The final step in the process is the generation and delivery of the full star catalog to the Navy, which occurs one year after the end of the flight mission.

"In addition to the Department of Defense applications for which the mission is being flown, an advanced star catalog and technology will benefit other users, including the commercial satellite community and NASA. Potential NASA applications of these new, advanced capabilities include improving the ability to navigate within our solar system and enabling the discovery of planets outside our solar system," said Dr. Bryan Dorland, principal investigator for JMAPS at the USNO.

The newly transitioned ACAT II JMAPS program is focusing on delivering a star catalog that meets the program's key performance parameters that ultimately align with SPAWAR Commander Rear Adm. Patrick Brady's goal of providing vital capabilities to the fleet while achieving the Navy's vision for information dominance. CHIPS

Nicole Collins is a public affairs specialist with the SPAWAR corporate communications office.

Enterprise Software Agreements

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

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

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

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

Software Categories for ESI:

Asset Discovery Tools

Belarc

BelManage Asset Management – Provides software, maintenance and services.

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

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

Ordering Expires: 30 Sep 11

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

BMC

Remedy Asset Management – Provides software, maintenance and services.

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

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

Ordering Expires: 23 Mar 15

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

Carahsoft

Opsware Asset Management – Provides software, maintenance and services.

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

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

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

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

DLT

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

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

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

Ordering Expires: 01 Apr 13

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

Business and Modeling Tools

BPWin/ERWin

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

The BPWin/ERWin products are now available from the C-EMS2 contract on page 46. The C-EMS2 contract number is listed below.

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

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

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

Database Management Tools

Microsoft Products

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

Oracle (DEAL-O)

Oracle Products – Provides Oracle database and application software licenses, support, training and consulting services. The Navy Enterprise License Agreement is for database licenses for Navy customers. Contact the Navy project manager on page 50.

Contractors:

Oracle Corp. (W91QUZ-07-A-0001); (703) 364-3110

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

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

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

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

Ordering Expires:

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

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

www.esi.mil

agencies, DoD components and authorized contractors.

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

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

Sybase (DEAL-S)

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

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

Ordering Expires: 15 Jan 13

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

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

Enterprise Application Integration

Sun Software

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

Contractors:

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

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

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

Ordering Expires: 24 Sep 12

Web Links:

Sun Products
www.esi.mil/agreements.aspx?id=160
Commercial Data
www.esi.mil/contentview.aspx?id=160&type=2
Dynamic Systems
www.esi.mil/contentview.aspx?id=162&type=2
World Wide Technology
www.esi.mil/contentview.aspx?id=161&type=2

Enterprise Architecture Tools

IBM Software Products

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

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

Ordering Expires: 02 Dec 10 (Please call for extension information.)

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

VMware

VMware – Provides VMware software and other products and services. This BPA has been designated as a GSA SmartBuy.

Contractor: ***Carahsoft Inc.*** (W91QUZ-09-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: 27 Mar 14

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

Enterprise Management

CA Enterprise Management Software (C-EMS2)

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

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

Ordering Expires: 22 Sep 12

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

Microsoft Premier Support Services (MPS-2)

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

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

Ordering Expires: 31 Mar 11

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

NetIQ

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

Contractors:

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

Northrop Grumman – authorized reseller

Federal Technology Solutions, Inc. – authorized reseller

Ordering Expires: 05 May 14
Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

Planet Associates

Planet Associates Infrastructure Relationship Management (IRM) Software Products – Provides software products including licenses, maintenance and training for an enterprise management tool for documenting and visually managing all enterprise assets, critical infrastructure and interconnectivity including the interdependencies between systems, networks, users, locations and services.
Contractor: ***Planet Associates, Inc.*** (N00104-09-A-ZF36); Small Business; (732) 922-5300 ext. 202
Ordering Expires: 01 Jun 14
Web Link: www.esi.mil/contentview.aspx?id=143&type=2

Quest Products

Quest Products – Provides Quest software licenses, maintenance, services and training for Active Directory Products, enterprise management, ERP planning support and application and database support. Quest software products have been designated as a DoD ESI and GSA SmartBUY. Only Active Directory products have been determined to be the best value to the government and; therefore, competition is not required for Active Directory software purchases. Discount range for software is from 3 to 48 percent off GSA pricing. For maintenance, services and training, discount range is 3 to 8 percent off GSA pricing.
Contractors:
Quest Software, Inc. (W91QUZ-05-A-0023); (301) 820-4800
DLT Solutions (W91QUZ-06-A-0004); (703) 708-9127
Ordering Expires:
Quest: 30 Dec 10 (Please call for extension information.)
DLT: 01 Apr 13
Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

Enterprise Resource Planning

Oracle

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

RWD Technologies

RWD Technologies – Provides a broad range of integrated software products designed to improve the productivity and effectiveness of end users in complex operating environments. RWD's Info Pak products allow you to easily create, distribute and maintain professional training documents and online help for any computer application. RWD Info Pak products include Publisher, Administrator, Simulator and OmniHelp. Training and other services are also available.
Contractor: ***RWD Technologies*** (N00104-06-A-ZF37); (410) 869-3014
Ordering Expires: Effective for term of the GSA FSS Schedule
Web Link: www.esi.mil/contentview.aspx?id=150&type=2

SAP

SAP Products – Provide software licenses, software maintenance support, information technology professional services and software training services.
Contractors:
SAP Public Services, Inc. (N00104-08-A-ZF41); Large Business; (202) 312-3515
Advantaged Solutions, Inc. (N00104-08-A-ZF42); Small Business; (202) 204-3083
Carahsoft Technology Corporation (N00104-08-A-ZF43); Small Business; (703) 871-8583
Oakland Consulting Group (N00104-08-A-ZF44); Small Business; (301) 577-4111
Ordering Expires: 14 Sep 13
Web Links:
SAP
www.esi.mil/contentview.aspx?id=154&type=2
Advantaged
www.esi.mil/contentview.aspx?id=155&type=2
Carahsoft
www.esi.mil/contentview.aspx?id=156&type=2
Oakland
www.esi.mil/contentview.aspx?id=157&type=2

Information Assurance Tools

Data at Rest (DAR) 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 to include approved U.S. thumb drives. All products use cryptographic modules validated under FIPS 140-2 security requirements and have met stringent technical and interoperability requirements.

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

Service component chief information officers (CIO) are developing component service-specific enterprise strategies. Accordingly, customers should check with their CIO for component-specific policies and strategies before procuring a DAR solution.

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

Mobile Armor – ***MTM Technologies, Inc.*** (FA8771-07-A-0301)
McAfee – ***Rocky Mountain Ram*** (FA8771-07-A-0302)
Information Security Corp. – ***Carahsoft Technology Corp.*** (FA8771-07-A-0303)
McAfee – ***Spectrum Systems*** (FA8771-07-A-0304)
SafeNet, Inc. – ***SafeNet, Inc.*** (FA8771-07-A-0305)
Encryption Solutions, Inc. – ***Hi Tech Services, Inc.*** (FA8771-07-A- 0306)
Checkpoint – ***immix Technologies*** (FA8771-07-A-0307)
SPYRUS, Inc. – ***Autonomic Resources, LLC*** (FA8771-07-A-0308)
WinMagic, Inc. – ***Govbuys, Inc.*** (FA8771-07-A-0310)
CREDANT Technologies – ***Intelligent Decisions*** (FA8771-07-A-0311)
Symantec, formerly GuardianEdge Technologies – ***Merlin International*** (FA8771-07-A-0312)
Ordering Expires: 14 Jun 12 (If extended by option exercise.)
Web Link: www.esi.mil

McAfee (formerly Securify)

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

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

Ordering Expires: 04 Jan 11 (BPA will be extended to 31 May 11.)

Web Link: www.esi.mil

Symantec

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

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

Ordering Expires: 31 May 11

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

Symantec Antivirus:

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

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

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

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

Websense (WFT)

Websense – Provides software and maintenance for Web filtering products.

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

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

Ordering Expires: 31 Aug 11

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

Xacta

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

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

Ordering Expires: 24 Sep 14

Web Link: https://esi.telos.com/contract/overview/default.cfm

Lean Six Sigma Tools

iGrafx Business Process Analysis Tools

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

Contractors:

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

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

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

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

Ordering Expires: 31 Jan 14

Web Links:

Softchoice
www.esi.mil/contentview.aspx?id=118&type=2
Softmart
www.esi.mil/contentview.aspx?id=117&type=2
SHI
www.esi.mil/contentview.aspx?id=123&type=2

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: www.esi.mil/contentview.aspx?id=73&type=2

PowerSteering

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

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

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

Ordering Expires: 14 Aug 13

Web Link: www.esi.mil/contentview.aspx?id=145&type=2

Office Systems

Adobe Desktop Products

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

Contractors:

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

CDW Government, LLC (N00104-08-A-ZF34); (703) 621-8211

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

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

Ordering Expires: 30 Jun 12

Web Links:

Adobe Desktop Products
www.esi.mil/agreements.aspx?id=52
Dell
www.esi.mil/contentview.aspx?id=53&type=2
CDW-G
www.esi.mil/contentview.aspx?id=52&type=2
GovConnection
www.esi.mil/contentview.aspx?id=33&type=2
Insight
www.esi.mil/contentview.aspx?id=54&type=2

Adobe Server Products

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

Contractor:

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

Ordering Expires: 14 Jan 14

Web Link: www.esi.mil/contentview.aspx?id=186&type=2

Microsoft Products

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

Contractors:

CDW Government, LLC (N00104-02-A-ZE85); (888) 826-2394

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

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

GTSI (N00104-02-A-ZE79); (800) 999-GTSI ext. 2071

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

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

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

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

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

Ordering Expires: 31 Mar 13

Web Link: www.esi.mil/agreements.aspx?id=173

Red Hat/Netscape/Firefox

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

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

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

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

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

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

Download Site: http://redhat.augustschell.com

Ordering Expires: 14 Mar 11

All downloads provided at no cost.

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

Red Hat Linux

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

Contractors:

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

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

Ordering Expires:

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

Web Link: www.esi.mil

Operating Systems

Apple

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

Contractor: ***Apple, Inc.*** (HC1047-08-A-1011)
Ordering Expires: 10 Sep 11
Web Link: www.esi.mil

Sun (SSTEW)

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

Contractor: ***Dynamic Systems*** (DCA200-02-A-5011)
Ordering Expires: Dependent on GSA schedule until May 31 2011
Web Link: www.disa.mil/contracts/guide/bpa/bpa_sun.html

Research and Advisory BPA

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

Gartner Group (N00104-07-A-ZF30); (703) 378-5697; Awarded 01 Dec 2006
Ordering Expires: Effective for term of GSA contract
Authorized Users: All DoD components. For the purpose of this agreement, DoD components include: the Office of the Secretary of Defense; U.S. Military Departments; the Chairman of the Joint Chiefs of Staff; Combatant Commands; the Department of Defense Office of Inspector General; Defense Agencies; DoD Field Activities; the U.S. Coast Guard; NATO; the Intelligence Community and Foreign Military Sales with a letter of authorization. This BPA is also open to DoD contractors authorized in accordance with the FAR Part 51.
Web Link: www.esi.mil/contentview.aspx?id=171&type=2

Department of the Navy Agreements

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

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

This license is managed by the Space and Naval Warfare Systems Center (SPAWARSYSCEN) Pacific. 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: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

Data at Rest Solutions BPA Navy Agreement only

The DON CIO has issued an enterprise solution for Navy users purchasing DAR software. Visit the DON CIO website at www.doncio.navy.mil and search for "Data at Rest" to read the new policy. The DON awarded MTM Technologies a BPA for purchase of the DON Mobile Armor software bundle. For Navy users, all purchases of DON enterprise DAR solutions must be executed through the enterprise BPA, which can be found on the ESI website at www.esi.mil/contentview.aspx?id=131&type=2. Procurement of other DAR solutions for Navy users is prohibited.

Navy Enterprise BPA for DAR Users:
Mobile Armor – ***MTM Technologies, Inc.*** (N00104-09-A-ZF30)
Web Link: www.esi.mil/contentview.aspx?id=131&type=2

NEED HELP?

CONTACT THE PROJECT MANAGERS BELOW FOR ASSISTANCE

PROGRAM MANAGER
HANK INGORVATE

ORACLE (DEAL-O) NAVY PROJECT MANAGEMENT
MIKE EBERZ

MICROSOFT PRODUCTS
RENÉE ROTHLEIN

IGRAFX, RESEARCH AND ADVISORY BPA, SAP
NINA DIEP

ADOBE DESKTOP PRODUCTS, ADOBE SERVER PRODUCTS, ENTERPRISE APPLICATION INTEGRATION, SUN SOFTWARE
SUSAN ELLISON

MINITAB, POWERSTEERING, RWD TECHNOLOGIES, PLANET ASSOCIATES
THAO VU

MTM TECHNOLOGIES NAVY PROJECT MANAGEMENT
LAUREN JOHNSON

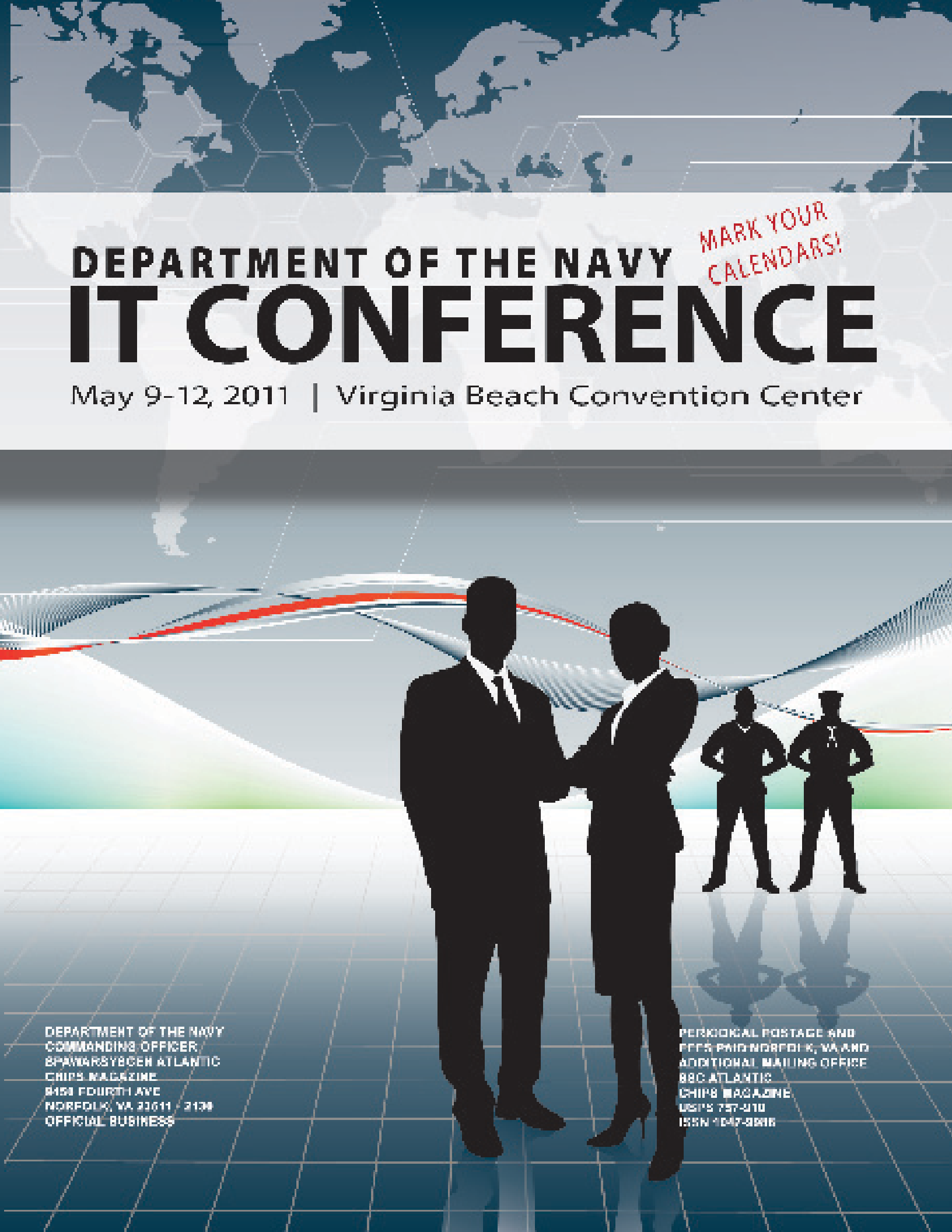
ALL ENTERPRISE CONTRACT INFORMATION HAS BEEN CONSOLIDATED UNDER
WWW.ESI.MIL
FOR YOUR TECHNOLOGY NEEDS

WWW.CHIPS.NAVY.MIL

WWW.DONCIO.NAVY.MIL

ENTERPRISE COST $AVINGS ARE JUST A CLICK AWAY

VISIT OUR E-COMMERCE SITE - WWW.ITEC-DIRECT.NAVY.MIL


DEPARTMENT OF THE NAVY
IT CONFERENCE
MARK YOUR CALENDARS!
May 9-12, 2011 | Virginia Beach Convention Center
DEPARTMENT OF THE NAVY
COMMANDING OFFICER
SPAWARSYSCEN ATLANTIC
CHIPS MAGAZINE
9456 FOURTH AVE
NORFOLK, VA 23511 - 2138
OFFICIAL BUSINESS
PERIODICAL POSTAGE AND
FEES PAID NORFOLK, VA AND
ADDITIONAL MAILING OFFICE
SSC ATLANTIC
CHIPS MAGAZINE
USPS 757-010
ISSN 1047-9988