Sharing Information – Technology – Experience

CHIPS

April - June 2010

Information Dominance

Interviews with VADM Jack Dorsett, DON CIO Rob Carey, VADM Barry McCullough, ADM James Stavridis, and VADM H. Denby Starling

CHIPS
April – June 2010 | Volume XXVIII Issue II

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

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

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

Senior Editor
Sharon Anderson

Assistant Editor
Nancy Reasor

Layout and Design
Sharon Anderson

Web Support
Tony Virata
DON IT Umbrella Program

Columnists
Sharon Anderson, Michele Buisch
Robert J. Carey
Tom Kidd, Steve Muck

Contributors
Eric Carr, DON CIO Graphics
Lynda Pierce, DON CIO Communications
Holly Quick, SPAWARSYSCEN Atlantic

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

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

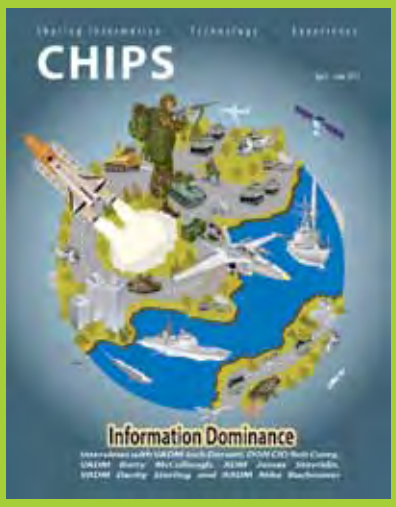
Submit article ideas to CHIPS at chips@navy.mil. We reserve the right to make editorial changes. All articles printed in CHIPS become the sole property of the publisher. Reprint authorization will be granted at the publisher's discretion.

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

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

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

Cover



The Chief of Naval Operations has positioned the Navy to take a strategic role in the information/cyber domain by realigning the Navy's intelligence and cyber assets in the stand up of the Deputy Chief of Naval Operations for Information Dominance (N2/N6); establishment of the Information Dominance Corps, U.S. Fleet Cyber Command/U.S. 10th Fleet; realignment of Naval Network Warfare Command's man, train and equip functions to the newly established Cyber Forces Command; and the elevation of the information/cyber domain as a main warfighting battery. Interviews with top Navy leadership discussing the cyber mission begin on page 6.

Chief of Naval Operations Adm. Gary Roughead approved the Information Dominance Corps warfare insignia Feb. 19 for wear by officers and enlisted personnel who complete a rigorous personal qualification program. The qualification requirements will be outlined in a forthcoming Navy instruction.

The Information Dominance Corps will consist of more than 44,000 active and Reserve Navy officers, enlisted and civilian professionals who possess extensive skills in information-intensive fields to develop and deliver dominant information capabilities in support of U.S. Navy, joint and national warfighting requirements. These fields include information professional officers, information warfare officers, naval intelligence officers, meteorological and oceanography officers, space cadre officers, aerographer's mates, cryptologic technicians, intelligence specialists, information systems technicians and civilian personnel.

The insignias will be available for purchase at Navy Exchange Uniform Centers and Navy Exchange Uniform Support Centers by August 2010.

Navigation Guide

Featured Interviews with

In Every Issue

From the DON CIO

Information Dominance/Cyber

SAN DIEGO (Feb. 3, 2010) Under Secretary of the Navy, the Honorable Robert O. Work, speaking at the Cyber/IT Workforce Town Hall, part of the Department of the Navy Information Technology Conference, held at the San Diego Convention Center, Feb. 1-4, 2010. The DON IT Conference provides opportunities to exchange information with colleagues, learn about DON IT policies and programs and ask questions of DON CIO leadership and subject matter experts. Photo courtesy of AFCEA International.

Editor's Notebook

While pundits and blogs have been buzzing about the direction the Navy should take in cyber operations, the Chief of Naval Operations strategically realigned Navy missions and organizations to achieve information dominance. This issue explores the CNO's vision in a series of interviews with several of the Navy's top leaders in this emerging warfare domain.

Acting on the CNO's cyber mandates, the Navy is now positioned "at or near the front of the pack" to assist U.S. Cyber Command when it is established, said Vice Adm. Barry McCullough, commander of FLTCYBERCOM/10th Fleet.

There is an ongoing international cyber discussion as well. Adm. James Stavridis, Supreme Allied Commander Europe and commander for U.S. European Command, calls this domain the "Cyber Sea" — a largely complex and ungoverned environment that can be used for "strategic connection" for good but too often is used by "bad actors," ruthless predators and rogue nation-states for espionage and other malicious purposes. The admiral envisions global cooperation and agreed-upon rules and standards, similar to the Law of the Sea Treaty, to chart the course in navigating the Cyber Sea.

At the same time, Stavridis is an indefatigable social media user because of its power to reach out to many people, not only to inform them, but to bring them together to work on the issues facing the global community.

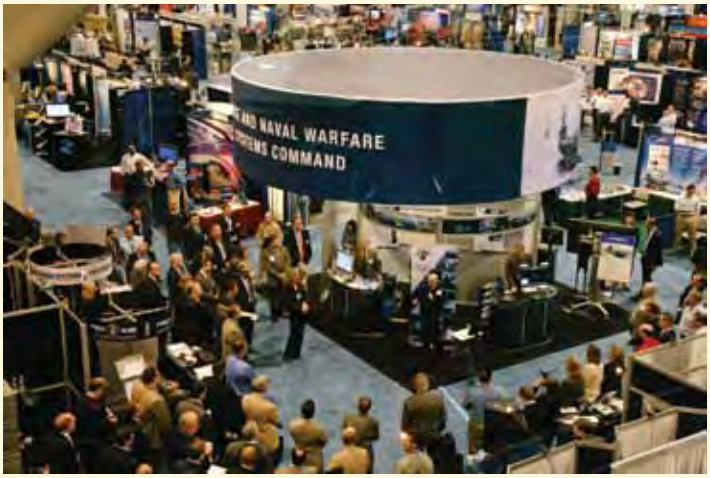
I hope this information dominance/cyber issue will spark debate and discussion with your colleagues and in the larger Defense Department community. The departments of the Navy and Defense must work collaboratively with public, private and international entities to secure cyberspace and America's cyber assets. In fact, national security leaders are counting on your ideas and help to preserve "America's digital infrastructure — the backbone that underpins a prosperous economy and a strong military and an open and efficient government," the president said in May 2009.

In February, the CHIPS staff participated in the Space and Naval Warfare Systems Command booth at West 2010, co-sponsored by AFCEA International and the U.S. Naval Institute. SPAWAR leadership and subject matter experts played a leading role in panel discussions throughout the West conference, as well as the DON Information Technology Conference, which was held at the same time and location as the West conference.

Welcome new subscribers!

Sharon Anderson

FT. MEADE, Md. (Jan. 29, 2010) Chief of Naval Operations (CNO) Adm. Gary Roughead salutes Vice Adm. Barry McCullough, commander of U.S. Fleet Cyber Command and U.S. 10th Fleet, at the commissioning ceremony for U.S. Fleet Cyber Command at Ft. George G. Meade, Md. U.S. Navy photo by Mass Communication Specialist 1st Class Tiffini Jones Vanderwyst.



SAN DIEGO (Feb. 4, 2010) Aerial view of the Space and Naval Warfare Systems Command exhibit at West 2010, co-sponsored by AFCEA International and the U.S. Naval Institute. SPAWAR Commander Rear Adm. Michael C. Bachmann is speaking in the center of the SPAWAR exhibit. Bachmann was just one in a series of distinguished Team SPAWAR speakers who gave presentations at the SPAWAR exhibit. Photo courtesy of AFCEA International.

SPAWAR Commander Rear Adm. Michael C. Bachmann speaking at the SPAWAR exhibit. Photo by Holly Quick/SPAWARSYSCEN Atlantic.

MESSAGE FROM THE

DON CIO

22 March 2016 Horn of Africa: A human intelligence source reports unexpected hostile activity near a recently deployed Marine Expeditionary Unit. The report is published to a shared network space accessible to all U.S. Central Command components and alerts a Navy collection manager based on pre-established criteria. He immediately finds a network device and consults a dynamic library of intelligence data and requests priority surveillance by air and space resources in the area, which had previously registered their services and availability on the network. One of these assets, an Air Force autonomous unmanned vehicle (AUV) (read more about the AUV in the article: Full Spectrum: Unmanning Unmanned Systems in this issue), provides visual confirmation of the threat and targeting information to the network.

At this point several firing units in theater, including Navy vessels in the Red Sea and the Gulf of Aden, which are tracking the information flow, indicate their availability, while Marine commanders on the ground are notified of the threat. Based on established attack criteria, a decision to fire is made. Battle damage assessments (BDA) from the fired munitions are then correlated with BDA from the AUV and reported back to the firing unit, Marine commanders and theater combatant commanders and published to the network for future retrieval and reference.

Information has power, and those that can harness its capabilities will take the "high ground" in future battles. With formation of the Deputy CNO for Information Dominance (N2/N6) and the stand up of Fleet Cyber Command/U.S. 10th Fleet, as well as Marine Forces Cyber Command, information management and information warfare are taking their rightful place as a core warfighting capability of the Department of the Navy. Critical to the success of the Navy and Marine Corps is the capability to publish and consume information to support warfighting decisions at will. The Navy termed this outcome "information dominance" which is the focus of this issue of CHIPS. But what is it? I believe simply it's about providing any information, to any device, anywhere, at any time giving us the freedom to quickly identify, counter or defeat any threat.

Information has power, and those that can harness its capabilities will take the "high ground" in future battles.

To meet this challenge, the DON is moving rapidly forward on the Naval Networking Environment (NNE~2016), the department's path to information dominance and an information advantage.

The NNE~2016 is a multifaceted strategy which includes moving toward a more homogeneous network architecture, a more agile decision making process that provides for unity of command, a consistent computer network defense and information assurance architecture, and an enterprise approach to provisioning, which will reduce the costs of operation. In addition, we will develop and deploy information/knowledge management strategies to enable better decision making from anywhere on the network.

We are working toward the implementation of DoD's Enterprise User concept, which is at the heart of NNE's ability to provide secure, rapid and seamless, on-demand, on-the-go, ubiquitous access to information, for all authenticated DON users. Additionally, we are actively and aggressively reducing our excepted and legacy network footprints across the department. Simply put, NNE is central to our ability to enable information dominance and complete our naval mission.

The future landscape of conflict is unknown, but as we lay the groundwork for information dominance now and in the future, we know it must not be static. The NNE must evolve and adapt to meet warfighter objectives and new missions that we will be asked to undertake.

The NNE must support naval operations across the full width and depth of the joint battlespace: from the seabed to air and space, from deep blue waters to operational objectives ashore, from a forward-deployed Marine Air-Ground Task Force (MAGTF) and strike groups on the scene of a developing crisis, to reach-back centers in the United States. It must provide seamless access from ship, shore/garrison or tactical environments to the network via both the information and cyber domains.

Today and tomorrow, we know that to defeat the enemy we must manage information better than our adversaries do. We must evolve not only our technologies to accommodate better information flow but also evolve the way we view information. We must move from a mindset of "need to know" to "need to share" so that every Sailor and Marine, no matter where they are, has the information they need to execute their mission successfully. This is information dominance.

– Robert J. Carey

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

Talking with Vice Adm. Jack Dorsett
Deputy Chief of Naval Operations for Information Dominance
Director of Naval Intelligence


Vice Adm. Jack Dorsett

In July 2009, the Chief of Naval Operations directed the establishment of a new directorate on the OPNAV staff, Deputy Chief of Naval Operations (DCNO) for Information Dominance (N2/N6). The directorate was formally established on Nov. 2, 2009, following Senate confirmation of Vice Admiral Jack Dorsett as the DCNO for Information Dominance. Vice Adm. Dorsett serves concurrently as Director of Naval Intelligence (DNI).

The establishment of N2/N6 represents a landmark transition in the evolution of naval warfare, designed to elevate information as a main battery of the Navy's warfighting capabilities, and firmly establishes the U.S. Navy's prominence in intelligence, cyber warfare and information management.

On March 23, 2010, CHIPS asked Vice Adm. Dorsett to talk about how information dominance will be operationalized in the Navy and how the stand up of N2/N6 improves the Navy's warfighting ability in this new warfare domain.

CHIPS: Many have used the terms information dominance and information superiority interchangeably. Is there a distinction and does N2/N6 have a definition?

Vice Adm. Dorsett: We do have a definition. When we talk in terms of information dominance we talk about information dominance over potential adversaries. We don't talk in terms of information superiority; in the Navy, we say decision superiority — that is a function that we want our operational commanders to enjoy.

Information dominance is achieved when every platform becomes not just a platform but also a sensor, the sensors are all networked, and our ability to command and control is better than that of potential adversaries. So you can become dominant either for a long period of time or for a short period of time and space depending on how you employ your information capabilities.

The term 'decision superiority' is relatively well-understood in the joint world. Decision superiority is achieved when the decision maker has the right information in a timely manner that permits the commander to decide and take the right action.

In the Navy, when we talk about information dominance and decision superiority, we talk about a competitive advantage that we have today, and we want to strive to retain that competitive advantage.

CHIPS: When you say the commander's decision superiority ability, what level of operations are you talking about?

Vice Adm. Dorsett: All levels, and it's not just the commander. It's the operational forces — anybody who is going to need access to some form of information, whether it is the daily weather report or it's the intention of an adversary — individuals need to have access to the information they need to take action. In some cases, it is aviators who need to avoid a thunderstorm. In other cases, it is a battleforce commander, a fleet commander, who needs to maneuver the fleet as part of the joint force.

CHIPS: Is information dominance realistically achievable as it is in the other domains — air, space, surface and subsurface warfare?

Vice Adm. Dorsett: I think it is, and I have two examples from history. One is related to cyber and the other to signals intelligence. The first one was during the Shenandoah Valley Campaign of 1862 when Stonewall Jackson had superior knowledge of the operating environment. He knew the Shenandoah Valley, he knew the lines of communication, he had local knowledge of maneuver options — and he also possessed a network of spies. So that knowledge of the environment and the adversary, the Union forces, gave Stonewall Jackson what I would call information dominance in his day.

More close to home, during World War II when the U.S. Navy was breaking the Japanese naval codes we were able to understand the Japanese Navy's plans, their actions and their intentions, in many cases, before they took action — that gave us information dominance. While those codes we broke were largely on high frequency communications, it is very similar to the issue of maintaining dominance in the cyber arena. The challenges today are a little more difficult, but it is still the electromagnetic spectrum; it's still information that we are either protecting or trying to gain access to and exploit.

I do think we can achieve information dominance; it's probably easier to maintain that dominance for shorter periods of time and over specific networks because like ourselves our potential adversaries are always thinking about how to overcome our defenses.

CHIPS: Retired Vice Adm. John Michael McConnell, former director of national intelligence, told the Senate Commerce Committee at a hearing Feb. 23 that the United States was the "most vulnerable" target for a massive, crippling cyber attack, primarily because the country is also "the most connected" to the Web, and that if the U.S. were in a cyber war today, we would lose. Would you agree?

Vice Adm. Dorsett: I think that it is more complex than that.

We are the most connected, networked nation on earth. But because we are so connected, because we are so open with our networks; the U.S. is more vulnerable to cyber attacks than closed societies. Our adversaries, at least some of our adversaries, are eroding what I think are some of our longstanding warfighting advantages by leveraging low cost capabilities to disrupt — or potentially deny our communications. So I do think in some respects, we are in a war; our networks are being probed and penetrated on a daily basis. We haven't seen truly crippling attacks on our networks, but I grow increasingly concerned about the defenses of our networks.

CHIPS: When it comes to policy and law in regard to waging cyber warfare and defending against it and prosecuting those who engage in it — does the Navy have sufficient higher level guidance and room to maneuver in this new domain?

Vice Adm. Dorsett: I think we have enough guidance to take the steps that we are taking. We do have enough guidance to organize, to move out with other organizations in the Department of Defense, but I don't believe we have all of the right laws or policies for the long term. We are still using what I call Industrial Age mindsets, and we are still using those pre-information era laws and policies, so it is really important for the lawyers and the policy makers to be thinking through how the policies and law need to evolve.

> "We are in the midst of a national dialogue at the moment regarding how we protect both our networks and, at the same time, protect our civil liberties. I don't think that dialogue has concluded, and I would expect in the years ahead a greater clarity of thought and precision in the development of additional laws and policies."

We are in the midst of a national dialogue at the moment regarding how we protect both our networks and, at the same time, protect our civil liberties. I don't think that dialogue has concluded, and I would expect in the years ahead a greater clarity of thought and precision in the development of additional laws and policies.

CHIPS: In a nutshell, the need for actionable intelligence delivered to the right organization at the right time seems to be the overarching mandate for N2/N6. Is this a fair assessment — or is your mandate much broader?

Vice Adm. Dorsett: This is the mandate for the Information Dominance Corps, the professionals who deal with information in the Navy. But in addition to actionable intelligence, they need to provide assured communications, and that means communications and networks that are defended, and that commanders and operating forces can use them.

In terms of N2/N6's mandate, I think actionable intelligence is just one aspect of the job. I think the larger mandate that the CNO has given me is to take a holistic approach to how we manage and resource the Navy's information capabilities. Part of that is he has asked us to develop new concepts, new strategies, and more improved architectures that will, in essence, chart our course for the future — that will break down barriers — and ultimately deliver much more robust information capabilities for the Navy.

These barriers include the platform-focused manner in which the Navy procures its warfighting capabilities. For years we have procured our platforms — ships, submarines and aircraft — with an eye to their weapons and weapons delivery systems. We then built our warfighting capabilities around those platforms. Unfortunately, communications, networks, intelligence, and other information-based capabilities that were critical to the effective employment of those platforms were secondary considerations.

Today, we need to retool our programming and acquisition process, and seek capabilities-based solutions. We need to look across all platforms and ensure we are delivering fully integrated solutions. Our objective is for every platform to be a sensor, for every sensor to be networked, and for every shooter to be capable of using data derived from any sensor.

CHIPS: Can you talk about N2/N6's responsibility to "boldly introduce game-changing strategies and concepts"? Does this mean that the Navy hasn't been bold enough in the past or too risk averse to take a leap of faith in new ideas or breaking down old paradigms?

Vice Adm. Dorsett: Let me answer that in two ways. First, the Navy is not risk averse at all. I think we have a history and tradition over the last 100 years of being innovative. We introduced naval aviation in between World War I and II, and really prepared ourselves for World War II — pretty innovative moves at the time.

In the 1950s, we introduced nuclear power. I think that was extremely bold, shifting from steam to nuclear power.

Most people don't realize that back in the 1960s, the U.S. Navy operated more than 700 unmanned aerial vehicles from our surface ships — that was hardly risk averse at the time. What we found though is that the technology was very immature for those UAVs, and we lost an awful lot of them because the control mechanisms didn't work well. So the Navy went away from using UAVs for about four decades, and now, with advanced technology, we are starting to embrace unmanned capabilities again.

The other thing I would say, especially in the cyber arena, [now deceased] Vice Adm. Art Cebrowski was one of the leading thinkers in net-centric warfare. He, and many others, wrote about and led the development of the netted warfighting concept. Those writings and that dialogue that occurred in the mid-1990s basically set us in great shape for where we are today.

In terms of our unmanned capabilities and our net-centric or cyber capabilities, we, along with the other services, have been focused on Iraq, Afghanistan and other hot spots over the last 10 years, and while it may look like we didn't take advantage of opportunities, I think there was a confluence of many different events in the last couple of years that have permitted us to really jump forward. Adm. Roughead, when he made his decisions, said we are going to go very bold; we aren't going to take any half steps. So I think you are seeing the Navy taking bold steps in both information and unmanned capabilities.

CHIPS: Can you talk about the Information Dominance Corps?

Vice Adm. Dorsett: Our goal is pretty simple. In essence, my vision is to recruit, hire, educate and then retain the world-renowned,

world-class workforce in the information arena — anything less than that is underachieving. To do that, we need to change some of the processes we have for how we recruit, how we hire, and certainly we need to alter our training and education structures. Right now we train by stovepipes, our intent is to broaden, as well as deepen, the skill sets of the members of the Information Dominance Corps.

It is about getting the right people in, incentivizing them, encouraging them, giving them opportunities and building their professional skills so they are a much improved workforce over old folks like me.

CHIPS: The Navy already has a program for allowing, for example, Information Systems Technicians, to get professional certifications through Microsoft, are you talking about training beyond that?

Vice Adm. Dorsett: Here is how we operate right now. If you are a naval intelligence officer, you get trained in the business of intelligence. If you are an information professional, you get trained in network management, communications, and command and control. But neither one gets trained in the other area. So the intelligence officer is not trained in networks, nor is the information professional trained in intelligence.

It is my belief, and the CNO's, that we need professionals who understand their specific skill areas, but also they need to have a broader perspective. I talked about stovepipes and Stonewall Jackson's knowledge of the environment. Oceanographers and meteorologists in the Navy are part of the Information Dominance Corps. Oceanographers, who I believe are the best in the world, know the operating maritime environment extremely well. But they don't know networks and communications as well nor do they have the background in intelligence.

> "Developing world-class expertise across an elite group of information professionals (Information Dominance Corps), will be the means by which we earn the same reputation for excellence as the Nuclear Navy. More importantly, in the process we will revolutionize Navy warfighting capabilities."

We are trying to bridge the [knowledge] gaps between all of our information professionals, have people understand the environment, have them understand space and how space supports all of our activities, to understand the various elements of intelligence, cyber warfare, network management, and command and control. What we are asking of our future workforce is to be much more knowledgeable than they are today.

You mentioned Microsoft certifications, a certain group in the workforce need to have Microsoft certifications, other members need to be aware, and certainly the leaders need to be aware of who needs Microsoft certifications, and how to get them. A small segment of the workforce probably just needs to vaguely understand that Microsoft certifies people, but we need to do a deepening of our entire knowledge base for the Information Dominance Corps. We protect ourselves by barriers between those disciplines, and I think those barriers need to come down.

CHIPS: The Corps will need to have knowledge beyond their specialties. So beyond what Information Professional Officers are required to know as IPs, they will also need to have an overarching understanding of all the information domains in the Navy. And that is in development right now?

Vice Adm. Dorsett: Yes, it is. We are creating a common PQS, Professional Qualification Standard, across all of our disciplines. We are going to have everyone trained to that common qualification standard, and then if you are specialized; if you're an oceanographer, then you will go deep into your oceanography related qualifications. But everyone will at least have a common understanding across the information domain.

CHIPS: That's pretty exciting.

Vice Adm. Dorsett: It is. We've looked at a grandfathering approach. What happens to those folks like myself who have been in the Navy for 32 years, do we just get qualified automatically because of our past experiences? What we have chosen to do is take the high ground, and those of us who have been around awhile are going to have to take an exam to get qualified across the Information Dominance Corps.

CHIPS: Do you think it will be hard to adjust to this change for those older members in these specialized domains?

Vice Adm. Dorsett: It will be hard for some who have focused their entire career on their community or specialty skill and don't necessarily think of themselves as part of the Information Dominance Corps. I think that is probably a small minority of people; those folks will be more challenged than the young adults coming in. Young adults coming in will see the benefit of not only being specialized in one key area but then also being broadly trained across the board.

CHIPS: I talk to young ITs; they love what they are doing, and they are always eager for more training.

Vice Adm. Dorsett: Sure, and by broadening their training, there will be more career opportunities open to them than those currently in the program. That should be exciting for many folks. Other folks will be pleased just to stay in their current business line, if you will.

CHIPS: Industry will be looking at recruiting the same movers and shakers that you are interested in. Have you looked at recruiting incentives?

Vice Adm. Dorsett: Yes, there are a couple of incentives that we are looking at right now. The first incentive that the Chief of Naval Personnel came up with is to give ROTC scholarships to individuals who do well in the U.S. Cyber Challenge competitions. I understand that to do well in this competition you actually have to hack into a certain program.

From the Chief of Naval Personnel's perspective, these are the kind of people we want to draw into the Navy. He's also looking at options for bringing people into the workforce in nontraditional ways. We haven't finalized anything so it would be premature for me to give you any examples, but I would expect the Navy in the months ahead to be offering unique opportunities

that we haven't offered previously to people with cyber expertise.

CHIPS: Do you foresee the education, reputation and expertise of the Information Dominance Corps becoming on par with the elite Nuclear Navy?

Vice Adm. Dorsett: Absolutely. The creation of the Information Dominance Corps is a revolution on par with past transformations. The Nuclear Navy is an outstanding example of what we can achieve when we lean far forward and invest in the recruiting, education and training of our workforce. We are fully prepared to make the investment in our people, and their education and training, to gain the in-depth expertise we require in all information-centric disciplines. Developing world-class expertise across an elite group of information professionals, will be the means by which we earn the same reputation for excellence as the Nuclear Navy. More importantly, in the process we will revolutionize Navy warfighting capabilities.

"Our operational commanders in the Navy will view cyber perhaps as the very first arrow out of the quiver as we plan and prepare for a military operation. Instead of information just being a supporting function, information will be a main battery of the Navy. I think that isn't only our goal — but we will actually be there in five years."

CHIPS: Can you talk about how you will be working with the other service components to U.S. Cyber Command?

Vice Adm. Dorsett: I think all the services are aligning themselves up appropriately and effectively for supporting the U.S. Cyber Command.

All of the services have had discussions with the prospective Cyber Commander, Lt. Gen. Keith Alexander, and we have all presented our plans for how we are going to organize, how we are going to provide forces, and how we are going to work. The U.S. Cyber Command, the pre-organization, has started to develop a concept of operations, and they brought in all of the services in the meetings so we are all doing that together. I'm very pleased that this is truly a joint DoD-wide approach.

Our relationship with the other service component commanders will be run through Vice Adm. McCullough who is the Fleet Cyber Command/10th Fleet commander. He will be the primary conduit conducting operational cyber activities for the Navy; he is already located in Fort Meade, Md., the prospective home of the U.S. Cyber Command, so I think we have set ourselves up for success in that regard.

CHIPS: At the 2010 West conference in San Diego, Adm. Roughead said that the Navy's cyber mission is still evolving and there is much work to be done with 10th Fleet in the lead. Where do you hope the Navy will be in a year from now — and five years from now in regard to cyber warfare and working effectively in this new domain?

Vice Adm. Dorsett: A year from now, our Fleet Cyber Command will be fully operational; it will not just be organizing itself, which is where it is right now. It will be focused on actual planning cyber defenses and cyber operations as a component to the U.S. Cyber Command. I believe the Fleet Cyber Command will have an improved management capability over our operations. Its subordinate command, Naval Network Warfare Command, which is responsible for network management, network ops, network defense, will have more enhanced Host Based Security System (HBSS) software and procedural protections in place a year from now. In terms of our programs, a year from now, we will have provided additional funds to fix some shortfalls in our networks and command and control capabilities. In a year you can't do a tremendous amount, but we will be headed in the right direction.

In a year from now, our most significant improvement will be in our Information Dominance Corps professionals. I mentioned a few of the initiatives we have [for the workforce]. I think we will look at ourselves dramatically different than we do today. We will be viewed as warfare professionals with a rigorous training and qualification program.

Probably several dozen of our officers will have been assigned in key billets across the information disciplines. There are about 25 officers that we are reassigning right now. If you are an intelligence officer, you are moving to a cyber job. If you are a cyber officer, you are perhaps moving into a signals intelligence job. In a year from now we will have made significant progress [in crossing training].

Five years from now, our goal is to be viewed as the nation's premier cyber organization, that we will be viewed as full partners with the other services, and the key component to U.S. Cyber Command. We aren't competing with the other services; we set our standards high so I think that is the appropriate goal to have.

I think the Fleet Cyber Command will be conducting complex cyber activities five years from now. Our operational commanders in the Navy will view cyber, perhaps, as the very first arrow out of the quiver as we plan and prepare for a military operation. Instead of information just being a supporting function, information will be a main battery of the Navy. I think that isn't only our goal — but we will actually be there in five years.

CHIPS: Do you have any other comments?

Vice Adm. Dorsett: You've mentioned it — this is exciting. These are extremely exciting times not just for the Navy but across the Department of Defense — whether it is the investments we are making in cyber, whether it's the Navy partnering with the Air Force for some unmanned capabilities, or the information management and technologies that we are putting out on the battlefield in Afghanistan today.

The flow of information has never been more important for the nation. The ability for us to network and deliver Information Age capabilities is truly exciting. The people in the information profession, especially in the Navy, are tremendously excited about the opportunities these days. CHIPS

For Vice Adm. Dorsett's biography and more Navy news, go to www.navy.mil.

Talking with Vice Admiral Bernard J. "Barry" McCullough III Commander, U.S. Fleet Cyber Command/ Commander, U.S. 10th Fleet

Vice Adm. Barry McCullough

Vice Adm. Barry McCullough, as the commander for U.S. Fleet Cyber Command/ U.S. 10th Fleet, will put into action the Chief of Naval Operations Adm. Gary Roughead's vision for a whole-warfighting approach to how the Navy operates its combat capabilities in the information/cyber domain with the ultimate goal of warfighting dominance across the full spectrum of operations at sea, under the sea, in the air, in the littorals, and in the cyberspace and information domains. CHIPS talked with Vice Adm. McCullough March 29.

Vice Adm. McCullough: The Navy has a vision to move out on cyber operations to include network and space operations; electronic warfare; signals intelligence; and other information operations. The CNO has invested a lot of his own time in this and has given Vice Adm. Starling, Vice Adm. Dorsett and me the gateway to take the Navy forward in this new operational domain. I look at it as an operational domain that's global, similar to the way we look at the undersea warfare, air warfare and surface warfare domains.

CHIPS: Can you talk about your short and long-term goals?

Vice Adm. McCullough: The first thing I did was to look at what the CNO told us to do. That was the vision that we laid out for dominance in cyber operations, signals intelligence, information operations, electronic warfare and space. I had to get my arms around where we were and what we had. So, I visited most of the major Navy Information Operations Commands and telecommunication facilities around the world to see what the state of play was. I visited 20 of my 24 subordinate commands and established the baseline. The predecessors at Naval Network Warfare Command — Vice Adm. Mayo, Vice Adm. McArthur and Vice Adm. Starling — have invested a tremendous amount of effort to define this new domain. They put us in the position to launch toward the Navy's vision.

The Navy has outstanding signals intelligence capabilities. We also have a sound electronic warfare program, specifically with aviation capacity. We need to do some work on what we have in surface warfare, but we have a relatively sound foundation there. Therefore, my initial focus is on networks and the ability to command and control our forces globally. How do we get from static and reactive network operations and defense to proactive and dynamic? My first near-term goal is to establish dynamic cyber operations, which includes defense, as well as exploitation and development of non-kinetic effects. When U.S. Cyber Command is established we will get more defined direction, as Fleet Cyber Command will be the Navy's component command to USCYBERCOM.

The Department of Defense has consolidated network warfare: Joint Functional Component Command Network Warfare (JFCC-NW), and global network operations, Joint Task Force-Global Network Operations (JTF-GNO), and JTFs (Joint Task Forces) — into a consolidated staff that works for Lt. Gen. Alexander now. I have spent some time with him, and I think our visions are aligned.

CHIPS: How many personnel are in FLTCYBERCOM/10th Fleet and what billets do you have?

Vice Adm. McCullough: Right now, a little less than 100. The initial size of the staff is to be about 182, with a mix of cryptologists, information operations professionals, intelligence specialists and line officers.

CHIPS: Can you talk about the Information Dominance Corps?

Vice Adm. McCullough: Vice Adm. Dorsett is the community leader for those folks. We have great capability. The Navy, through its cryptologists, has some of the best linguists and network operators that are in the military service today. My concern is capacity and retention. There was a plan to add a substantial number of personnel to this community with the 2011 budget, but due to competing priorities, we got a little less than half of what we planned. We still need to increase our capacity, our personnel, in this area.

CHIPS: Navy training is the best in the world. How are you going to retain these individuals since industry will be recruiting them too?

Vice Adm. McCullough: There is a limited pool of people with the right talent base that you can recruit into this business because these are highly specialized operators. We are competing with the rest of industry for these folks. Our pay doesn't necessarily match that of private industry. We can give these young men and women early responsibility and training for them to be among the best. In the end, it is about service and responsibility to the Navy and the nation — as opposed to the financial reward. It is incumbent upon the leadership, Vice Adm. Starling, Vice Adm. Dorsett and me, and the folks that work with us, to ensure that these people understand the importance of their contributions and to develop the right workplace environment so that these people want to stay and work with us.

CHIPS: Do you anticipate dramatic changes since the CNO has directed that cyber tactics, techniques and procedures need to mature quickly?

Vice Adm. McCullough: Navy cyber defense is run through the Navy Cyber Defense Operations Command in Norfolk, and that command does an excellent job. But what we have to develop is what I call near-real-time situational awareness (SA) so we can see what is going on in the network just like we monitor an air warfare battlespace. We still have a long way to go to get there. Once we achieve near-real-time SA, and we can monitor the domain like our other warfare domains, then we need to dynamically defend the network in near-real-time.

Everybody likes to say we are going to do this at machine speed, and I believe that some of it can and needs to be executed at machine speed, but some of it has to be done with human interfaces. A human being has to be able to understand the data presented and be able to take action on it. We need to move in the direction of dynamic operations to garner intelligence and have dynamic defense. I think they are areas where we need to substantially improve.

CHIPS: Is the Navy a late starter in cyber since the Air Force has been organizing its assets for several years now?

Vice Adm. McCullough: I would say the Navy is not disadvantaged in any way. My assessment is that we are at or near the front of the pack right now. The Navy has had an historical relationship with the National Security Agency through our cryptology folks for a long time. So we have a basis for being able to conduct operations in cyberspace. We are not just starting from zero.

The formulation of Cyber Forces and Fleet Cyber Command and splitting out the man, train and equip functions to the type commander, Cyber Forces, and the operations to Fleet Cyber Command that is collocated with the consolidated staff [JFCC-NW and JTF-GNO], the National Security Agency, and the future headquarters of USCYBERCOM at Fort Meade, has put the Navy at the forefront of cyber to take advantage of our historical position and what we now have.

CHIPS: Is there room to maneuver in the cyber domain to use offensive measures and not just to defend networks?

Vice Adm. McCullough: I don't like the word offensive, I would call it non-kinetic effects, and I think there is room for that in all domains of warfare. Historically, we have looked at kinetic effects. But what can we do utilizing non-kinetics to support operational commanders' con-plans and ops? I think we need to work on that and be better at non-kinetics. The networks are common battlespaces. We are in these battlespaces and so are our potential adversaries, be they nation-states or non-nation states; everybody is living on the same networks. So we have to get to that dynamic functionality that I talked about to be better positioned to take advantage of our cyber capabilities.

CHIPS: Vice Adm. Dorsett discussed the need to integrate all the functional areas of cyber that traditionally have worked in stovepipes: intelligence, cryptology, signals intelligence, information operations, electronic warfare, oceanography, meteorology, and then cross-training these professionals for a wholly integrated approach to the cyber mission. Do you foresee any difficulty in their integration?

Vice Adm. McCullough: Inside the service, no. But the federal U.S. Codes and other statutory and regulatory authorities involved in all of this, Title 10, Title 14 and Title 50, all have specific authorities that apply to this domain. We have to make sure that we work through the proper channels to make this happen. I think it is imperative to integrate, not only within the Navy, but with interagency [organizations] as well.

CHIPS: There is a national discussion in the media and blogs about the Navy's cyber mission. Do you find the discussion useful?

Vice Adm. McCullough: Yes, I have had the opportunity to talk with several different agencies in the intelligence community as well as the services. Everybody understands what needs to be done; it is just working through the bureaucracy to make it happen.

CHIPS: You are a seasoned warrior, having worked extensively in the acquisition community. Will you be working with the program executive offices as commander of FLTCYBERCOM/10th Fleet?

Vice Adm. McCullough: Yes, I've spent some time doing that already. I will be working with the PMAs and PMWs (warfare program offices) and with the Honorable Sean Stackley (Assistant Secretary of the Navy for Research, Development and Acquisition). We need to be able to rapidly prototype and field technical capabilities. There are approved procedures to follow, and we will need Secretary Stackley and his organization's help to do this.

CHIPS: Do you have any concerns about the delay in the Navy's satellite program, MUOS, the Mobile User Objective System?

Vice Adm. McCullough: Yes, I do. The satellite infrastructure has been around for a while. We all worry about the expense and the technical capability of replacing the constellation as it ages. It is something we all need to work on, all the services, as well as the civilian agencies, to come up with a consolidated strategy to make sure we maintain our advantage in this critical area.

CHIPS: I have heard some leadership discussion about bandwidth — that there will never be enough on ships. Do you agree?

Vice Adm. McCullough: I have a different opinion on that. We have more bandwidth now than we have ever had. You can always develop more demand for bandwidth than exists, so it comes to using the bandwidth that we have to get the right information at the right time to the right place. It is about dynamic bandwidth management rather than just buying more bandwidth.

CHIPS: Is there anything else you want to talk about?

Vice Adm. McCullough: Dynamic cyber operations is a huge challenge for the Navy, and I think there is one chance to get it right — and that is now. The Navy has the right vision to put us at the forefront of this capability and capacity in this new warfare domain. CHIPS

Go to www.navy.mil for more Navy news.

Join the Discussion in the Pulse

By Michele Buisch

In February, the Department of the Navy Chief Information Officer (DON CIO) launched the Pulse, a collaborative Web site for members of the DON information management/information technology (IM/IT) community. With its launch, DON personnel have the opportunity to shape the direction of the organization.

The Pulse is a secure extension of the DON CIO Web site created to foster candid discussion and provide a venue to collaborate on current and future IM/IT initiatives. The site allows members from anywhere within the department, both geographically and organizationally, to participate in the discussion. Mr. Rob Carey, DON CIO, describes his vision for the tool as a way to "harness the intellectual capacity of the 850,000-plus men and women in the Department of the Navy."

Visitors to the site must possess a Department of Defense issued Common Access Card and a .mil e-mail address to view content. However, to participate in the discussions, a visitor must become a registered member of the Pulse.

Once registered, members may participate by posting a topic of discussion in the form of a blog. They may also join a discussion by adding a comment or indicating they like a topic of discussion. Each member's activity (posts, discussions and comments) is listed on his or her profile page.

The default view of the homepage ("What we're: Saying") displays the most recent topic postings in reverse chronological order. Members may sort the homepage by activity ("What we're: Doing") to view the latest member activities. Each topic posting shows the number of associated comments and the number of likes received.

Most Discussed and Most Liked lists are also displayed on the homepage indicating to members which topics are generating the most interest.

The categories page lists the seven categories in which the topics are "filed." The categories are:

- **If I Were CIO –** What would you focus on or do if you were CIO?
- **In My DON 2016 –** What will the department be doing by 2016? What should we be doing by 2016?
- **Clear as Mud –** What do you want clarified because it makes absolutely no sense to you?
- **Bravo Zulu –** What are we doing well? What are the programs, projects, teams, individuals, etc., that we should all know about?
- **What Keeps Me Up at Night? –** What are you most concerned about: threats, challenges, shortcomings, oversights, etc.?
- **Help! –** What do you want help with or input on from the Pulse community? Help us help you!
- **Flotsam & Jetsam –** Odds and ends, cats and dogs, sundries, miscellaneous … you get the picture.

Clicking on a specific category will display all the blogs in that category, as well as the Recent Contributors, Most Discussed and Most Liked lists for that particular category.

Posting a topic is as easy as filling out a form. Simply type in the title and the topic text, and choose a category and at least one content tag. Members may also create their own tags if they want to further define what their topic is about. There is the option to submit the post or save it as a draft. Clicking *Submit* posts the topic at the top of the homepage as the most recent submission. And that is when the discussions begin.

Once members begin participating, they will receive system notifications each time they log in if someone has commented on their post or responded to their comments on someone else's post. This allows the discussion to continue. Members also have the option to sign up for e-mail notifications if someone comments or likes their post.

There are more than 350 members from a variety of commands engaged in a number of discussions with topics ranging from the cybersecurity workforce, standards compliant browsers, being a joint organization, to the return of thumb drives. There is also a site feedback topic, in which you may provide your comments about the site and suggestions for future enhancements. CHIPS

Michele Buisch provides communications support to the Department of the Navy Chief Information Officer and is the administrator for the Pulse and the DON CIO Web site.

The CIO

AN INTERVIEW WITH MR. ROBERT J. CAREY

DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER

Federal Chief Information Officers were directed by the Information Technology Reform Act (Clinger-Cohen Act) of 1996 to address and improve information management and information technology (IM/IT) at the enterprise level.

The Secretary of the Navy established the office of the Department of the Navy Chief Information Officer in 1997 to provide department-wide leadership and advocacy in the development and use of IM/IT and to create a unified IM/IT vision for the DON as it supports the mission of the Navy and Marine Corps.

The DON CIO develops strategies, policies, plans, architectures, standards and guidance, and provides process transformation support for the entire Department of the Navy. Additionally, the DON CIO ensures that the development and acquisition of IT systems are interoperable and consistent with the department's objectives, mission and vision.

The Chief of Naval Operations stood up the Deputy Chief of Naval Operations for Information Dominance (N2/N6) Nov. 2, 2009, with Vice Adm. Jack Dorsett as the head of both N2/N6 and Director of Naval Intelligence (DNI).

The stand up of N2/N6 was quickly followed by the establishment of Marine Forces Cyber Command and U.S. Fleet Cyber Command; and re-establishment of U.S. 10th Fleet in January. These initiatives signify cyber warfare and information management/warfare as top priorities within the DON.

CHIPS asked DON CIO Rob Carey to talk about how these recent changes affect the DON CIO's objectives.

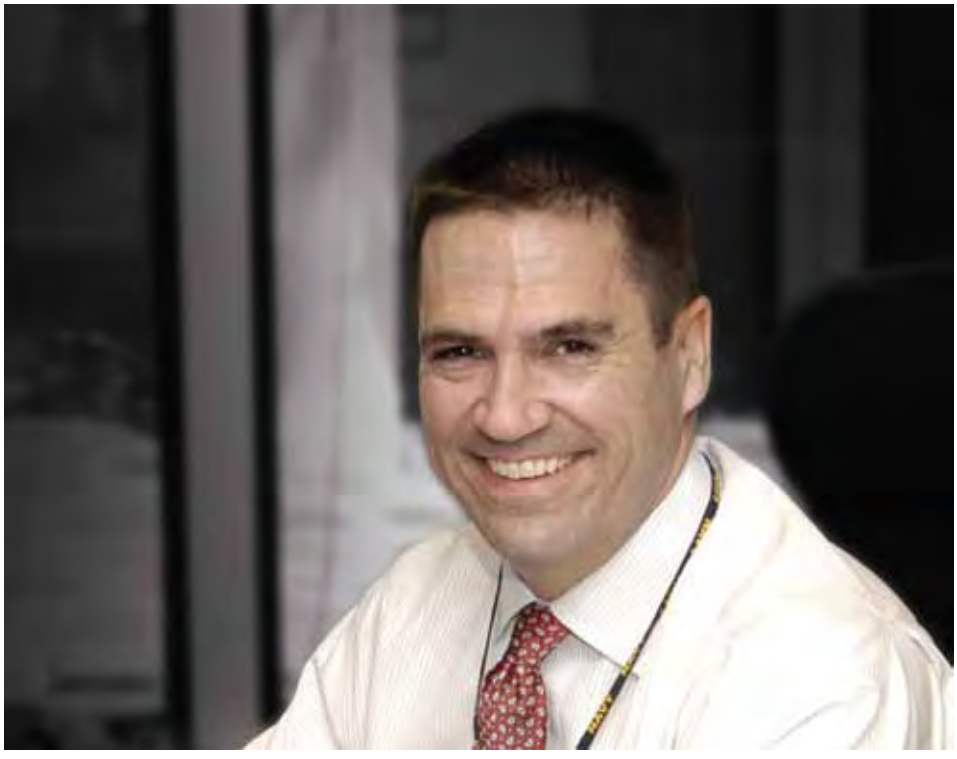
CHIPS: The DON CIO has been in the IM/IT business since 1997. Have the recent changes with the establishment of N2/N6, the Marine Forces Cyber Command, U.S. Fleet Cyber Forces Command and Fleet Forces/10th Fleet led to any organizational changes within the DON CIO? Have your priorities or objectives changed?

Mr. Carey: There have been no organizational changes within the DON CIO as a result of the establishment of these commands; however, we have accelerated our development of the Naval Networking Environment ~ 2016 strategy to ensure it supports the Navy and Marine Corps information management and cyberspace objectives.

Almost all of the work we do, ranging from cybersecurity and the future Naval Networking Environment, to knowledge management and enterprise standards support these commands.

So we embrace their establishment, as it underscores the importance the DON places on information and the security of that information as a crucial element of warfighting.

DON CIO, N2/N6, Marine Forces Cyber Command, U.S. Fleet Cyber Command and 10th Fleet all have complementary roles and we are working toward a common goal of enabling real-time decision making from anywhere with secure, accurate and actionable data.



CHIPS: How would you define information dominance?

Mr. Carey: N2/N6's working definition of information dominance is: the ability to seize and control the information domain 'high ground' when, where and however required for decisive competitive advantage across the range of Navy missions. Information dominance means freedom of action to maneuver and act in cyberspace — conduct offensive and defensive actions, kinetically and non-kinetically — at the intersection of maritime, space, information and cyberspace domains. At this intersection, Navy exploits deep penetration, expanded maneuver space and information advantage to deliver warfighting options and effects.

I believe we achieve information dominance as a byproduct of a successful development and deployment of the Naval Networking Environment. We must ensure that the network architecture supports these goals, the decision making process supports these goals, the computer network operations support these goals and the development and deployment of systems support these goals.

Without changes to broad facets of our 'system,' we will only marginally increase our decision advantage. We must get to the place where we can make decisions inside the OODA (observe-orient-decide-act) loop of our adversaries… and net-centricity is the basis of this way ahead.

CHIPS: You serve as the community leader for the DON Cyber/IT workforce and develop 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. With the N2/N6 stand up of the Information Dominance Corps, will the IM/IT workforce now become the Information Dominance Corps? Will training requirements change for the IM/IT workforce?

Mr. Carey: The Cyber/IT workforce is a key part of the Information Dominance Corps. There are other communities in the Information Dominance Corps such as intelligence, information warfare, oceanography and space cadre personnel. As the work, environment and missions change, so will training. Technical and business skills, as well as oversight and command and control skills, will also continue to evolve. The Cyber/IT workforce must constantly upgrade its skills and have the ability to adapt to changing technology and product demands through lifelong learning. Lastly, we need to ensure there is fungibility across the military, civilian and contractor communities for specific jobs because we will need flexibility and consistency across skills.

CHIPS: I've read comments from Navy, as well as DoD leadership, about the urgent need to develop a force of cyber warriors because the next 9/11 is likely to be in the form of a catastrophic cyber attack. How can the DON prepare for such an attack? Are there offensive measures that the DON can take to prevent such an attack from occurring?

Mr. Carey: The DON CIO made cybersecurity a key focus area several years ago. The foundation involves people, process and technology. All too often we jump to technology as the answer, but cybersecurity is not just about technology. A lot of it is about changing behavior and making people 'cyber warriors' — making them aware of possible threats and vigilant in protecting against them.

Central to this effort is ensuring that the 'defenders' of the network and its information are trained as attackers. In this way I believe we will be better able to provide mission assurance.

The DON's computer network defense (CND) strategy is one of defense-in-depth and defense-in-breadth across the entire life cycle to protect the department's information and information systems. The defense-in-depth strategy forces adversaries to penetrate multiple protection layers, thereby decreasing the likelihood of success. Our defense strategy is also about risk management — focusing our finite resources on the high payoff tools.

There are many additional efforts and initiatives underway in the DON to improve CND posture to prevent such an attack from occurring. They include the Host Based Security System (HBSS) to detect and counter against known cyber threats in real time; NIPRNET DMZ to add protection between internal and external networks; and Intrusion Protection Systems to monitor networks and system activities for malicious and unwanted behavior.

These are just a few of the offensive measures we are taking. The Computer Network Defense Roadmap we published last year goes into more detail (available at www.doncio.navy.mil). With our cybersecurity/IA/CND workforce, we are developing a cadre of skilled professionals who perform IA/CND/network operations functions for our information systems and networks.

CHIPS: As the DON's senior IM/IT (including National Security Systems), and information resources management (IRM) official, can you talk about how cyber threats have changed policies and processes within the DON regarding its networks and cyber assets?

Mr. Carey: As the threat has become more persistent and sophisticated, so have we. We're addressing the threat holistically, which involves changing culture, conduct and capabilities. For example, we will never go back to the days of anyone/everyone using a personal thumb drive on a DON network.

This change affects culture — knowing you can't take a thumb drive you get from a conference and plug it into a military network; it affects conduct — the thumbs drives are for mission use only; and it affects capabilities — we need to be able to technically enforce this policy. Good security hygiene starts with basics and moves outward toward the edge with the deployment of advanced network tools.

We need to make security part of the culture and a command priority. We need to change conduct by ensuring we have an adequate assessment/compliance program. We need to ensure adequate capabilities; ensuring trained personnel are assigned where they need to be and that technology is utilized smartly.

Cyber threats are constantly evolving; therefore our reactions to these threats must constantly evolve. Two policy

changes that we instituted in response to cyber threats come to mind. Mandatory annual information assurance awareness training was instituted four years ago to educate users on the threats, and how to identify and prevent them.

We also made cryptographic logon mandatory several years ago to improve the security of DON networks by eliminating reliance on usernames and passwords. We are digitally signing e-mails to address spear phishing and encrypting sensitive information to protect information in transit. We are now working to extend the protections of PKI and cryptographic logon to our classified networks.

In addition to training and individual precautions, we are also taking action at the network level. I mentioned HBSS earlier, and I think it is an important element in securing our networks. HBSS is a suite of integrated IA/CND tools that will enable system administrators or IA/CND operators to maintain up-to-date protection, configure/enforce protection policies, create asset baseline configurations, monitor a system's security and compliance status, and detect rogue systems operating on the network at the host machine level.

HBSS will also provide application monitoring with both whitelist and blacklist capability. Security is an ever-evolving process as new threats are continuously emerging; however, by taking the precautions above, we significantly reduce the impact on our networks.

CHIPS: Can you provide an update on the DON CIO's work regarding the Next Generation Enterprise Network (NGEN) planning?

Mr. Carey: The NMCI contract ends on Sept. 30, 2010, and the transition to NGEN begins in earnest on Oct. 1, 2010. However, October will not see a spike in network capability; rather we believe it will be a seamless and almost boring event. It will be the beginning of a transition with plans for continued incremental capability growth in our largest network environment. The first element of this transition is a continuity of services contract which is being negotiated with EDS, our NMCI partner, to bridge the timeframe between the end of the NMCI contract and the competitive award of the NGEN contract (or contracts).

We are working on the early transition activities (ETAs) with both the Navy and Marine Corps to lay the groundwork for NGEN. These ETAs are key enablers for the overall success of this transition to NGEN. The ETAs will establish government management capabilities, allow greater participation in operational decisions, reduce risk, help expedite transition time, and provide the foundation for full and open competition for services. Also, the NGEN Acquisition Strategy is currently in review and provides the acquisition roadmap for NGEN's successful implementation.

The DON CIO, Program Executive Office for Enterprise Information Systems, and NGEN System Program Office (SPO) are focused on ensuring a smooth transition from NMCI to NGEN, with the goal of achieving the NNE~2016 vision.

THE INFORMATION AGE DEMANDS THAT WE POSSESS THE ABILITY TO MAKE DECISIONS AT NETWORK SPEED, AND OUTMANEUVER OUR ENEMIES

CHIPS: Can you talk about department progress toward the Naval Networking Environment ~ 2016?

Mr. Carey: We are making a lot of progress, and there are many initiatives underway that are furthering our vision for the Naval Networking Environment. We have defined our future as:

A Department of the Navy net-centric environment that securely leverages the full range of information resources enabling rapid, on-demand, ubiquitous access to authenticated users and systems in support of the Joint enterprise environment and all Navy and Marine Corps strategic, operational, and tactical missions.

Efforts in this area include: the stand up of NGEN, Consolidated Afloat Networks and Enterprise Services (CANES), Marine Corps Enterprise Network (MCEN) and Marine Air Ground Task Force Command and Control (MAGTF C2) concept, as well as the stand up of the CNO's information dominance initiatives.

We are aggressively pursuing the use of enterprise software and hardware initiatives. We are forging a path to implementing the DoD Enterprise User concept that includes enterprise e-mail and active directory optimization — so an authenticated DON user will be able to go anywhere in the DoD, log in and be productive.

Effective use of our resources is important, and we are actively implementing green IT initiatives as a part of the NNE. As such, we are actively and aggressively reducing excepted and legacy networks and consolidating portals, data and servers.

The Information Age demands that we possess the ability to make decisions at network speed, and outmaneuver our enemies. In short, we believe we need to be able to deliver any content, anywhere, anytime to any device to arm our warfighters with necessary information. The NNE is central to everything we do in the department. And information dominance is a byproduct of NNE.

CHIPS: Department of the Navy personnel now have the opportunity to discuss and help shape current and future IM/IT initiatives using the Pulse, a collaborative Web site, sponsored by the DON CIO, for members of the DON IM/IT community. What led to the establishment of this Web site and what recommendations or comments do you hope to receive from the workforce?

Mr. Carey: I've had a blog for more than two years now, and although it has been successful and has encouraged the exchange and sharing of ideas and opinions, I wanted to take the dialogue a step further by creating a site that would provide the opportunity to engage the department more directly and candidly than possible on a public Web site.

We researched existing tools but found that, for our purposes, we would still need a degree of customization and security. My Web development team redesigned our public Web site and incorporated Web 2.0 tools a couple of years ago. So we already had the infrastructure in place to make this an extension of our public site, and we already had resources dedicated to the maintenance of the Web site. We decided to make the Pulse a Common Access Card-restricted site open to users with .mil e-mail addresses.

Since the Pulse went live on Feb. 8, 2010, 27 blogs have been posted and more than 400 members have joined. So far it is enabling the candid exchange that I had hoped for. Users are able to talk about what's on their minds, ask questions, and get answers from knowledgeable DON personnel, regardless of their positions within the organization.

The Pulse has provided a forum for department personnel to discuss and collaborate on key information management, information technology and cyberspace initiatives, and it is providing insight into the concerns and challenges being felt across the department.

CHIPS: Is it a nonattribution site? I realize that personnel must behave professionally, but can they make suggestions or provide constructive criticism without fear of reprisal?

Mr. Carey: Yes. Members create their own usernames so they can be creative if they want to be and some certainly have been. And by all means, I want members to feel they can be open and honest in their discussions. In order for the department to get to where it needs to be, we need to know both what is working and what is not working. All opinions are welcome and considered.

CHIPS: Will you comment on the new social media memo that just came out?

Mr. Carey: The department completely supports the Directive-Type Memorandum (DTM) 09-026 issued Feb. 25 by the Deputy Secretary of Defense on the responsible and effective use of the Internet. In the past there has been confusing and conflicting guidance on the use of social media, Web-based e-mail, etc. We collaborated with the DoD CIO on the content of the memo to ensure that Navy and Marine Corps inputs were heard. The DTM is valid for 180 days from the date it was signed and is meant to clarify DoD policy and provide guidance until more permanent policy (a DoD directive) is released.

It is a very basic policy that says: (1) the NIPRNET shall be configured to provide Internet capabilities across the DoD; (2) DoD components shall continue to defend against malicious activity affecting the networks; (3) DoD components shall continue to deny access to sites with prohibited content and to prevent users from engaging in prohibited activities on social media sites; and (4) all use of the Internet shall comply with Joint Ethics Regulations. We have worked with the Navy and Marine Corps to develop DON specific guidance that is based on the DoD guidance.

CHIPS: I always look forward to talking about your recommended reading list.

Mr. Carey: My recommended reading list comes primarily from books we read during what we call our "Expanding Boundaries" seminars. I hold a quarterly seminar to encourage personal growth, superior leadership and innovation among my staff.

We read a book before the seminar and then take a day away from the office with facilitators to discuss it and apply its principles. The last one we read is called, 'Building the Bridge as You Walk on It.' It's about people who embraced change — whether voluntarily or out of necessity — and entered the fundamental state of leadership. It shows how anyone can enter this state by putting into practice eight principles that center on integrity.

One of my all-time favorite books is 'The Speed of Trust' by Stephen Covey Jr. Right now I am reading 'Who Says Elephants Can't Dance' by Lou Gerstner, which is about the turnaround of IBM in 1993.

Although leadership is a running theme, the topics vary and include creating a sense of urgency to effect change, creating a culture of candor through transparency, using Web 2.0 tools for mass collaboration, executing or closing the gap between results promised and results delivered, and discovering your strengths.

Also included on the list is, 'Rule Number Two' about the experiences of a Navy psychologist deployed to Iraq. I highly recommend this read to better understand the experience of a deployment supporting the global war on terror.

The reading list can be found at www.doncio.navy.mil.

CHIPS: Can you discuss the DON's greatest IM/IT challenges and successes?

Mr. Carey: One of our greatest challenges, which also became one of our greatest successes, is NMCI. The centralization of the majority of Navy and Marine Corps networks was a daunting effort that proved over time to be a success. Understanding our IT spending and getting a handle on all the legacy systems out there and getting everyone to accept and adopt this totally new way of managing desktop computing was a huge achievement.

But we persevered and in doing so we standardized our desktop computing hardware and software, reduced legacy applications, and greatly enhanced the security of our networks. As we move on to NGEN and then NNE, I'm sure there will be additional challenges, the most prominent of which remains the culture of control. But with the careful planning that's underway, we are looking forward to successes in our future networks also. CHIPS

Visit Rob Carey's blog at www.doncio.navy.mil/blog.aspx.

Get the latest news and blogs on your mobile device at www.doncio.navy.mil/mobile.

Join the Pulse, a collaborative Web site for the DON IM/IT community at https://www.doncio.navy.mil/Pulse.

Talking with Adm. James G. Stavridis
Supreme Allied Commander, Europe
Commander, U.S. European Command


Adm. James G. Stavridis

The inexhaustibly optimistic and indefatigable head of the U.S. European Command and Supreme Allied Commander, Europe Adm. James G. Stavridis spoke to an enthusiastic audience and national-media at West 2010, a conference co-sponsored by AFCEA International and the U.S. Naval Institute, in early February. Uppermost on his mind are the dramatic increases in cyber attacks worldwide, the good that social media can accomplish in the global arena, and the power of technology combined with human capital to exponentially create opportunities for education, cooperation and progress in developing countries.

In speaking about cyber threats, Stavridis said they could well prove to be provocation for a future war. Adm. Stavridis said that four Balkan countries: Latvia, Lithuania, Estonia and Georgia were victims of foreign cyberattacks within the past four years. In the case of Georgia, a debilitating cyberattack on the country's Web sites occurred simultaneously with a conventional military attack.

While NATO's Article 5 allows for the common defense of the alliance in the event of an attack on any one NATO member, the admiral said NATO needs to reconsider the definition of an attack because of the increasing number of attacks in cyberspace, which did not exist when NATO was formed 61 years ago. Adm. Stavridis spoke with media representatives Feb. 2.

Q: How would you rate the interoperability of the NATO allies in their ability to work together?

Adm. Stavridis: Interoperability among the NATO allies is good. It is a force that connects us. If I step back and look globally, say in my previous job, where I was commander of U.S. Southern Command and we were trying to interact with nations in Latin America and the Caribbean, I would say that it was less good and therefore becomes something that we have to work hard to correct … to have that interoperability.

The fundamental answer is that it depends on which group of allies. In NATO, I would rate interoperability as strong and as a connective force between the 28 nations of NATO.

Technology is one of the crucial elements in our ability to connect our alliance structure, and it is not just the interoperability piece, it is also the sensor piece, ordnance [and] cyber. In those particular domains, technology is at the top of what I need to focus on in terms of moving the alliance forward.

I think we all appreciate that the most important thing of all is human capital. It is finding interoperability between people that is particularly important in an alliance when we have 28 different cultures and 20 different languages represented.

I would connect those two as follows … I am interested in technologies that help me develop interoperability in the human side — connective mechanisms in the cyber world, linguistics, translation, the ability to take information from different domains, the thin client process, all of that is crucially important.

Anytime you get into coalition warfare, you need that ability to be interoperable in a purely technical sense, but also how you connect with human capital.

Q: Does NATO have a cyber policy for prosecuting network attacks?

Adm. Stavridis: Not yet, we are at the beginning of that conversation, but I think that is important that we have that conversation in NATO. What we have is a Center for Excellence for Cyber Defense that is in [Tallinn] Estonia.

Secondly, we are having the conversation as part of the development of the NATO strategic concept this year. By the end of this year, I think we will see emerging in NATO a real awareness of cyber. Eventually, we will see similar structures emerge in the alliance as we are seeing individually within the nations.

I think cyber is much more than the military component. Today, cyber activity rests on connecting the international world, the interagency [organizations] in each of these individual countries, and indeed the private and public sectors. The term I like to use is 'strategic connections.'

We hear a lot about strategic communication. Strategic connection is bringing together international, interagency, private and public [groups] to address very complex problems, and I will put cyber at the top.

It is important that we get the military structures [for example, U.S. Cyber Command] in the United States. They will eventually be a part of a much larger [national] architecture that deals with cyberspace.

Estonia suffered a series of cyber intrusions at a high level in 2007 … I think in Estonia there is a high degree of appreciation for the importance of understanding the cyber world and [the need for a strong] cyber defense. As we all know, in the cyber world, one of the hardest things to do is to attribute this kind of activity. I think it is very difficult to say, 'This is the result of the activity of a particular nation, or not.'

It could be a hacker; it could be somebody who is affiliated with a nation-state. Estonia definitely felt the effects of significant cyber intrusion that particularly focused on its financial system. As a result, it seemed like a good place for NATO to put the Center of Excellence.

Q: There has been talk among the coalition about reducing or removing troops in Afghanistan due to lack of progress.

Adm. Stavridis: I think there are four crucial things we need to do in Afghanistan, and I think if we do these well over the next 18 to 24 months, we will see a distinct level of progress, and I am optimistic that we will.

The first is putting the Afghan people at the center of gravity;

it is protecting them and partnering with them. As my good friend Stanley McChrystal (U.S. Army general and commander, International Security Assistance Force and commander, U.S. Forces Afghanistan) says, we are not going to 'kill' our way out of Afghanistan. We have to protect the Afghanistan people so that they will turn away from the insurgents.

Frankly, if you look at the polling data in Afghanistan today, we see this beginning to happen. The Taliban are polling less than a 6 percent approval rating, and the Afghan government and the Afghan security forces are polling over 80 percent. That's from the BBC/ABC/ARD [news] poll that was conducted a few days ago on 1,500 independent Afghans around the country.

… Secondly, strategic communications, it's articulating what we, the coalition, need and must do in Afghanistan and back in our (nations') capitals. If we do a good job of strategic communication, we will be capable of explaining to the populations in all of the capitals why we are there, and continue to see the same sort of spirit we saw in the International London Conference on Afghanistan last week where [more than] 60 countries and 19 international organizations came together to pledge long-term support in Afghanistan.

Let's face it, in the end, it is not going to be about troop levels in Afghanistan. We will not deliver security in Afghanistan through the barrel of a gun… It has to be a comprehensive approach. That brings me to the third thing we need to do which is to bring together the political, economic, cultural and the linguistic [elements] along with security in order to achieve the effects that we need in Afghanistan.

The fourth, and most important thing, in terms of any date we look forward to in the future [before pulling troops out] is training Afghanistan's [National] Security Forces. It is the ability to transition security activities that will enable all of us to leave when the time is right.

I am very, very optimistic about our ability to train the Afghan [National] Security Forces. There is risk in it, but we have a new NATO Training Mission – Afghanistan stood up by Lt. Gen. Bill Caldwell 60 days ago. We are populating that rapidly. Nations are sending their best people. Job 1 for the alliance is training the Afghan security forces.

The real question is not that this nation may leave or that nation may leave, it is based on those four things. The wild card is reconciliation with the Taliban. That has been a topical discussion over the last couple of weeks — again a bounce out of the London conference.

I believe that there are openings, certainly for re-integration of lower-level Taliban. There could be a political process, and it has to be Afghan-led, that may lead to reconciliation of some of the most senior Taliban. That is a process that is under construction, but has possibilities to fundamentally change the situation.

Q: Do you use social media?

Adm. Stavridis: It's huge for me. I use Facebook, Twitter and LinkedIn. I invite all of you to 'friend' me if you are on Facebook. I will give you an example of how this kind of thing works. I was giving a talk in London to a small group, maybe 100 people, and as part of the talk I said, 'I am on Facebook, friend me.' I got a little chuckle.

An AP reporter wrote a story with the headline, 'NATO Admiral Needs Friends.' It ran in two countries: Finland and Indonesia. The next day I had hundreds of Finns and Indonesians friending me on Facebook and the general tenor was, 'I heard you need a friend. What's NATO?'

STUTTGART, Germany — Chiefs of Defense from 11 Western European nations within U.S. European Command's area of focus gathered Feb. 18, 2010, for a conference hosted by Adm. James Stavridis, to discuss mutual and regional security issues, foster cooperation in engagement of mutual theater objectives and the importance of collective efforts in Afghanistan and Iraq. U.S. Army photo by Martin Greeson.

That's a funny story, but that is exactly why I use social networking because it affords me the opportunity to bring people into the conversation and tell them about something that I think is very important to the security of the 21st century — NATO.

[Another example] … STAR-TIDES, a very impressive system, it is a kind of a network in a box that is using social media to connect to Creole speakers. The language of Haiti is not French; it is Creole, which is a difficult language to speak. I speak French and Spanish but I can't follow Creole, which is an amalgam of those two plus African tribal dialect.

The STAR-TIDES system is using social networking effectively to create translators that tap into this network. It is a perfect match. [In response to the earthquake in Haiti, organizations and individuals collaborated to create a short message system [SMS] code [4636] that allowed the exchange of short text messages between mobile phones and related devices to provide information and bring help more quickly to the Haitian people.]

Back to your question Sharon, about technology and human capital, you are bringing together a technology in a box that allows you to tap into the social network that allows you to create strategic effect with translators, with text messages written in Creole. If the responders can't translate them, they go back on social media and get the translation, and it comes back to the STAR-TIDES machine in Haiti. It is a wonderful example of how all these elements can fit together [to produce a desired outcome, in this case, disaster relief].

I think social networking is vitally important to security… I am talking about strategic connections, and social media is a powerful form of that.

Q: What are the new military strategies for Afghanistan?

Adm. Stavridis: We, the military, have a program, the Afghan

Pakistan Hands (AFPAK Hands). Gen. McChrystal has pioneered this. It is taking superb officers at the 0-3 and 0-4 level, giving them language training in Pashto, Dari or Urdu, and then focusing them throughout the bulk of their mid-career on Afghanistan and Pakistan.

They will cycle in, do an operational tour and then come out and do a refresh tour. They will remain hooked to a staff focused on this part of the world, and then they will go back into Afghanistan or Pakistan. I think that is the model for the U.S. military as it looks at a variety of regions in the world.

Secondly, Afghanistan requires an interagency effort, it's our ability in defense to team up with USAID — U.S. Agency for International Development — as they do development, and State as they do diplomacy, the three Ds (defense, development, diplomacy). But it is bigger than that — it is the Department of Justice, it is the DEA (Drug Enforcement Administration) and the Department of Treasury. It is all of that interagency effort coming together to accomplish effects.

The third thing is the private sector. In Afghanistan, we are not going to deliver security with the barrel of a gun; we are going to deliver it by educating a generation of young Afghanis. We, and I mean the big we, everybody from Greg Mortenson's 'Three Cups of Tea' building schools, to USAID building the schoolhouses and bringing in the notebooks and computers, to the private sector, and Nicholas Negroponte's [program] One Laptop per Child with hand-cranked, ruggedized computers that automatically network and link together with any other One Laptop per Child [user] that they find within the cell phone architecture.

All of those things must come together to create the effects we need in Afghanistan or anywhere else. When I was in U.S. Southern Command, we worked very hard on this approach, for example, in Columbia, which I think is continuing to move in a positive direction. [Columbia] has taken this international, interagency, private/public approach, comprehensively bringing all those things together.

Q: Do you think the people of Afghanistan are ready for these changes?

Adm. Stavridis: I think that every society will have its own way of approaching things, but look at the numbers. In Afghanistan, eight years ago there were effectively zero cell phones, today there are 9 million cell phones in Afghanistan. This country is going to skip brick and mortar banking, it is going to go from paper and coins handed out at the pay line directly to electronic transfer via cell phone.

Right now Iraqi forces are paid through a cell phone. It cuts corruption, it permits instantaneous transfers, and it obviates the need to build brick and mortar banks.

I can give you many more examples of Afghanis who are willing to reach out. There is this mythology that they are people that live in remote villages, and they don't want to enter the 21st century, but that hasn't been my experience.

I find the Afghanis to be hungry for education and hungry for technology. They want a better life for their children, the way we all do. CHIPS

Adm. Stavridis and EUCOM can be found on LinkedIn, YouTube, Facebook, Flickr, Twitter, Delicious and www.eucom.mil.

Exploring the "Cyber Sea"

By Adm. James G. Stavridis
Commander, U.S. European Command and
Supreme Allied Commander Europe

The cyber world really caught my attention about a year ago when my daughter's Facebook account was pirated and her identity used for a swindle. Ugh!

Earlier this month, I gave a speech in San Diego that addressed the issue of the cyber domain — what I like to refer to as the "Cyber Sea" (I'm a Sailor, after all!). The speech has received a fair amount of attention. I appreciate all the feedback I've received on it so far and look forward to any you may have.

I am keenly interested in exploring and investigating solutions to balance the tension between the desire for collaborative openness against sustaining the necessary protection of the underlying networks and systems. Since my speech in San Diego, I've thought a lot more about the subject, and I keep coming back to the idea that there are two possible outcomes to the current complex and largely ungoverned Cyber Sea environment:

The first, and vastly preferred outcome, is that we work together as an international community to create a comprehensive set of rules and behavioral norms that would govern behavior within the cyber domain. Think of an effort along the lines of the Law of the Sea Treaty negotiation, a very big project indeed.

Yet a second possible, albeit highly undesirable outcome, is that we find ourselves in a deterrence posture similar to the Cold War but with different tools. A stalemate, if you will, wherein actors —individuals? organizations? nation-states? — are deterred from "doing harm" by the threat that harm will, in turn, be done to them.

In our pursuit of the preferred cyber domain, I expect we'll find ourselves navigating the Cyber Sea somewhere between the shores of both possible outcomes. Current cyber attack events highlight the existence of "cyber-citizens" who demonstrate a proclivity for disruptive, self-serving behavior. And just like pirates, smugglers and traffickers on the high seas, who ignore the law of the sea, we'll have to take measures to protect ourselves, and deter the activities of these "bad actors" in the Cyber Sea. It will take time, work and commitment, but I'm confident if we proactively work together today, we can ensure that the first outcome becomes our collective future.

My own thinking on this subject has been informed by a whole host of resources and conversations, but I am by no means an expert… whereas some of you undoubtedly are. So, in the spirit of conversation, I thought I'd share some of my favorites, and hope that you, in turn, will share with me some of your ideas and inspirations:

• Lt. Gen. Keith Alexander. A brilliant leader on the cutting edge of this topic within the national security context. Some of his speeches and Congressional testimony can be found at www.nsa.gov.

• Clay Shirky. Author, speaker, thinker. Google him and perhaps check out one of his many talks at www.ted.com — and be sure to browse the site for lots of other remarkable thinkers and ideas!

• Two books which are a little older but no less important as we develop our collective thinking on how to navigate the Cyber Sea:

– *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage* by Clifford Stoll, a real-life story about life within the Cyber Sea.

– *Secrets and Lies: Digital Security in a Networked World* by Bruce Schneier, who is an expert in the field and shares the language and thinking of those whose profession it is to guard networks and systems.

I'll see you on the Cyber Sea! CHIPS

Taken from Adm. Stavridis' blog, From the Bridge, on USEUCOM's Web site, posted Feb. 24, 2010. Go to www.eucom.mil to find the admiral's blog.

Interview with Vice Admiral H. Denby Starling II
Commander, Navy Cyber Forces
Commander, Naval Network Warfare Command

Vice Adm. H. Denby Starling II

The Chief of Naval Operations has postured the Navy to play a strategic role in the cyber domain by realigning organizational elements and establishing new naval commands. To complement the stand up of the Deputy Chief of Naval Operations for Information Dominance (N2/N6), on January 29, 2010, the Navy established Fleet Cyber Command (FLTCYBERCOM) and recommissioned the U.S. 10th Fleet at Fort George G. Meade, Md., to oversee the operational aspects of cyber warfare.

FLTCYBERCOM/COMTENTHFLT is the U.S. Navy component command to DoD's proposed sub-unified command, U.S. Cyber Command (USCYBERCOM). Earlier that week, Navy Cyber Forces (CYBERFOR) was established at Joint Expeditionary Base, Little Creek-Fort Story as the dedicated type commander (TYCOM) for cyber, subordinate to Commander, U.S. Fleet Forces Command. Many functions now performed by Fleet Cyber Command/10th Fleet and Navy Cyber Forces were formerly conducted by the Naval Network Warfare Command (NETWARCOM).

Vice Adm. H. Denby Starling II, having served as the NETWARCOM commander since June 2007, played a significant role in reshaping Navy's cyber organization to meet CNO's vision. He has assumed command of Navy Cyber Forces and retains command of NETWARCOM. CHIPS asked the admiral to discuss the realigned missions of CYBERFOR and NETWARCOM in early February.

CHIPS: Can you discuss the recent changes within the Navy cyber domain and how you prepared for the establishment of CYBERFOR?

Vice Adm. Starling: The CNO had a vision from the start that cyber in the Navy was going to be a real growth area. He spent a lot of time in his first months as the CNO soliciting input both inside and outside the Navy about how to organize it. In the middle of last year, he made his decision and came out with three big pieces of guidance. The combination of N2 and N6 was the first big announcement, but that was in the OPNAV arena.

The CNO also directed the Navy to stand up Fleet Cyber Command at Fort Meade, with a three-star commander. When he made that decision it really moved the operational center of gravity from NETWARCOM to FLTCYBERCOM.

CNO further directed that NETWARCOM would have a more focused mission on network operations and space operations. This meant that NETWARCOM's man, train and equip mission would realign back to U.S. Fleet Forces Command. As we looked at the ways to execute that guidance, we ultimately made the decision to establish a stand-alone global type commander — Navy Cyber Forces.

We prepared by looking at what CNO was trying to accomplish, which was the establishment of a very strong cyber operational presence at Fort Meade, while retaining a very strong man, train and equip function here at Little Creek that would continue to serve, not just the fleet, but the whole Navy.

With that in mind, we looked at all of those things that NETWARCOM did. We took our own mission, functions and tasks, and dissected them. At the same time, we worked with the implementation team in Washington, D.C., to stand up Fleet Cyber Command. We essentially took all those functions and put them into bins for FLTCYBERCOM work, CYBERFOR work, and NETWARCOM work, aligned the people and the resources accordingly, and pressed on from there.

When CNO said he wanted to effect this change, it gave us an opportunity to do something revolutionary. The CNO wanted us to leap ahead aggressively in the things that Navy is doing at Fort Meade. But it is also evolutionary, if you look at the way that NETWARCOM came together in 2002. At the time, it was a revolutionary step as we gathered up all of our computers, C4I, space and cryptology into a single organization. From that perspective, this is another step in the evolution, although I think CNO sees it as moving much faster this time.

CHIPS: Can you talk more specifically about how those functions were divided between the three commands?

Vice Adm. Starling: When I first came to NETWARCOM, we were the 'one-stop shop' for all things cyber. We didn't call it cyber back then, but we were the Navy's primary point of contact for networks and C4I. This past year, as we looked at all the functions NETWARCOM performed in big picture terms, we asked: 'Is it an operational function, a command and control function?' If so, it would belong inside FLTCYBERCOM/COMTENTHFLT or NETWARCOM.

Then we asked, 'Which of these functions are man, train and equip, which ones address the administration of organizations, which ones address the training of our personnel and the training of organizations and the delivery of equipment?' Those functions were pulled into CYBERFOR as the type commander.

If you look at the way Navy does this in other warfare areas, you'll see that what we have actually done is to put cyber in the same sort of alignment as a warfare area that we have in air, surface, subsurface. So, Navy Cyber Forces is now more appropriately aligned with the other Navy TYCOMS: Navy Surface Forces, Naval Air Forces, Navy Submarine Forces and Navy Expeditionary Forces.

Before I came to this job, I was the aviation East Coast type commander (Commander, Naval Air Force Atlantic), responsible for the man, train and equip functions to provide the resources necessary to enable our operators (the Naval aviation workforce) to perform their duties and achieve mission success. The commander of Navy Cyber Forces will do the exact same thing.

CHIPS: Can you talk about CYBERFOR's man, train and equip role?

Vice Adm. Starling: When I came to NETWARCOM almost three years ago, I really felt that we needed to build a stronger type commander function, just like the platform side had — an organization that looked at the basics, and an organization that paid close attention to the readiness of our fleet to do its business in the information domain. The organization was doing that, but not in a focused fashion.

When it came time to split out the man, train and equip function, I thought it made great sense, and I believe Adm. Harvey, commander of Fleet Forces, saw that it made great sense. CNO agreed to stand up this function as a type commander. If we want to be preeminent in the information domain, just as we want to be preeminent in submarine warfare, air warfare and surface warfare, the fundamental building blocks are forces that are properly manned, trained and equipped. As the type commander for Cyber Forces, I'll support CNO's vision of information dominance by providing Vice Adm. McCullough, as well as the remainder of our fleet, with the most ready systems, the strongest networks, and the best trained people that we possibly can.

CHIPS: Why was it necessary to stand up 10th Fleet, wasn't the establishment of FLTCYBERCOM sufficient to sustain the cyber mission?

Vice Adm. Starling: Back in World War II, 10th Fleet was established to combat German U-boats. They were causing us tremendous problems in the Battle of the Atlantic. It was much like cyber is today — a new warfighting area with a lot of disagreement on the direction we should go. Tenth Fleet was stood up in the early years of World War II to combat that threat, and by the end of World War II, we were dominant in the Atlantic, and we were dominant in ASW.

Much like Fleet Cyber Command, when 10th Fleet was first stood up, it didn't have regularly assigned ships. It wasn't a hardware organization; it was an organization dependent upon intelligence and tactics and the development of new ways of doing business in this new warfare arena. Interestingly, at the end of World War II, 10th Fleet was disestablished.

As the Navy was looking for what we wanted to do with this new cyber fleet, it seemed most appropriate now that we have arguably a new warfare domain, and one that has many of the same characteristics that the submarine threat had in 1942, to reactivate 10th Fleet.

In regard to why we have Fleet Cyber Command and 10th Fleet, it's a Navy model. It's just like in 5th Fleet where there is the commander, U.S. Naval Forces Central Command, as well as the commander, U.S. 5th Fleet. One is a component commander designation, and one is a warfighting designation.

CHIPS: What will be NETWARCOM's mission?

Vice Adm. Starling: NETWARCOM, as of the 26th of January, became an organization wholly focused on network operations and space operations in support of 10th Fleet. In the past, NETWARCOM had a tremendously broad range of functions — all of the operations that we just talked about, as well as all of the man, train and equip functions.

The NETWARCOM that exists today, and that will move into the future, will be smaller, more operationally agile, and totally focused on network and space operations as directed by the commander of 10th Fleet.

NORFOLK, Va. (Jan. 26, 2010) Adm. J. C. Harvey Jr., commander of U.S. Fleet Forces Command, speaking at the stand up of Navy Cyber Forces. At right, Vice Adm. H. Denby Starling II, commander of Navy Cyber Forces, and Adm. Harvey cut a cake commemorating the command's establishment during a ceremony at Joint Expeditionary Base Little Creek-Fort Story. CYBERFOR is the type commander for cryptology, signals intelligence, cyber, electronic warfare, information operations, intelligence, networks and space disciplines. CYBERFOR will report to Commander, U.S. Fleet Forces. Navy photos by Mass Communication Specialist 3rd Class Nina Hughes.

CHIPS: What does the NETWARCOM workforce look like now?

Vice Adm. Starling: The workforce looks very much like what we had in the 'Ops Department' in what I would call the 'old NETWARCOM.' We carved out our operational function, which largely existed under the directorship of Rear Adm. 'Peg' Klein as the Global Operations Officer. We beefed it up a little bit with some pieces that were done in other parts of the organization, for instance, adding CARS (Cyber Asset Reduction and Security), and ODAA (Operational Designated Approving Authority) Directorates. But if you were to walk onto the NETWARCOM watch floor today, it would look very much like the watch floor did two weeks ago or two months ago.

We took functions, such as network operations, network defense, in our operational dealings with our subordinates — the Navy Information Operations Commands and NCTAMS LANT and PAC (Naval Computer and Telecommunications Area Master Stations, Atlantic and Pacific) — and we have aligned functions operationally, so instead of going through NETWARCOM to U.S. Fleet Forces, now these functions report to Commander, 10th Fleet. So those things that we used to report operationally to Adm. Harvey, we now report to Adm. McCullough and his staff.

By the same token, those things we did for man, train and equip under the old NETWARCOM hat — enlisted training, career management to some extent, fleet readiness, requirements generation, budgeting and administrative functions — the

same people who did those things here are largely still doing them. They are just doing them now with a name tag that says CYBERFOR instead of NETWARCOM.

What we have really done is to create an organizational structure that better supports the business of cyber inside the Navy. With FLTCYBERCOM at Echelon II, there is a direct line to the CNO and a direct line to the joint side. NETWARCOM will be able to focus better on operations. CYBERFOR, an Echelon III command focused on administrative functions and reporting to U.S. Fleet Forces, will have a commander whose job it is to focus wholly on man, train and equip.

I am fortunate to command both of these organizations, but I think it is unlikely that this will be the case in the future. Navy Cyber Forces and NETWARCOM are two separate commands, and as this organizational construct continues to mature, it will become more evident what each of these commands is designed to do. I recognize that to many today, it may not be completely clear, but that's because we are looking not only at new organizations, but at new ways of doing business — which is exactly what CNO wanted us to do.

CHIPS: Do you have a new vision for NETWARCOM?

Vice Adm. Starling: I'd say it's not so much a new vision, but a re-focused one. The vision is that NETWARCOM will be the most operationally agile network and space organization in the world. Without the man, train and equip overhead, it will make NETWARCOM a better organization. By that same token, the focus for Navy Cyber Forces will be to develop and deliver the best cyber readiness capabilities to the fleet and Navy.

CHIPS: Will NETWARCOM continue to manage the space cadre?

Vice Adm. Starling: Part of CNO's guidance writ large was the establishment of the Information Dominance Corps. The center of gravity for management of the Information Dominance Corps was realigned to the DCNO for Information Dominance, N2/N6. We still will do some of the bean counting functions for the space cadre for billets and where people are, but the management, policy and community management piece for the space cadre will reside in N2/N6.

CHIPS: Many security experts have said that the Defense Department has lagged behind in cyberwarfare concentrating on defending networks instead of using an offensive approach. Will Navy strategies for protecting cyber assets change now?

Vice Adm. Starling: The alignment that CNO has put into place — the establishment of N2/N6, the way CNO looks at resources, the way he wants to position Navy to move both on the offense and defense with the establishment of Fleet Cyber Command close to the center of the action, as well as having Navy Cyber Forces to keep a solid focus on the fundamentals and the equipment — all of this best positions Navy to respond to any demand that comes from DoD.

There are lots of opinions on how to do cyber, but what I have learned in my three years at NETWARCOM is that there has to be a balance between the offense and the defense. There just has to be. I'm an aviator by training. The old adage that the best defense is a good offense is probably a very good one to use when you are talking about force-on-force confrontation — which is how we have always looked at warfare. I line up my forces on one side; you line your forces up on the other side, and we see who comes out on top. But cyber doesn't work like that. You have to defend everywhere, and there is no equivalent of the force-on-force approach for cyber that exists on the kinetic side of warfare.

If you listen to the greater discussion beyond cyber with regard to where the Secretary of Defense is trying to take DoD, and much of the discussion with regard to how to fight terrorism, and in the wars in Afghanistan and Iraq, some would argue strongly that our offensive mindset has to change. Many of our deep thinkers, both in and out of uniform, recognize that these threats require a different type of warfare. Cyber also requires a different way to think.

You have to defend everywhere, just like in the homeland defense of the country, we have to defend everywhere. We have to have strong networks, we have to have good defense, and we have to be able to defend the command and control systems on which we rely so heavily.

Navy is a netcentric organization. Crucial to everything we do is our ability to keep our networks functioning, and to do that we have to have a strong defense. I have great confidence that we have outstanding offensive capabilities. I think I'll just leave it at that. One of the difficulties of talking about capabilities is that we immediately get into a classified area.

CHIPS: Do you think information dominance globally is achievable?

Vice Adm. Starling: I think it is a goal that we need to keep working toward. The ability to turn inside the enemy's decision cycle, which is really what information dominance is all about, is critical to any fight that we are in. Can we achieve information dominance 24/7 worldwide? … Probably not. But what we need to do is to better understand those areas where it is critical that we be able to achieve information dominance over those that we think pose the greatest threat to us.

The term information dominance has only been around a few years, and it has gone from theory to the practice stage. I can tell you that Navy is better aligned to achieve information dominance now than it has ever been.

We've made a lot of big changes in the Navy in the last four to five months in the cyber world. I believe there will be a lot [of people] out there who don't deal in this world day-to-day, and who are either unaware or see the name changes and don't understand what has occurred, so I appreciate the opportunity to clarify some of the changes. CHIPS

Editor's Note: The CNO announced prospective commanders for CYBERFOR and NETWARCOM March 31. Rear Adm. Thomas P. Meek will be assigned as the commander of Navy Cyber Forces, and Rear Adm. Edward H. Deets III will take the helm of Naval Network Warfare Command at a Change of Command ceremony May 14 at Joint Expeditionary Base Little Creek-Fort Story. CYBERFOR/NETWARCOM Commander Vice Adm. H. Denby Starling II will retire at the ceremony at the conclusion of 36 years of Naval service. For more information about Navy Cyber Forces, visit the command's Navy News site at www.navy.mil/local/ncf.

Information Dominance for Navy Medicine Decision Makers

Space and Naval Warfare Systems Center Atlantic delivers innovative capabilities in an NMKMS architecture

By Holly Quick

Sponsored by the Office of the Chief of Naval Operations, Medical Resources, Plans and Policy Division (OPNAV N931), the Navy Medicine Knowledge Management System (NMKMS) began as a research and development project to: address high-value capability gaps in current Joint Electronic Health Record capabilities; assess the value of data warehousing techniques for data storage and retrieval; and design an open architecture that could be leveraged by multiple sources with ease of integration.

The goal of NMKMS is to collect the highest quality of casualty care data in an operational setting with the minimum amount of disruption to the healthcare providers. Rather than simply exchanging data files, Navy Medicine requires interoperable applications that not only share data, but also leverage computing and storage resources.

What is NMKMS?

NMKMS is a data warehouse capability for the collection, standardization, storage and servicing of operational medical data of interest and value to Navy Medicine.

Data Collection

NMKMS accepts multiple data sources, including Armed Forces Health Longitudinal Technology Application – Theater (AHLTA-T) encounters; Shipboard Non-tactical Automated Data Processing (SNAP) Automated Medical System (SAMS) 8 and 9 environmental, logistical and medical encounters; and Theater Medical Information Program (TMIP) Composite Health Care System (CHCS) Cache (TC2) medical encounters. The encounters are transferred through either the TMIP Framework or SAMS Communicator in an encrypted manner to a centralized NMKMS data collection and storage instance (see Figure 1).

Data Standardization

At point of entry into NMKMS, the data is parsed and each individual data element is compared to the business rules governing that data element. These business rules allow NMKMS to reduce the "apples," "oranges" and "peaches" to "apples" so the reporting is performed using the standardized data. This apples-to-apples approach accounts for differences in data such as numeric code, capital letters and lowercase letters, and converts data to a standard format that can be used for query and reporting purposes.

Data Storage

Once the data has passed all validation tests and has been transformed according to the business rules, it is then stored in a data warehouse for optimal analysis and reporting.

"In the future, the NMKMS data warehouse is envisioned to serve as the collection point and data broker for all authoritative sources of Navy and Marine Corps operational medical data. NMKMS will then serve up properly normalized data marts that support critical applications and services to Navy Medicine decision makers, including the Navy Surgeon General and combatant command (COCOM) surgeons," said Claudia Kiefer, Space and Naval Warfare Systems Center (SPAWARSYSCEN) Atlantic project manager for NMKMS.

Data Servicing

NMKMS uses customized data marts that are specific to the reporting need. This prevents users from directly accessing the data warehouse, and helps to protect personally identifiable information. Additionally, these data marts allow for distributed networking of the enterprise components, abstract reporting

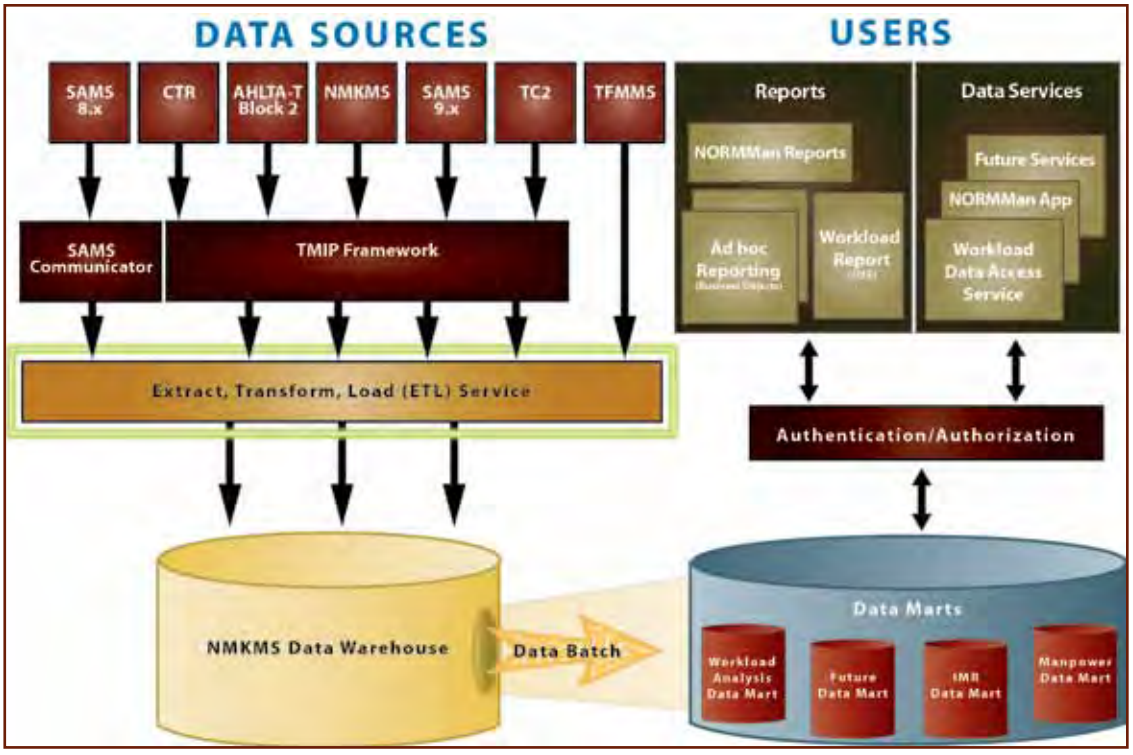


Figure 1. NMKMS supports aligned, centralized and operational Navy and Marine Corps data.

from data storage, and allow the data model within NMKMS to evolve without breaking third party visualization tools.

Solving Business Problems and Creating Business Opportunities

SPAWARSYSCEN Atlantic employs agile software development and Lean Six Sigma methodologies within the overarching Department of Defense (DoD) Software Development Life Cycle (SDLC), using short iterations to break down larger goals. SPAWARSYSCEN Atlantic practices open and transparent communication with its partners and customers and believes in providing training and support in the adoption and implementation of best practices for agile software development and Lean Six Sigma methodologies.

Most recently, SPAWARSYSCEN Atlantic has been involved in extending the current NMKMS architecture to include new capabilities, such as the Naval Operational Requirements for Medical Manpower (NORMMan), Operational Workload Reporting (OWR) and Epidemic Outbreak Surveillance (EOS). Additionally, SPAWARSYSCEN Atlantic is pursuing new opportunities to extend NMKMS capabilities in support of a Joint Medical Distance Support and Evacuation (JMDSE) demonstration, and in the integration of Navy Medicine Online (NMO) and NMKMS.

Benefits of NMKMS

The capabilities of NMKMS offer great benefits to the field of Navy Medicine. These benefits include:

- Lower operating costs;
- Greater security over PII within the data through decreased exposure;
- Higher quality data from more disparate data sources;
- Greater accessibility to standardized data;
- Reduced application and development costs; and
- Near real-time reporting capabilities.

Naval Operational Requirements for Medical Manpower

NORMMan is a medical manpower modeling and simulation capability that resides within the NMKMS architecture. The goal of the NORMMan application is to provide a scenario-driven, predictive model for Navy medical manpower requirements, based on occupational specialty.

NORMMan outputs are used as inputs in the overarching process of medical staff planning. NORMMan receives data from the Total Force Manpower Management System (TFMMS), performs complex computations and produces manpower predictions.

TFMMS tracks more than 50,000 Navy medical billets distributed across approximately 300 medical occupational specialties.

Essential to the NORMMan application is the algorithm that modifies and clusters these billets into occupational specialties and generates report data. While many billets cluster to obvious specialties, there are also special situations that must be accounted for, such as Navy policy, location-specific situations, education-based constraints and personnel availability issues. The NORMMan application utilizes Drools, a business rule engine, which facilitates the clustering of algorithms and produces the NORMMan models.

The predictions supplied by NORMMan will be used by various organizations within the Navy to support formulation of the Future Years Defense Program (FYDP) for the Program Objective Memorandum/Program Review (POM/PR). These predictions are also used to support other medical manpower requirements analyses such as the Medical Readiness Review and Quadrennial Defense Review.

Operational Workload Reporting

The OWR capability that leverages the NMKMS data warehouse architecture provides Navy Medicine with information on the Navy and Marine Corps medical workload in operational theaters worldwide. To alleviate the cumbersome task of manually collecting, cleansing and collating monthly data from the multiple medical data sources, SPAWARSYSCEN Atlantic developed a Web-based OWR capability that displays medical workload data of Navy and Marine Corps deployed medical units.

Data from the Joint Medical Workstation (JMeWS) and the Theater Medical Data Store (TMDS) are uploaded into the application where data are dynamically analyzed to provide the user with a series of views of workload information by unit, unit type and COCOM over time.

OWR is currently servicing the Navy Surgeon General's requirement for monthly reports on worldwide operational medical workload.

Epidemic Outbreak Surveillance

The EOS advanced concept technology demonstration (ACTD) was initiated to deliver a validated, integrated, operational biodefense system that accelerates command decisions and improves joint force sustainment.

The Epidemic Outbreak Surveillance ACTD's system-of-systems approach enhances both biodefense operations and operational medicine through the integration of technology and data components that are needed to provide individual patient care on the front end while serving a higher public health/operational need, in real-time, on the back end.

At the request of U.S. Joint Forces Command (USJFCOM), SPAWARSYSCEN Atlantic extended the NMKMS architecture and services to provide a data fusion capability for the EOS ACTD that would transform integrated data from existing medical health information systems into decision quality information. An EOS-NMKMS test event was conducted to demonstrate an outbreak detection capability that met the EOS program goals using the NMKMS infrastructure.

The EOS-NMKMS test event was conducted to simulate a scenario involving influenza outbreaks on the USS Shoup (DDG 86) and USS Peleliu (LHA 5) over a three-day period. The demonstration utilized simulated patient encounter records that were created using AHLTA-T.

The records were imported into the load directory of NMKMS, simulating TMIP's expeditionary framework. The demonstration record set contained data that would cause alerts to be activated on both ships. The records also contained data that would trigger the software to notify the local medical department that a reportable event had occurred.

The success of the EOS-NMKMS test event highlighted the

value of a capability that provides for the near real-time environmental surveillance, detection and reporting of disease outbreak.

Joint Medical Distance Support and Evacuation

NMKMS is currently being evaluated for use as a platform to support the Joint Medical Distance Support and Evacuation (JMDSE) joint capability technology demonstration (JCTD). JMDSE will provide a virtual triage and remote patient monitoring and care capability.

The role of NMKMS in this demonstration would be to collect and integrate medical encounter data generated by forward-deployed medical first responders, and deliver custom patient information displays to remote healthcare providers.

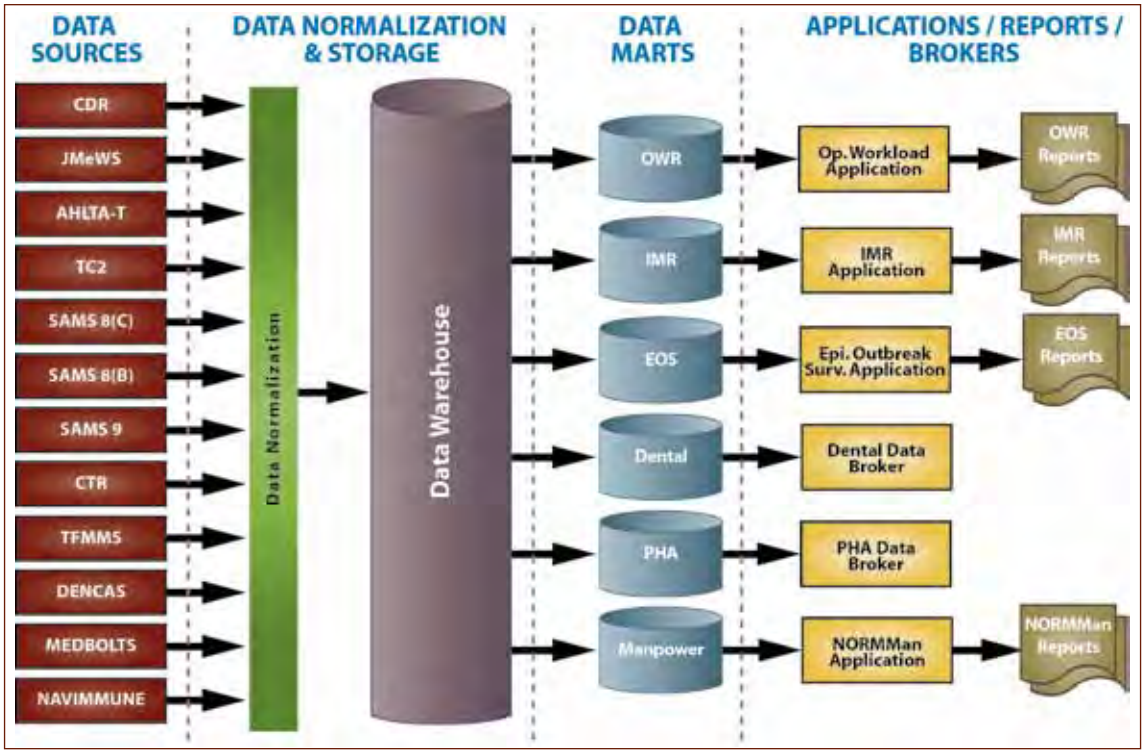


Figure 2. Merged NMO/NMKMS capability architecture.

Integration of NMO and NMKMS

Navy Medicine Online currently serves as data broker for Navy Medicine, by collecting individual readiness information from legacy Navy Medicine data systems, such as SAMS, Dental Common Access System (DENCAS) and Navy Medical Board Online Tracking System (MEDBOLTS), and transmitting select information to the Medical Readiness Reporting System (MRRS) to support DoD Individual Medical Readiness (IMR) reporting, Defense Health Information Management System (DHIMS), Force Health Protection and other Navy systems.

Additionally, NMO hosts critical applications for specific Navy Medicine communities of interest. Originally built in the 1990s, NMO uses obsolete technology, and a stove-piped architecture that is costly to maintain.

SPAWARSYSCEN Atlantic is currently embarked in the planning phase to merge NMO and NMKMS capabilities into a common extensible data warehouse architecture that will service the current and future information needs of Navy Medicine.

The outcome of this merged NMO/NMKMS capability will support a reduction of computing and storage hardware, and provide a scalable, extensible solution that will meet the performance requirements of existing and future projects (see Figure 2).

The merger of NMO/NMKMS capabilities is aligned with Navy Medicine's strategic goals and is expected to generate the following desired outcomes:

- Provide an enterprise-wide operational Navy Medicine data repository;
- Reduce duplication in Navy Medicine systems;
- Support current and future Navy and Military Health System (MHS) stakeholders;
- Provide data marts for specific stakeholders;
- Support receipt of additional medical data elements that are not currently captured via existing interfaces;
- Leverage existing Navy Medicine technology for data normalization, data warehousing and data marts;
- Support customized reporting;
- Support future applications;
- Provide data curation, resulting in improved data quality; and
- Eliminate stove-piped systems and reduce hardware footprints.

In merging the NMO/NMKMS capabilities, SPAWARSYSCEN Atlantic will enable enhanced information sharing and knowledge management across Navy Medicine, and deliver an extensible data warehouse architecture that provides improved management of Navy Medicine information technology investments, and reduces duplication in Navy Medicine systems. CHIPS

For more information about SPAWAR, go to www.spawar.navy.mil. To learn more about Navy Medicine, go to www.med.navy.mil/.

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

Challenges to Acquiring C4ISR Systems Based on Service Oriented Architecture

- Better understand the migration from traditional stovepipe systems to systems based purely on services
- Understand the significant changes to how we specify, acquire, integrate, test and field systems as the Navy moves to services-based systems

By Lee Zimmerman and Antonio Siordia

The Space and Naval Warfare Systems Command develops the standards, policies and integrated architectures for innovative and interoperable command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) solutions that meet warfighters' requirements. The departments of the Navy and Defense are in the midst of a multi-year transition from legacy stove-piped system architecture to a services oriented architecture (SOA) approach. Stand-alone applications are migrating to reusable services within a system, and systems are now starting to share services.

The next step in this evolution may be to do away with systems altogether and, instead, to field loosely integrated suites of services that can be fielded within multiple platforms including ships, command centers and tactical assets to enable net-centric operations for the Navy and joint customers. Although there are numerous benefits in applying SOA to C4ISR systems, significant challenges remain, which we will explore.

How Do You Buy a Services-based System?

Let's start with a scenario. A program, Alpha, might develop a service, for example, a particularly unique data visualization solution, for its own use and would logically scale the supporting infrastructure to an appropriate demand based on expected use. Alpha's developers would follow net-centric guidelines and share their new service in a directory where users associated with program Bravo discover it and find it useful. As a result, usage of the service suddenly doubles and the supporting infrastructure might be overwhelmed.

With current acquisition practices, both Alpha and Bravo are out of luck because the service was built to meet the specific requirements of Alpha, and there is no funding to upgrade the service infrastructure to support the Bravo users. Also, since this was not a planned dependency, there isn't a service level agreement (SLA) between the Alpha and Bravo programs, and subsequently there is no guarantee that the service won't go away or change its interface (application programming interface or API) or its data format. This reuse of services would be considered good news, but only if the acquisition system can be modified to be able to react by shifting resources to the Alpha program and to put in place an SLA to recognize the service reuse and the new inter-program dependency.

In fact, this scenario is limited because it still speaks in terms of programs or systems. If you take the DoD and Navy visions for net-centric operations enabled by rapidly fielded, reusable and user configurable applications to a logical extension, it makes more sense for organizations to develop interoperable services rather than complete systems. An integrating organization could then assemble a collection of services, arranged into workflows, to meet the combined mission requirements for a particular platform. Instead of systems, services become the key unit of functionality, which has huge implications for how we define, buy, test, accredit and field capabilities. This approach causes technical, schedule and cost risks shifting from relatively self-contained programs of record (POR) to solutions composed of services developed by multiple programs and organizations. In this case, project and acquisition program managers are unlikely to be pleased with having their success dependent on how well other programs execute. Instead, they may prefer to have their resource sponsors fund them to supply individual services rather than whole systems.

Today, we integrate applications into systems and then systems into platforms. In the near future, this model could conceivably shift to integrating services directly into platforms and bypassing the system level altogether. This raises the question of who is responsible for integrating these services. Additionally, concerns of how to partition requirements to services and then services to developers also arise.

Once you have partitioned requirements to the service level, you then have to distribute funding appropriately. Further, as the previous scenario shows, funding decisions are not just limited to the development phase, but have to be revisited throughout the life cycle of each service.

The Network Enabled Command and Control (NECC) program took one approach to allocating requirements and funding. Funding for the services' (Air Force, Army, Marine Corps and Navy) programs of record for command and control systems was shifted to the Defense Information Systems Agency (DISA) to meet

an agreed upon set of joint requirements. DISA, in turn, partitioned the money back to the services to develop sub-elements of the overall solution. Unfortunately, a perceived loss of both control and funding by the services led to significant "push back" against the NECC program.

The Global Command and Control System – Integrated Imagery and Intelligence (GCCS-I3) program, on the other hand, illustrates a "coalition of the willing" approach where individual programs retained their own funding but adopted a shared technical approach. The Consolidated Afloat Networks and Enterprise Services (CANES) development approach is midway between NECC and GCCS-I3 — all hardware funding shifted from individual programs of record to CANES, but the programs retained funding and responsibility for software development. In addition, CANES provides enterprise services that programs of record have been adopting, either voluntarily or by mandate.

Once requirements and funding are allocated to multiple services, two major aspects of development remain that need coordination and control: schedule and technical standards. Ideally, schedule alignment for services should not be an issue; services would be seamlessly interoperable, could undergo continuous development, and we could just implement the most recent version of a service as needed.

In cases where hosting the service is not required in-house, we can simply link the desired service into our workflows. This is a future goal because in the foreseeable future integrators of services at the system or platform level will still need to worry about interoperability and capability issues for each service that is tied to specific releases. Therefore, there will have to be some forcing function, typically integrated test events, to align development schedules and services. If failing any of these events, they are not fielded in that baseline and fall back to the next release.

That potential failure of services to work together is what we hope to prevent using appropriate technical standards. For the most part, we do not care what goes on inside a service, giving developers considerable creative and technical latitude. We do, however, care very much about the interactions between services, so that well-defined, rigidly enforced standards for data formats, inter-service communication and the use of common services (e.g., security services) are critically important.

How Do You Test a Services-Based System?

The fundamental challenge in testing services-based systems is the realization that it's not practical to test all possible combinations of services. While not every service can be used in combination with all other services, this still approaches an N-factorial problem in terms of combinations and permutations of possible service compositions. One way to address the challenge is to identify the critical mission threads for any given "system" (i.e., a deployed collection of services) and make sure you test all the service compositions that support those mission threads. This has the advantage of ensuring that what must work, works, and in theory, should test almost all of the services in at least one workflow because the majority of services we should be fielding are those supporting key missions.

A more generalized approach would be to test several mission threads against a collection of services to create an approved baseline of services known to work together and to then pick from this baseline of services to field on a specific platform. This is similar to the Global Command and Control System – Maritime "segment" approach where all segments are tested, but not every ship gets all segments.

With either of these two approaches, the test environment presents challenges due to the sheer scope of the services required. Using CANES as an example, there are Navy-specific enterprise services running locally on a ship, but they need to be able to hand off user credentials and requests for information to services that are off the ship (typically through Net-Centric Enterprise Services).

To fully test CANES you need the full CANES baseline (ideally spread across representations of several platforms), the naval telecommunications and Global Information Grid infrastructure that provides the connection, and all the other services (external to CANES) that support the mission threads under test. For this reason, SPAWAR and the Program Executive Office for C4I have developed the Enterprise Engineering and Certification labs and process to provide the very large-scale, distributed, end-to-end environment supporting this type of testing.

A key element of this approach is to get the certifying agencies involved in planning test events so that a small number of large-scale end-to-end tests can be performed to serve as the development, the interoperability and, perhaps, operational acceptance tests. This is supported by having the certification agencies involved in defining graduation criteria as services move up through maturity levels, as well as having them ensure that the test environment includes the platforms, mission threads and services necessary to meet test requirements. Another demand on the test environment is the level of instrumentation or sensors that will be required for SOA testing. We need to be able to collect the data needed to validate key performance parameters and other performance criteria — at the individual service level — and across the entire mission thread workflow. This baseline, end-to-end mission thread-based test approach is workable, but it does not answer the speed-to-capability requirement that is one of the selling points of

the SOA model. To achieve speed-to-capability, we also need the ability to test an updated version of a single service. This could be accomplished by plugging the updated service into the full baseline testing environment and re-running the full multiple mission thread test. However, there needs to be a less resource intensive way of understanding the touch points for single service and testing those elements of the service interaction, as well as for the correct service functionality.

How Do You Certify and Accredit (C&A) a Services-based System?

The challenges of achieving service/system C&A in a services-based net-centric environment range from dealing with the very newness of SOA and its evolving security model, to trust among various service providers, to the decades-old C&A experience in DoD's traditional stovepiped information systems. The modular, dynamic, distributed design of a SOA system goes against the underlying approach to C&A today. In a traditional system, you can define the exact components that make up the system, where they are located, what version of every software element they are running and all the physical and logical interfaces. With that knowledge, you can identify known weaknesses and verify, through testing, that vulnerabilities have been addressed. A SOA system does not have well-defined boundaries because the services that compose a system can be hosted anywhere on any hardware platform running any operating system. In addition, in a system design that allows for dynamic composition of services, we are unable to specify the full range of services that will be working together. Clearly, a new approach to C&A is going to be required.

How Do You Field a Services-based System?

Most of the challenges of fielding a SOA system have been addressed in previous sections; however, there are a few system delivery issues that still need to be addressed. Typically, a system is a collection of software applications, and a version of that system is a specific collection of specific versions of those applications. That concept can still carry forward in a SOA environment, if a single enterprise controls all of the services that make up a system. For example, the CANES program can develop, test and accredit a baseline version of the system and field that version to some collection of platforms. That works today because most, if not all, of the services in the CANES environment are running locally and the CANES program can ensure that the different versions of CANES can talk to each other.

However, in a distributed, joint, net-centric environment, this is not the most likely scenario. The likely future environment includes hundreds of different services, developed by different organizations and enterprises, both public and private, updated continuously and used by creative service members in ways not originally intended. Clearly, this requires a new approach to the concept of configuration management and release schedules that extends beyond the boundaries of any single enterprise.

The Way Ahead for C4ISR Acquisition

The technical challenges of implementing SOA systems, while not easy, are well-known. As illustrated by the cancellation of the NECC program, the programmatic challenges of implementing SOA may be greater. Realizing this vision of purely services-based systems is going to require significant changes in how we:

- Define requirements in terms of mission threads and services;
- Allocate requirements across multiple organizations for implementation of services;
- Allocate resources for the sustainment of services;
- Test services;
- Accredit systems composed of services; and
- Sustain systems composed of interdependent services.

Team SPAWAR is engaged on several fronts to help bring about the necessary changes. First, Team SPAWAR personnel have leadership roles on many of the programs that are leading the way to SOA, including: GCCS-I3, NECC, CANES and the Command and Control Rapid Prototype Continuum (C2RPC), to name a few. Second, SPAWAR's Net-Centric Engineering and Integration competency has created communities of interest to share SOA best practices and to develop SOA standards and policies. Finally, Team SPAWAR personnel are actively engaged in the current information technology acquisition reform efforts recently enacted into law in Section 804 of the Fiscal Year 2010 Defense Authorization Act. CHIPS

Lee Zimmerman is the national competency lead for net-centric engineering and integration for SPAWAR.
Antonio Siordia is on the net-centric engineering and integration staff for SPAWAR Systems Center Pacific.

Coming soon to a theater near you: VALIANT ANGEL

New integrated system allows far-forward warfighters access to the rapidly expanding motion imagery collection

By Nancy Reasor

Warfighters need to make decisions quickly, but managing and accessing the growing number of images and videos available has become increasingly difficult due to the proliferation of unmanned surveillance technologies. Making sense of the overwhelming amount of sensor data is another stumbling block where battlefield decisions must be made instantly.

But intelligence specialists at U.S. Joint Forces Command Intelligence Directorate (J2) will be fielding a system in April that will give warfighters the ability to access, archive and analyze the enormous number of images and video collected on the battlefield.

A Valiant Angel network operations center packed in preparation for deployment to Afghanistan. Using Valiant Angel, warfighters will be able to search and retrieve images of interest, including full motion video. Photo by Air Force Staff Sgt. Vanessa Valentine/USJFCOM photographer.

Valiant Angel will eliminate the need for videos and images to be physically transported between units or commands, which is both dangerous and time consuming, due to roadside bombs and poor road conditions. What's more, VA gives operators at every level the ability to fuse analysis with motion imagery records, exposing a larger community of warfighters to insights and analytic discoveries.

U.S. Joint Forces Command conducted a demonstration of Valiant Angel on March 17. Air Force Col. George J. Krakie, USJFCOM deputy director of Intelligence (J2), Norfolk Naval Support Activity, Va., explained that Valiant Angel uses commercial technologies that are standard in the motion picture industry and television, integrates them into a solution, and then packages them to fit into the military environment.

"We set out to enhance irregular warfare and our counterinsurgency operations by improving warfighter access to full motion video and wide area data over the existing networks that they have in theater now and to reach the guy at the tactical edge that may only have a laptop and a 56k modem," Krakie said.

Justin Thurber, operations officer for the Valiant Angel program, explained that the number of sensors that can be seen collecting data over a U.S. or joint base, or in Afghanistan, represents only a portion of the sensors that actually exist.

"We are talking about terabytes of data [produced] every hour, 24 hours a day, seven days a week. Gone are the days when we can allow [valuable] data like this to fall through the cracks to the cutting floor, never to be seen or used," Thurber said.

Instead, intelligence specialists will be able to analyze data to identify trends or locate persons of interest. Valiant Angel can also send automatic alerts when new images that match a warfighter's interests enter the system. Valiant Angel will use existing sensors and networks, and it is standards-compliant, so operators can use their own software or the VA software that provides additional capabilities.

The Valiant Angel software package improves operators' ability to search a secure, networked database. Operators will be able to conduct searches based not just on where and when the video was gathered, but also using key words, Krakie explained.

For example, users will be able to type in "explosion" and see all video in the system with that word in it. Valiant Angel also will provide alerts when specific intelligence a user designates becomes available.

"It enables users who don't have time to watch all the video to receive alerts that something they are interested in is coming across or available in the video archive," Krakie said. "I may not be able to sit there and watch the video today, but I want to know if any [roadside bombs] explode and we have video of that."

In addition to the thick client software provided by Valiant Angel, the VA team is developing a Web interface so that operators that do not have Valiant Angel software can use the Web interface to access some of its capabilities.

A Valiant Angel network operations center and VA nodes will be collocated near ground sites for existing sensors that will ingest sensor data. The NOCs will not store all the video, but will act as a "catalog" for available content. The configuration of a NOC will be different for each site based on the infrastructure of the bases slated to receive the equipment, Thurber said.

Andrew ("AJ") Forysiak, deputy program manager and technical manager for Valiant Angel, emphasized that a single version of Valiant Angel can take feed from numerous types of sensors.

"Every day a new sensor shows up in theater, and we are postured to take advantage of that sensor going into theater. We can do it by using traditional means. There are ground control systems, and we can put one of our nodes near the ground control station, take that feed, and make it available to the systems that are out there," Forysiak said.

March 17, 2010 – Valiant Angel demonstration. Background, Andrew ("AJ") Forysiak, deputy program manager and technical manager for Valiant Angel; center, Thaddeus Walker, Lockheed Martin; right, Justin Thurber, operations officer for the Valiant Angel program.

March 17, 2010 – Ramel Bush and Richard Tucker, with Lockheed Martin, demonstrating Valiant Angel. Photos by Air Force Staff Sgt. Vanessa Valentine/USJFCOM photographer.

The data that Valiant Angel will make available to warfighters may have only been available to a small number of warfighters in the past. Forysiak explained, "Our capability takes that information and makes it available to everybody on the network."

Valiant Angel is providing not only equipment and software but also instructions, training and support representatives, according to Krakie.

"The deliverables from this project are integrated hardware components, software for the users, training, CONOPS (concept of operations) and TTPs (tactics, techniques and procedures) for the users so they know what they are getting and how to use it. The final deliverable is field support representatives so that we don't just drop this equipment on an Army unit or Marine unit in the field and say: 'Good luck — here is your documentation — start working it,'" Krakie said.

Joint Interoperability Test Command (JITC), the third-party evaluator for this system, had evaluators on-site, to assure that they are sending embedded and tested capability to the warfighters in theater. JITC evaluators conducted lab testing with users from the Army, Air Force and National Geospatial-Intelligence Agency, in an environment replicating the architectural environment in Afghanistan.

Much of the Valiant Angel equipment was already in packing crates in preparation for shipping to Afghanistan, with fielding expected in April. Once the equipment is deployed, it will undergo a 60-day assessment. The remainder of the equipment will be shipped to Afghanistan and other locations in July or August with full operational capability expected in late summer.

Krakie explained that several U.S. military commands and agencies, as well as industry partners, were involved in the planning and development of Valiant Angel.

"Although Joint Forces Command is the lead and we are executing the Valiant Angel project on behalf of the ISR (Intelligence, Surveillance, Reconnaissance) Task Force," Krakie said, "it really has been a partnership between Joint Forces Command, USCENTCOM (U.S. Central Command), our partners at the National Geospatial-Intelligence Agency, and other combat support agencies, as well as partners in industry, and representatives from all the services including the Army and the Air Force who have been involved with the Valiant Angel program since its inception."

Once fully deployed Valiant Angel will dramatically improve intelligence, surveillance and reconnaissance for far-forward deployed troops. CHIPS

Valiant Angel can:

• Collect, store and rebroadcast incoming video streams from a variety of sensors in a secure, networked database.

• Fuse intelligence data from multiple sources into incoming video streams. For example, the system allows users to discuss a video clip over instant messenger and then will embed their chat history into the video stream.

• Categorize and manage videos by keywords, geographic region or other tags and set up alerts to inform users of new clips with their specific descriptions when they are posted to the network. For example, users can type in "explosion" and the system will show the user all the video with the keyword "explosion" in it.

Valiant Angel operational value:

• Provides access to previously unavailable motion imagery sources. It correlates and collates to assist finding relevant records.

• Packages information for access by bandwidth-constrained users, saving time and giving a more complete intelligence picture.

• Connects analysts input including chat and telestration (allows its operator to draw a freehand sketch over a motion picture image which amplifies data) to motion imagery and sends updates to tactical users as needed, limiting needed radio communication and conversation delays.

• Provides theater and reach-back intelligence support that takes into account all relevant collections.

• Gives all users the ability to access WAAS and tactical UAS collections and fuse analysis to motion imagery records, exposing the larger community to insights and analytic discoveries.

Nancy Reasor is the CHIPS assistant editor. For more information about Valiant Angel, contact USJFCOM public affairs officer at (757) 836-6559.

security for cloud computing

By Christopher R. Perry

Achieving and maintaining information dominance will require continuous and timely advances in both technology and operational processes. Cloud computing is one such rapidly emerging area of technology and operations that the Department of the Navy (DON) is already planning for and beginning to pilot. To achieve information dominance, it is vital that all new technologies and processes, such as cloud computing, be thoroughly evaluated prior to adoption or transition to proactively assess and address the associated cybersecurity requirements, vulnerabilities and risks. This article provides a preliminary look at some of the cybersecurity aspects and concerns related to cloud computing.

What is Cloud Computing?

There is no single, common and authoritative definition for the term "cloud computing." A simple Google search readily yields a wide variety of definitions, descriptions and explanations. An authoritative source, the Information Technology Laboratory of the National Institute of Standards and Technology (NIST) has published a two-page definition of cloud computing, now in its 15th version, which can be found at http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc.

The NIST definition states: "Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. …" It goes on to describe "five essential characteristics," "three service models," and "four deployment models."

While the NIST definition provides a generic overview and basic foundation to begin to understand cloud computing, the relative immaturity of the concept, the variety of implementations, and the rapidly evolving associated practices, result in causing the definition and understanding of cloud computing to take on a "cloud-like" quality — nondescript, fluffy and amorphous — open to individual interpretation.

The Challenge of Security

With the uncertainty surrounding the characterization of cloud computing, it should come as no surprise then that authoritatively and precisely specifying the security requirements and controls for cloud computing is an even greater challenge.

There is, however, some good news. Since most of the underlying building blocks (e.g., servers, network and storage devices, and software — operating systems and applications) of cloud computing remain the same as those used in traditional information technology systems, much of the existing security policies, practices and solutions can be readily repurposed to fit the new cloud computing paradigm.

The validity of the security principles, requirements and methods described, for example, in the NIST publications, Federal Information Processing Standards and Special Publications, or Department of Defense (DoD) guidelines, such as the Security Technical Implementation Guides (STIGs), remain germane. The main challenge is how to adapt the implementation of those longstanding principles to new business processes and relationships.

Apply Legacy Security Best Practices

The specific characteristics, service models, and deployment models of a cloud computing implementation, will affect how readily existing cybersecurity practices can be applied and implemented. The following are some of the security functions that will need to be adapted and/or addressed.

Security Controls Assessment and Operational Authorization. Cloud-based systems and services must be held to the same certification and accreditation (C&A) requirements as existing systems and networks. This includes security requirements definition, thorough system documentation, security controls assessment, risk analysis and ultimately the authorization to operate made by a Designated Approving Authority (DAA). The complexity of a centralized, shared and/or outsourced cloud environment could make this already arduous process much more difficult and may also require pre-negotiated service level agreements and contractual requirements that stipulate and include agreed-upon, recurring, and independent testing and verification.

Alternatively, leveraging a cloud service that has been intentionally developed with DoD security policies and requirements in mind could actually simplify and streamline the C&A process for the cloud customer. For example, the Defense Information Systems Agency (DISA) is developing a host-tenant accreditation model for its Rapid Access Computing Environment (RACE), which ensures compliance with the DoD Information Assurance Certification and Accreditation Process (DIACAP). For more information about RACE, go to www.disa.mil/computing/other/index.html.

Security Configuration Management. DoD and federal government agencies are in the process of applying common security configuration baselines to their systems. The DoD STIGs and the Federal Desktop Core Configuration (FDCC) standard is an example of this. Such configurations must be readily applied and promptly updated to deploy patches and modifications by the cloud service provider in response to emergent vulnerabilities and attack methods.

Additionally, life cycle configuration control practices, implemented with the oversight of configuration control boards, ensure that risks associated with system changes are properly assessed, understood and addressed. The governance, standards, management and oversight for ensuring adequate and reliable security configuration management must be proactively addressed and defined in advance of transitioning to cloud computing.

Cloud service providers must demonstrate that they exercise an equivalent and similarly disciplined process for security configuration management that takes into account the security and availability concerns and requirements of their customers. In some existing situations, migration to centralized cloud-based systems and services may actually better facilitate standardization and implementation of security configuration management, but at the same time, the potential complexity of a combined cloud environment could ultimately make it much more difficult to secure and fragile to maintain.

Shared Resources and Virtualization. The characteristic of rapid elasticity is commonly facilitated through resource pooling and the implementation of virtualized systems and networks. The vulnerabilities and security ramifications associated with virtualization are still being assessed, and the associated security best practices are still in the process of being developed and implemented.

Even longstanding security practices, such as those related to security configuration management, need to be adapted to ensure they are promptly and reliably applied to online and offline virtual images. Additionally, processing, storage and network communication resources that are shared through rapid reprovisioning must be thoroughly and reliably cleared or sanitized to preclude controlled information. System virtualization

and rapid reprovisioning could also potentially hinder or further complicate security incident forensics, and associated investigations could temporarily diminish access to cloud computing resources.

Continuity of Operations and Disaster Recovery. As with all current systems, proper measures must be taken to assure cloud-based systems and services reliably provide the requisite level of operational continuity and disaster resiliency. The inherent cloud computing characteristics of resource pooling and rapid elasticity can serve to enhance continuity of operations by ensuring prompt and reliable failover. However, unanticipated substantial resource overloading or denial-of-service conditions elsewhere within the shared cloud environment may inadvertently, unexpectedly or indirectly result in a cascading impact to another of the shared cloud-based systems or services.

Disaster recovery planning must be coordinated with the cloud service provider, thoroughly documented, and regularly tested or exercised to verify that the essential level of recovery can be attained within the requisite timeframe. Specific attention must be given to shared priorities and processes for restoration in the event of a complete catastrophic failure of a service provider's shared cloud computing site or its resident capability.

Authentication and Access Control. Many of the current user enrollment, identification, authentication and authorization mechanisms and processes rely on local or otherwise internal resources, services and processes. A cloud environment will either need to be able to leverage and apply these methods to its access control measures or reliably replace them with community or cloud-based alternatives offering equivalent or better protections.

Relocation or replacement of existing local and/or dedicated directories with remote, wide area network (WAN) based, and/or community directories may necessitate that additional security controls be applied to ensure that account management processes remain secure and trustworthy. Cloud services and applications must be public key-enabled and must readily interoperate with and fully implement DoD's existing Common Access Card (CAC)-based strong authentication processes.

Operation and Maintenance. The possible centralization, outsourcing and/or sharing of computing resources, brings with it the challenge of ensuring that all privileged users who configure, operate and maintain cloud-based systems, software and applications are properly cleared, controlled, monitored and audited commensurate with the collective level of sensitivity of the information being processed and stored by the shared system for which they are granted access.

Further, it must be verified that cloud service providers and their subcontractors comply with the training and certification requirements of DoD's Information Assurance Workforce Improvement Program (DoD 8570.01-M).

Data Portability, Protection and Sanitization. In addition to the confidentiality concerns associated with shared resources, processes and assurances should be established, agreed upon, tested and verified in advance that allow for data to be readily, reliably and securely transferred on and off the system, thus facilitating portability of the service. Additionally, procedures to reliably sanitize the systems and storage media need to be likewise defined, agreed upon, and tested in advance regularly, and independently verified thereafter.

Security Monitoring, Aggregation, Analysis and Reporting. As with security configuration management, the centralization of cloud-based systems and services may better facilitate access to, and the aggregation of, security related logs and metrics necessary for analysis leading to detection and reporting of security related events and incidents. Alternatively, it could just as easily make those processes much more complex, difficult and obscure; particularly in virtualized, shared, and outsourced environments. Existing organizational policies and processes for system monitoring, log and event data aggregation and incident reporting must be considered and accommodated when planning to use, or migrate to, a cloud-based solution.

Securely Transitioning to Cloud Computing

With the experience gained and associated lessons learned from the Navy Marine Corps Intranet (NMCI), the DON is well positioned to take the next steps toward transitioning to cloud-based systems and services. NMCI has already exposed the DON to the security ramifications of transitioning many critical IT systems to a centralized and outsourced environment on a large scale, where many of the security services and controls are contractually provided by an external entity.

While concurrently planning for the Next Generation Enterprise Network (NGEN), the Consolidated Afloat Networks and Enterprise Services (CANES) and, more broadly, the Naval Networking Environment (NNE) ~ 2016, the DON is able to proactively adapt, apply and build on the cybersecurity lessons learned from NMCI to secure future cloud computing implementations.

Additionally, the DON will be able to proceed in close coordination and collaboration with the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)), and other DoD services' and agencies' cloud computing initiatives. This will include DISA, which is already in the process of establishing the foundation for a secure Community Cloud for DoD. DISA's Rapid Access Computing Environment has been developed with DoD security policies and requirements in mind.

RACE uses a host-tenant accreditation model, standardized system configurations, the Vulnerability Management System (VMS) and the Enterprise Mission Assurance Support Service (eMASS) to ensure compliance with the DIACAP and the DISA Security Technical Implementation Guides.

Finally, the DON will be able to leverage and actively participate in the ongoing community efforts associated with cloud computing headed up by NIST and adopt and apply NIST's standardized security guidelines to the DON's emerging and evolving cloud computing initiatives. CHIPS

Mr. Perry is a retired naval officer and a Certified Information Systems Security Professional. Mr. Perry provides support to the DON CIO Cybersecurity and Critical Infrastructure Team.

Renewing and Improving Human Resources Processes to Support DON Cyber/IT Personnel

An interview with Chris Kelsall, DON CIO Cyber/IT Workforce Director and Tammy Johnson, Deputy Director, Human Resources Service Center, Northwest

The civilian cyber/IT workforce senior leadership across the De partment of the Navy regularly deals with new processes and procedures to accomplish the DON's IT work. Recently, the federal government di rected several new civilian human resources (HR) initiatives to include transition from the National Securi ty Personnel System (NSPS) back to the General Schedule (GS) system. While working new initiatives is time consuming, this effort can be seized as an opportunity to renew and sta bilize civilian workforce manage ment within DON commands.

Good HR practices often include in telligent trade offs between fund ing, people, automation, control, flexibility and timeliness. To be ef fective, senior leadership must be fully apprised of not only the cyber/ IT functional environment, but also HR responsibilities. They must be comfortable understanding the au thorities, resources and flexibilities available to the community, hiring managers and the people in the cyber/IT community.

Chris Kelsall, the cyber/IT workforce director in the office of the DON CIO, works closely with Tammy Johnson, deputy director, Human Resources Service Center, Northwest. Tammy is designated as the HR consultant to the cyber community.

By Mary Purdy

At the West Coast 2010 DON IT Conference, Mary Purdy sat down with Mr. Kelsall and Ms. Johnson to ask a few questions about civilian HR management in view of upcoming workforce changes.

Ms. Purdy: Why is the civilian workforce transitioning from the National Security Personnel System (NSPS) to other pay schedules, and what does this mean to the cyber/IT community?

Mr. Kelsall: The National Defense Authorization Act (NDAA) for Fiscal Year 2010 repealed NSPS. When passing the NDAA, Congress required all employees to be transitioned from NSPS no later than 1 January 2012. As the cyber/IT HR adviser, Ms. Johnson will work with our community to ensure a smooth transition.

Ms. Purdy: What is the DON's plan to transition out of NSPS?

Ms. Johnson: Most of the DON's NSPS employees will transition to the GS personnel system; this will take place during 2010, on a cycle over the next several months. Once transitioned to the GS, employees will not be eligible for a 2011 NSPS performance payout. However, as GS employees, they will be eligible for within-grade-increases and all recognition and rewards within that system. Until your NSPS organization transitions, NSPS rules will continue to apply.

Ms. Purdy: How does the cyber/IT community know what alternative pay plan to transition to?

Ms. Johnson: If the NSPS position was previously classified under GS, there has been no significant change in duties and responsibilities of the position, and the appropriate GS classification standard remains unchanged, then NSPS positions will revert to the GS classification and full grade level previously assigned.

Ms. Purdy: Do civilian position descriptions need to be updated right now?

Ms. Johnson: Very few PDs will require rewriting immediately. The transition period for completing the mass action to move employees from NSPS to GS is simply too short. Since rewriting a PD requires a personnel action to place the employee on the new PD, it would be a challenge to accomplish both in the allotted timeframe.

As a manager, you may be contacted by your HR representative if a GS determination cannot be made based on the current PD because some titling in NSPS does not exist in the GS. In the IT community, there are only two NSPS classifications that do not exist in the GS. NSPS classification 2203 (Computer Operator) will become GS classification 0332 (Computer Operations); and NSPS classification 2204 (Computer Technician) will become GS classification 0335 (Computer Assistant).

That being said, this may be a good time to pen and ink current PDs, ensuring conditions of employment (COE) (for the IA workforce) include the security clearance and the commercial certification requirements as defined in DoD and SECNAV manuals (DoD 8570.01-M/ SECNAV M-5239.2). At some later date when time permits, command HR personnel may update the PDs to include any newly defined work tasks and the new COE requirements.

Ms. Purdy: Cyber/IT personnel often comment about the lack of personnel to accomplish the required job tasks. What would you advise our commands to do?

Mr. Kelsall: First, we must understand the work that needs to be done. The cyber/ IT work requirement routinely changes, and must be considered as we continue to develop the right workforce to design, manage, operate, defend and secure our networks. A presidential directive issued

Jan. 8, 2008, formally established the Comprehensive National Cybersecurity Initiative. Under CNCI we are reexamining workforce roles. Additionally, there are numerous ongoing studies to review and refine competencies, occupation standards, manpower mix, and personnel and training requirements. Expect to see additional guidance in the coming year. While there are high level studies, in the end the work requirement must be defined within the command, and billet funding must be requested through the chain of command.

Ms. Purdy: We hear about new in-sourcing guidelines. What can you tell us?

Mr. Kelsall: On April 6, 2009, while introducing the FY 2010 DoD budget, Secretary Gates announced an initiative to rebalance the department's workforce and reduce the percentage of contracted services as compared to the department's organic workforce. His plan, which proposed an increase in government performance, oversight, and control of critical services, is commonly referred to as 'in-sourcing.'

Ms. Purdy: How can the DON shorten the hiring timeline, but ensure it is hiring the best qualified to fill new in-sourced positions?

Ms. Johnson: We forget that hiring the best qualified candidates is dependent upon active recruitment of those best qualified applicants. Simply posting announcements on the DON HR Web site isn't enough. As managers, we must continually market the positive aspects of working in the public sector and for our particular organizations. Many factors contribute to the hiring timeline, whether it is the impact of your local position management board, how long the announcement is posted, or your command's in-processing requirements such as medical or security requirements. The Corporate Business Process for Recruitment (CBP-R) is designed to ensure a consistent approach to the 'processing in' of new employees. It is still in the pilot stage and is being tested by Headquarters Marine Corps; the Assistant for Administration, Office of the Under Secretary of the Navy, Secretariat Headquarters, Human Resources Office; and Fleet Industrial Supply Center, Pearl Harbor.

Department of the Navy
Cyber/IT Workforce Directorate

Ms. Purdy: DoD 8570.01-M and SECNAV M-5239.2 documents require the cybersecurity/IA workforce [to] acquire commercial certifications and commence a continuous learning program. Do you expect the entire cyber/IT workforce to eventually move to similar training and certification requirements?

Mr. Kelsall: Yes, we are working with the Federal CIO Council and the DoD IT workforce integrated process team (IPT) to institutionalize a cyber/IT professional workforce to include career mobility and career growth by continuous learning.

Ms. Purdy: What are some of the tools the cyber/IT workforce can use to help achieve their training goals?

Ms. Johnson: Important tools include the Defense Civilian Personnel Data System (DCPDS), the Navy's Total Workforce Management System and Marine Corps Training Information Management System. In the DCPDS, My Biz Web-based tools allow personnel to access and manage their individual personnel records. Service directives provide guidance on the use of these workforce tracking and planning mechanisms. They help us collect metrics on our workforce, which in turn, help us provide better guidance for our cyber/IT community.

Mr. Kelsall: Other training support tools include e-Learning sites that house the SkillSoft online course library. The Navy IA workforce can access IT courses through https://navyiacertprep.skillport.com, and Marine Corps personnel will find the courses at http://www.marinenet.usmc.mil/. Both services can easily access the Defense Information Systems Agency IA Support Environment or Carnegie Mellon Virtual Training Environment, which have some government specific and commercial IT courses at http://iase.disa.mil/eta.

Ms. Purdy: Do you have anything else you would like to add?

Mr. Kelsall: In an effort to keep some enterprise workforce planning consistency, at the DON CIO, I host biweekly conference calls and hold monthly IPT meetings with our cyber/IT workforce managers. Other Navy and Marine Corps managers who provide timely IT community HR guidance are: Mr. Pete Gillis, HQMC, community manager, Marine Corps Information Technology Management Community of Interest; Mike Knight, Navy Cyber Forces Command, IA workforce improvement program manager; and all Navy Echelon II command information officers and workforce managers. CHIPS

Mary Purdy is the cybersecurity/IA workforce management oversight and compliance manager supporting the DON CIO Cyber/IT Workforce Team.

GOING MOBILE

Cellular Devices in Classified Spaces

By Mike Hernon, Tony Soules and Bob Turner

Not a week goes by without an inquiry to the Department of the Navy Chief Information Officer (DON CIO) or the Navy or Marine Corps Designated Approving Authority (DAA) regarding the desire to bring a commercial wireless device, usually a BlackBerry, into restricted areas where classified information is discussed, stored or otherwise processed.

These requests are not surprising given the increase in the DON's enterprise mobility capability. As this capability increases, our mobile devices become more closely integrated with our desktop environment — for both voice and data applications — and more critical to our ability to perform our jobs.

Many people, of course, work full or part time in environments where these devices are prohibited and most tend to accept the prohibition as a function of their job requirements. On the other hand, for the many people whose jobs occasionally entail going into classified areas, the prospect of being without the information stored on the device even for a short period of time is viewed as a significant impediment and has led to this rise in inquiries.

Regardless of your job requirements, if you fall into the category of wanting this capability, well, there is a policy for that!

DoD Policy, "No, but…"

The standard reply to an inquiry regarding bringing a commercial cellular device into a classified space is "No, but…" As in all things wireless, we turn for overarching guidance to DoD Directive 8100.02, "Use of Commercial Wireless Devices, Services and Technologies in the DoD Global Information Grid." The relevant sections state:

> *4.2. Cellular/PCS and/or other RF or Infrared (IR) wireless devices shall not be allowed into an area where classified information is discussed or processed without written approval from the DAA in consultation with the Cognizant Security Authority (CSA) Certified TEMPEST Technical Authority (CTTA).*
>
> *4.3. Wireless technologies/devices used for storing, processing, and/or transmitting information shall not be operated in areas where classified information is electronically stored, processed, or transmitted unless approved by the DAA in consultation with the CSA CTTA. The responsible CTTA shall evaluate the equipment using risk management principles and determine the appropriate minimum separation distances and countermeasures.*

Therefore, while the presumptive answer is "no," if there is a bona fide mission requirement, there may well be a way of getting your BlackBerry into that restricted space — but you have to convince your local security authority and the DAA first. Their risk management evaluation will weigh the benefits of such approval against the security risks inherent in the scenario of cellular devices in an area where there is also classified information.

Risky Business

You may ask, "How risky can it be? After all, I use this device everyday and have never had a problem." The answer is that it can be very risky indeed, to the point that you could potentially be the source of a compromise of classified information and would never even know it. To gain an appreciation of the risk, go to your favorite Internet search engine and search for "cellular vulnerabilities" or a similar phrase. The results may surprise you.

Although we refer to them as mobile "phones," any cellular device is actually a mobile radio, one that receives and transmits just like any other radio. Furthermore, they do a fair amount of transmitting and receiving on their own outside of your oversight or control.

Regular readers of *Going Mobile* may recall during the discussion of texting, that cellular networks operate on two distinct sets of channels — the traffic channel where your calls and data sessions are conducted, and the control channel which handles network maintenance, operational tasks and text messages (see "Going Mobile: Putting Text to the Test," www.chips.navy.mil/archives/09_oct/web_pages/Going_Mobile.html).

Some of the tasks that are conducted over the control channel include the phone letting the cellular network know where it is (and, by extension, where you are), call set-up and initiation. The control channel can also put the phone in diagnostic mode, which includes turning on the microphone. This, in a nutshell, is the primary reason that cellular devices are not allowed in classified spaces.

Using the control channel, an adversary or run-of-the-mill hacker could turn on the microphone — without any visible change in the phone's appearance — and freely listen in. Thus, you have just brought a bug into an area where classified information is now being transmitted into the ether. Not a pleasant scenario.

In addition to the inherent cellular vulnerabilities, all electronic equipment is capable of emitting electronic emanations. This is where TEMPEST (Transient Electromagnetic Pulse Emanation Standard) practices come into play. TEMPEST refers to the shielding of these electromagnetic emanations, which is different than the actual interception of these emissions.

Due to the vulnerabilities associated with electronic equipment in general, it is mandated that the CTTA play a role in accepting the use of these devices in classified spaces.

Process and Practice

Given these risks, it is clear why the presumptive answer is "no." If, nonetheless, you still believe there is a mission requirement to maintain possession of your cellular device when in an area where it is normally prohibited, you may begin the process outlined in DoDD 8100.02 by consulting with the CSA for the location in question.

It is important to note that the risk management and approval processes are tied to specific locations — not to individuals or job functions. While there are general vulnerabilities shared by all wireless devices, the specifics of any given location could either mitigate or aggravate the risks that would be incurred by the introduction of a device.

If approved, the practice is managed locally under the overarching guidelines specified by the DAA. Day-to-day compliance monitoring and enforcement of any mitigation actions would be conducted under the auspices of the CSA for the location. Such mitigation actions could include allowing only government-owned and inventoried mobile devices into the Sensitive Compartmented Information Facility (SCIF).

Disabling all radios while in a SCIF should be strictly monitored and enforced as well (e.g., through the use of cellular detection systems). In addition, requiring mandatory user awareness training should be implemented for all users who work in classified environments.

Future

It is likely that the desire to utilize BlackBerrys and other commercial cellular devices in classified spaces will only grow. However, the vulnerabilities of devices designed for consumer consumption will not be easily overcome. Even the secure mobile environment, portable electronic device (SME PED), recently deployed, is prevented by DoD policy from being brought into an area where classified information resides — and it has a "SCIF" switch that turns off the radio.

Moving forward, the DON remains engaged with industry and our government partners to develop additional, secure use cases for commercial, cellular-based technologies.

We are also engaged in a review and re-write of DON wireless policy; you may participate by joining the discussion on the Pulse, the DON collaborative site for the information management community (https://www.doncio.navy.mil/pulse (CAC-enabled)). CHIPS

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

Tony Soules supports Headquarters Marine Corps C4 Information Assurance in wireless technologies and solutions.

Bob Turner supports the Naval Network Warfare Command office of the Designated Approving Authority.

JSTeF 2010:
Crucible of Innovation

Annual Joint Tactical Radio System forum provides a marketplace to connect buyers and sellers, promotes entrepreneurial business models and encourages game-changing innovation

By Mike Daily

When Charles H. Duell, Commissioner of the U.S. Patent and Trademark Office, claimed in 1899 that: "Everything that can be invented has been invented" — he certainly could not have foreseen the innovation spurred by ever-changing threats, increasingly sophisticated adversaries, extreme and hostile environments — and defense research in the last 111 years.

In this spirit of innovation, the Joint Program Executive Office for the Joint Tactical Radio System (JPEO JTRS) sponsored its fourth annual JTRS Science and Technology Forum (JSTeF), March 9-11, 2010, at the University of California, San Diego (UCSD), in conjunction with the Wireless Innovation Forum (WINNF) and the California Institute for Telecommunications and Information Technology (Calit2).

The forum objectives included building relationships with academic institutions, growing a domestic vendor base and national talent pool; promoting common military/commercial software-defined radio (SDR) standards and architectures; and recruiting U.S. citizen-engineering students into the SDR field.

Mr. Howard Pace, acting Joint Program Executive Officer for the Joint Tactical Radio System, discusses the importance of JTRS wireless communications and networking capabilities for the DoD, and the critical roles played by industry and academia in developing future software-defined radio capabilities.

Rear Adm. Janice M. Hamby, Vice Director for C4 Systems (J6) Joint Chiefs of Staff, observes a capabilities demonstration from a JTRS Small Business Innovation Research (SBIR) exhibitor. Photos by Erik Jepsen/UC San Diego.

About JPEO JTRS

The JPEO JTRS, headquartered in San Diego, Calif., was formed in early 1997 to improve and consolidate the services' pursuit of separate solutions to replace existing legacy radios in the Department of Defense inventory. The JTRS program has evolved from separate radio replacement programs to an integrated effort to network multiple weapon systems platforms and forward combat units where it matters most — the last tactical mile. JTRS will link the power of the Global Information Grid to the warfighter to apply fire effects and achieve overall battlefield superiority.

JTRS is developing an open architecture of cutting-edge radio waveform technology that allows multiple radio types (e.g., handheld, aircraft, maritime) to communicate with each other. The goal is to produce a family of interoperable, modular software-defined radios which operate as nodes in a network to ensure secure wireless communication and networking services for mobile and fixed forces. These goals extend to U.S. allies, coalition partners and disaster response personnel.

Forum of Collaboration

Attended by defense, industry and academic leaders, the conference featured three days of presentations and exhibits by recipients of JPEO JTRS Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) contract awards, who demonstrated their projects with an aim for potential integration into defense or commercial applications and products. The forum also provided opportunities for information exchanges and tours of Calit2 research laboratory exhibits and facilities. Exhibitors and presenters explained new developments in cognitive radio, dynamic spectrum allocation (DSA), ultra wideband antennas and power amplifiers, modeling and simulation tools, software test tools, and enhanced waveforms.

The opening address was delivered by Acting Joint Program Executive Officer for JTRS, Howard Pace, who discussed the importance of JTRS wireless communications for the DoD and the critical roles played by industry and academia in developing future software-defined radio capabilities. Other noteworthy speakers included Rear Adm. Janice M. Hamby, Vice Director for C4 Systems (J6) Joint Chiefs of Staff and Rear Adm. Michael C. Bachmann, Commander, Space and Naval Warfare Systems Command (SPAWAR).

Pace's remarks underscored a sense of urgency for continuous improvements to meet the warfighters' need to maximize operational effectiveness and minimize coalition and civilian casualties. He also cautioned against underestimating an adversary's capabilities.

Human innovation is a global resource, and globally available commercial and consumer technologies can be adapted for wartime use. Pace counseled attendees that shrinking budgets require "doing more with less." He said we must take advantage of technology's ability to improve and add new capabilities while reducing costs.

This annual forum fosters strategic dialogue between JTRS government stakeholders, large defense businesses, small business entrepreneurs, universities, and other organizations.

"[The forum] provides a marketplace to connect buyers and sellers and promote economic development of research and entrepreneurial industry," Pace said.

JTRS is much more than a radio replacement program; it is a wireless communications device, a router and an access point — all in one secure environment.

Forum participants were challenged to build on the software-defined capabilities of a JTRS radio beyond traditional communications and to focus on development of cyber-hardening defenses to keep the network secure. The result of these efforts would include improved joint force supportability through reduced manning requirements, streamlined training and improved logistics support.

The conference identified several areas requiring technology insertion for joint, coalition and first responder communications, including the Next Generation "Mobile Ad Hoc Network" (MANET) and network management of multiple MANETs at the tactical edge. Improvements are needed in enhanced user interfaces, battery technology and lower procurement and maintenance costs.

Conference attendees witnessed a revolutionary demonstration of the Project 25 (P25) waveform, developed jointly by UCSD and JPEO JTRS, which is capable of providing interoperability between U.S. first responders and the DoD to be used in emergency situations like Hurricane Katrina or the recent earthquakes in Haiti and Chile.

Interoperability for a first-responder participant requires public safety agencies (fire, police, medical) to have direct communications when they operate with one another across disciplines and jurisdictions. In order to facilitate this communication goal, agencies are looking at non-military waveform standards such as P25.

Using a standardized suite of waveform standards allows radio sets, manufactured by different vendors, to communicate. Ultimately, porting the P25 waveform to JTRS radios will allow military organizations to interoperate with state and local agencies in times of an emergency, such as a disaster relief scenario.

The conference highlighted that the era of SDRs for military tactical communications is here with flexible, field-reprogrammable radio systems. At the same time, the JTRS Enterprise Business Model is providing cost effective interoperability and capabilities among multiple form factors and vendors.

Improvements and Evolution

Networked tactical communications is not the end product of JTRS but the beginning of new joint and coalition capabilities. Open architecture and government-owned software enable continued business opportunities and innovative technology insertion to JTRS product lines, maintenance and upgrades to existing products, and new products to support emerging requirements.

As JTRS prepares to transition from Increment 1 design and development to production and sustainment, the effort of small business innovation research organizations will be a key component of a successful trend of continued JTRS product improvement and evolution.

Join us next time — the next JSTeF forum is scheduled for March 2011. For more information please visit http://jtrs.calit2.net. CHIPS

Resources:
JPEO JTRS: http://jpeojtrs.mil
WINNF: www.wirelessinnovation.org
Calit2: www.calit2.net
JSTeF: http://jtrs.calit2.net/

For more information about JPEO JTRS, please contact the director of Strategic Communications for JPEO JTRS at (619) 524-5701.

MIDS JTRS Receives NSA Certification

The Joint Program Executive Office for the Joint Tactical Radio System (JPEO JTRS) has announced that the Multifunctional Information Distribution System Joint Tactical Radio System (MIDS JTRS) has received National Security Agency (NSA) certification to provide secure distribution of situational awareness and command and control information among airborne warfighters. The NSA certification was granted March 9, 2010 by Mr. Richard C. Schaeffer Jr., director for the NSA Information Assurance Directorate (IAD). This is the first JTRS product to be certified at this level of security by the NSA.

"Formal NSA certification is a monumental accomplishment for the MIDS JTRS program and the JTRS enterprise. This is another first for MIDS JTRS as the program continues to blaze new trails and pave the way for other JTRS products to be successful and meet warfighter requirements.

"The MIDS program office has been working extremely close with NSA for over six years to bring this leading edge, next generation technology to the warfighter at the right time. I want to thank NSA, the MIDS JTRS vendors, and all the government personnel for their outstanding work. This is huge for the MIDS JTRS program," said Navy Capt. Scott Krambeck, MIDS program manager.

The NSA certification confirms that the MIDS JTRS terminal has met the highest standards in ensuring the confidentiality and integrity of the data and the availability of the system.

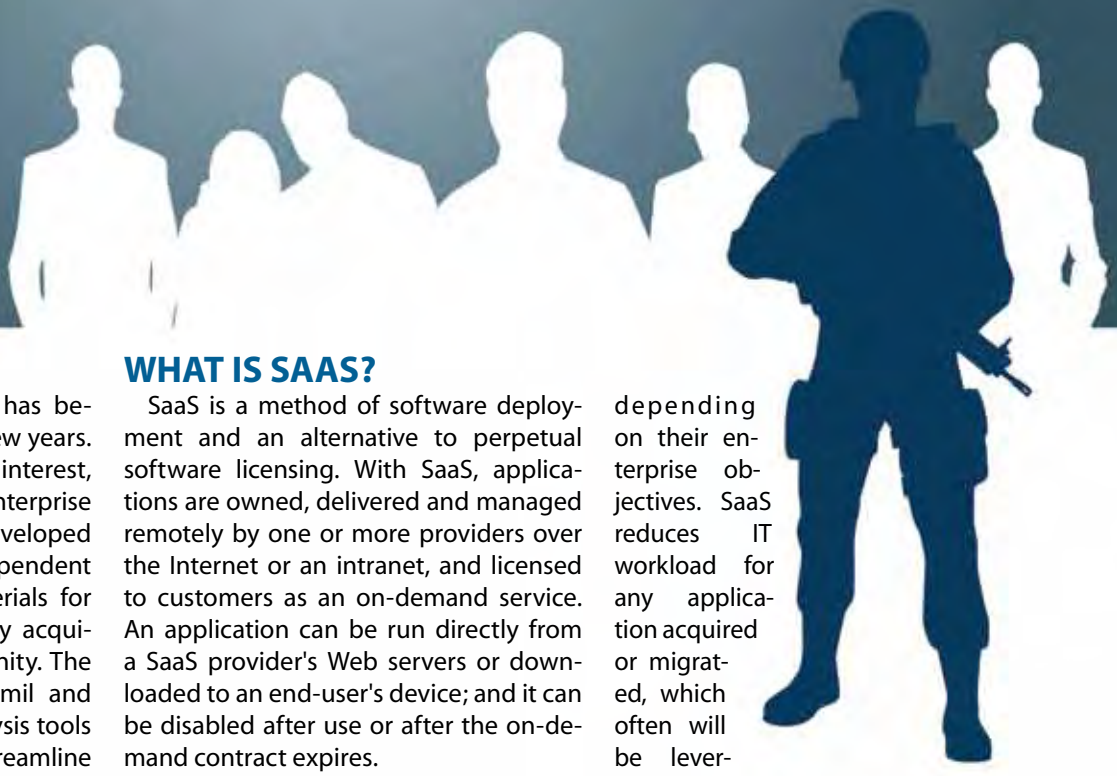
NSA certification is a critical milestone in support of the Initial Operational Capability (IOC) for MIDS JTRS on the F/A-18E/F Super Hornet. A successful NSA Technical Review Board (TRB) was conducted on MIDS JTRS in December 2009 which was the precursor to this NSA announcement.

The MIDS JTRS terminal is the first in a series of networking systems that will provide a single chassis, multiple channel capability to the warfighter, significantly reducing the number of different and unique radios in the operational environment. Use of JTRS radios also means a very real reduction of the upkeep and spare parts necessary to support forward deployed forces. CHIPS

SaaS

SOFTWARE AS A SERVICE

BY CHRIS PANARO



INTRODUCTION

Software as a Service (SaaS) has become a hot topic over the past few years. As a result of this heightened interest, the Department of Defense Enterprise Software Initiative (DoD ESI) developed the SaaS Toolkit to provide independent and unbiased educational materials for the DoD information technology acquisition and management community. The toolkit is available at www.esi.mil and provides access to decision-analysis tools and contract-related forms to streamline the process of understanding, evaluating and acquiring SaaS offerings throughout the DoD. This article captures some of the key educational content from the toolkit and explains the key differences between perpetual licensing and the SaaS model.

WHAT IS SAAS?

SaaS is a method of software deployment and an alternative to perpetual software licensing. With SaaS, applications are owned, delivered and managed remotely by one or more providers over the Internet or an intranet, and licensed to customers as an on-demand service. An application can be run directly from a SaaS provider's Web servers or downloaded to an end-user's device; and it can be disabled after use or after the on-demand contract expires.

SaaS falls within the overarching delivery model that packages technical offerings "as-a-service." This includes Infrastructure-as-a-Service and Platform-as-a-Service. These other offerings are not addressed in this article or in the SaaS Toolkit.

With on-premises, perpetual software licensing, the customer owns, operates and maintains software applications and the hardware servers that support the applications. With a SaaS model, the SaaS provider owns, operates and maintains the software and supporting hardware servers, which also reduces the customer's data center floor space and utility requirements.

Effects on the major asset of talented, skilled IT staff varies for customers depending on their enterprise objectives. SaaS reduces IT workload for any application acquired or migrated, which often will be leveraged to free IT staff to focus on more important tasks (since there are fewer applications, systems and data center facilities to maintain). See Table 1 for a summary of SaaS benefits.

HISTORICAL VIEW

In the early years of the commercial computer industry, applications were bundled with computer hardware which, over time, became too expensive for vendors. The first software firms started in 1960 to support universities and businesses seeking to perform specific computing tasks.

The software industry began to expand rapidly with the introduction of personal computers in the mid 1970s.

In general, there are several promised features and benefits to a SaaS model.

Feature	Benefits
Reduced up-front capital requirements	• Reduces up-front costs of application(s) and implementation. • Reduces costs of hardware, maintenance and data center space to support application(s). • Avoids costs of software upgrades (automatic software updates by the SaaS provider). • Shifts software management from customer to SaaS provider. • Reduces IT support requirements for help desk and end-user training. • "Pay as you go" reduces/eliminates cost of capital. • Improves IT budgeting with lower and predictable monthly or annual fee.
Speed of implementation	• Applications available in less time.
Configurability	• Goals to expand value and usage within enterprises continue to drive industry advancements. Mature SaaS solutions come with many permutations that allow customers to meet unique requirements. Many SaaS providers offer tool sets that allow customers to design workflows, reports and user interface elements. SaaS also leverages the service oriented architecture model to expose functionality to other applications and incorporates data and functionality from other applications delivered as a service.
Simplicity for end-users	• Encourages high end-user adoption. • Requires less time to ramp up new users.
Improved flexibility	• Allows scaling users and functionality up or down as requirements change. • Avoids speculating and paying for excess capacity. • Allows hedging commitment to a particular type of software or software vendor (can discontinue use when contract expires versus the risks associated with committing to an on-premise software).

Table 1. SaaS Features and Benefits.

This included businesses involved in the development, delivery and maintenance of computer software, as well as consulting services for product selection, implementation and training.

The expertise and resources required to deploy and maintain increasingly sophisticated business software applications created opportunities for alternative forms of software delivery models. While service bureaus have provided some technology-based services, such as those for payroll processing, since the 1960s, the concept of application service providers (ASPs) emerged as a viable alternative to on-premise software licensing in the late 1990s. Among ASP business models, which include SaaS and managed hosting services, the market for SaaS solutions has gained far more momentum in the 21st century. See Figure 1 for a historical overview of fee-based applications software development.

PRICING

SaaS fee structures can vary greatly by application and service provider. At the most basic level, there are two general pricing models:

- Subscription pricing based on a per user, per functionality, per month/year fee; and
- Usage-based pricing with metrics such as number of transactions over a fixed period of time.

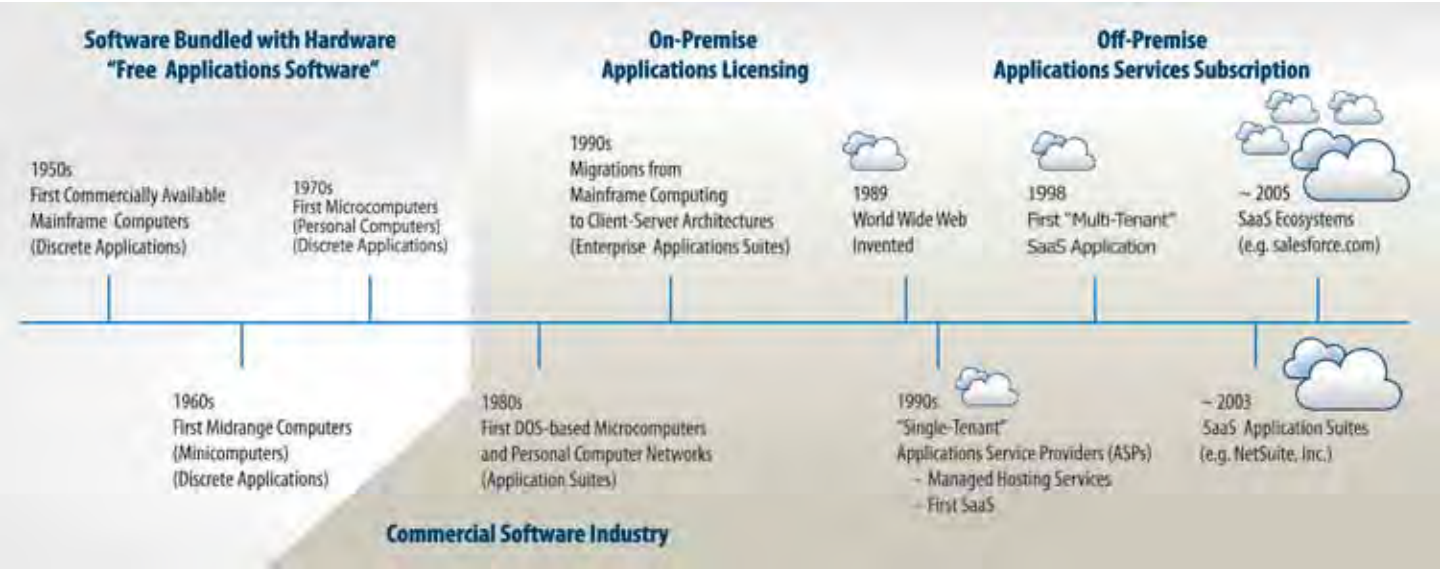


Figure 1. Historical Perspective on Fee-Based Application Software Development.

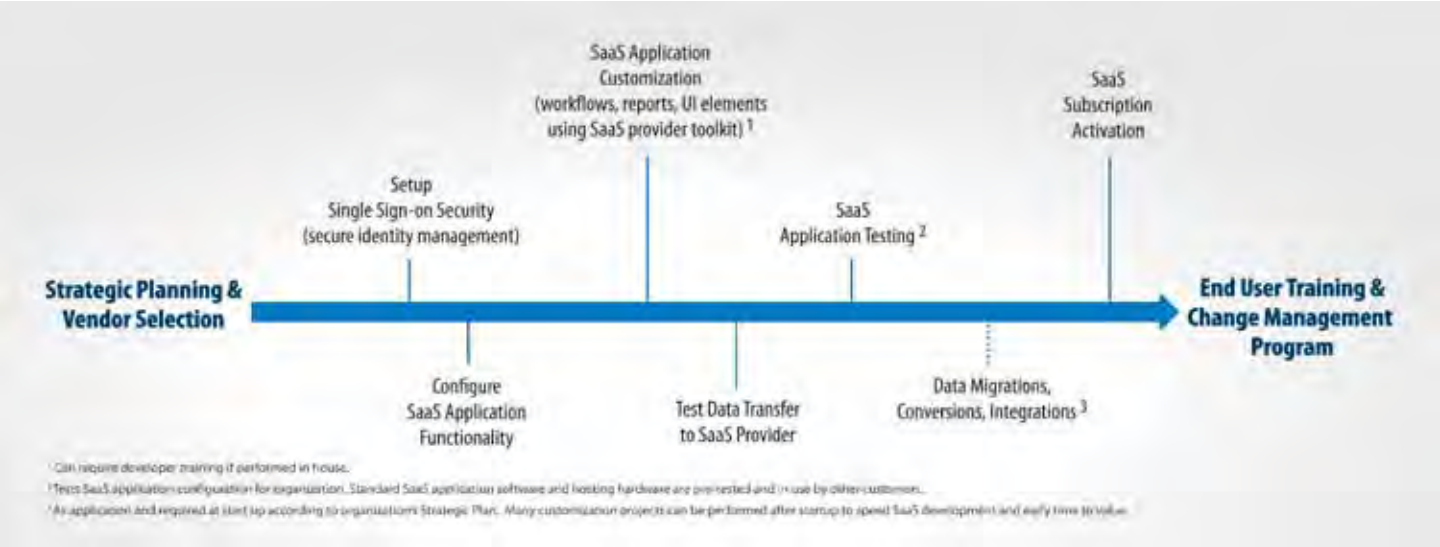


Figure 2. SaaS Implementation Roadmap.

Providers can charge a flat rate for unlimited access to some or all of an application's features, or varying rates that are based on number of users, application features, applications versioning, etc. (Note: A managed hosting service that requires a customer to license software and purchase or lease hardware servers is not SaaS.) Pricing can be affected by the providers' architectural models.

Multi-tenant (one-to-many) "pure" SaaS providers operate with the greatest economies of scale and pricing flexibility. Pricing can also be affected by a customer's special needs. A requirement that data cannot be transferred to any offshore location, for example, can impose additional operating costs on a service provider and therefore increase pricing to the customer.

IMPLEMENTATION

Roadmap

Most SaaS providers and third party systems integrators offer consulting services to help configure SaaS offerings to achieve a customer's objectives. Many independent consulting firms now include SaaS implementation in their services portfolio and several firms specialize exclusively in SaaS planning, implementation, training, change management and long-term support for follow-on integrations with other SaaS or on-premise software applications. Implementation processes range from simple to complex, depending on the scope of the business solution to be achieved. For applications that can be addressed by SaaS — and more appear on the market virtually every day — implementation tasks and time to deploy are significantly less than attempting the same solution with an on-premise software implementation. Figure 2 provides the major steps for implementing SaaS.

New Applications vs. Migration

It is generally agreed that data conversions and migrations can be as difficult for SaaS as they are for on-premises software. However, this thinking is evolving since SaaS delivers new "net native" applications that can be more easily integrated with any software available as-a-service (i.e., service oriented architecture). SaaS providers are also making advancements with new software frameworks and tools to reduce the cost of converting a traditional software product and/or building a new SaaS equivalent.

Typically, new SaaS applications are easier to implement, even if some functionality must be surrendered. Large organizations have an advantage of seeing that functionality restored through their SaaS solution by leveraging their business value to the SaaS provider in contract negotiations. Many SaaS providers will invest in accommodating new functionality to secure a large organization's business and to attract other like business from the growing prospect pools.

When evaluating a migration from a perpetual license to a SaaS alternative for use of the same software publisher's technology, there are additional financial issues to be raised. First, since a significant investment has already been made in the up-front license fee for the perpetual license, the negotiation of the SaaS price per month should allow for discounting or a credit since you already possess the license. Ask the SaaS provider for appropriate price concessions to reflect these existing licenses.

Second, it should be clear that your existing application, as configured and interfaced, should be maintained by the provider. This results in a relationship that is more aligned with an ASP than a pure SaaS model since you will want the title to the application to remain with the client.

In any migration from a perpetual license to a SaaS alternative that results in excess perpetual software licenses, the excess licenses should be made available for possible reuse within the DoD IT asset management framework. See Table 2 for a summary of pros and cons to be considered when evaluating a SaaS solution.

CONTRACTING

Service level agreements (SLAs) provide an agreed upon framework for the delivery of services and the measurement of service quality. SLAs are negotiated between the provider and the user to ensure that the expectations of services are realistic and within the provider's capabilities. SLAs provide detailed specifications of services to be delivered, the costs of delivering those services, the services'

When evaluating a SaaS solution, the following pros and cons should be considered.	
Pro	**Con**

Reduced risk and cost of acquiring software	• SaaS contract terms:
	  • Minimum term lock in.
	  • Potential hidden costs for increased numbers of users and expanded capabilities.
	  • Potential for uncapped price hikes on contract renewal.
	• Still a need for implementation process consulting.

Shift software management to SaaS provider	• Information security: Internet must be used to access data.
	• Some loss of control over data and business function.
	• Breadth and depth of functionality: customers must generally accept applications as provided or pay premiums for exceptions that increase a provider's costs.
	• Becoming dependent on SaaS provider(s) to perform business function:
	  • Long-term financial viability of SaaS provider is key.
	  • Changes in marketplace affecting levels of service or pricing at time of contract renewal.

Applications integration and Service Oriented Architecture (SOA)	• While many applications integration issues can be overcome with the evolution of SaaS application suites and ecosystems, SaaS integration with remaining on-premise systems can be problematic.
Disaster recovery and business continuity	• Providers can rely on offshore facilities for primary or backup business continuity and disaster recovery operations. Organizations bound to prohibit or limit transfer of data to offshore locations may not be accommodated or may be required to pay a service premium for additional costs to the SaaS provider.
Total Cost of Ownership	• Benefits unproven beyond five-year horizon due to lack of maturity of SaaS solutions and opportunities for analysis of return on investment over an extended period of time.

Table 2. SaaS Pros and Cons.

availability, problem management criteria and performance measurements. It is important to be accurate about the required level of service and how costs are determined for the varying levels of service required. The SLA should address what constitutes lack of service, how a failure to meet service levels is remedied and what happens if the SaaS subscription expires or is terminated. The contract should very clearly address what happens if the SaaS provider is sold or goes out of business or otherwise can't deliver the service required. For instance, all data must be transmitted in a format directed by the buyer to a location directed by the buyer within a clearly defined number of days after notice from the buyer. For critical applications, an escrow provision or third party escrow agreement should be entered to place the source code in escrow in the event the provider files for bankruptcy or closes its doors.

To assist DoD programs in the development of SLAs for SaaS, the DoD ESI is developing a Service Level Agreement Template and a Service Level Agreement Checklist to be made available in a future version of the SaaS Toolkit.

Figure 3. SLA Development Cycle.

SLA Development Process

Figure 3 illustrates the process that may be used when drafting and negotiating a SLA. This process may be helpful in guiding the contracting and program team in developing an SLA that meets the business and technical requirements desired.

SaaS is a software delivery model that should be considered by DoD programs but evaluated very carefully before selection. The SaaS Toolkit, located at www.esi.mil, should be consulted to provide a foundation of knowledge and access to tools to help any DoD program office decide if SaaS is the right model for its program. CHIPS

Chris Panaro supports the DON CIO Enterprise Commercial IT Strategy Team. He can be reached through ESISupportTeam@navy.mil.

Unmanning Unmanned Systems

By Thomas Kidd, Mikel Ryan and Antonio Siordia

The growth and diversity of military unmanned aerial vehicles (UAV) in the first decade of the 21st century has been unprecedented. To say that UAVs: "continue to be the most dynamic growth sector of the world aerospace industry" understates the obvious. "An insatiable demand for UAVs is fueling massive growth within this market," said Mr. Larry Dickerson, senior unmanned systems analyst for Forecast International. "No matter how many UAVs are built, military agencies want more."

Dickerson notes that a few years ago, UAV contracts in the millions of dollars were big news; now these awards are in the billions. "In addition to procurement, research funding for UAVs could exceed $20 billion through 2018," he added.

And while UAVs may be in the spotlight, unmanned systems aren't limited to air. Unmanned ground, air and sea systems are all force multipliers. They reduce the dangers to warfighters and represent a critical evolution in how the departments of Defense and Navy deploy military technology. But are unmanned systems truly unmanned?

More often than not unmanned systems are remotely operated via a strict and bandwidth-intensive electromagnetic tether. Radio communications between the unmanned system and a control station sequester the operator from the vehicle, but do not truly remove the man from the unmanned system. Maintaining positive control over a remotely operated vehicle requires highly reliable yet complex radio links. It also limits the capabilities of the system to those actions a remote operator can control.

Technological advances will eventually enable unmanned systems to evolve beyond their current remote-control architecture, an evolution necessary if just to somewhat relieve the burden these systems tend to impose on a finite, crucial, congested and contested resource: the electromagnetic spectrum. In this article we will examine some of the challenges as we remove the man and woman from unmanned systems and consider the future of autonomous unmanned vehicles (AUV).

It is generally accepted that a fully autonomous system would have the ability to:

- Gain information about the environment;
- Work for an extended period without human intervention;
- Travel from point A to point B to point C, etc., without human navigation assistance;
- Detect objects of interest such as people and vehicles;
- Avoid situations harmful to people, property, or itself (except when part of its mission); and
- Defend and repair itself without outside assistance.

An autonomous system may also be able to:

- Learn or gain new capabilities without outside assistance;
- Adjust strategies based on its surroundings; and
- Adapt to surroundings without outside assistance.

So why can unmanned systems be such spectrum gluttons? Unable to attach a 10,000-kilometer fiber optic cable, we link the unmanned system to manned support via bandwidth-intensive wireless data links. Human eyes are replaced by numerous wideband streaming video channels. Instruments and gauges are monitored by operators oceans away.

Unmanned surveillance systems transferring multispectral data from infrared and ultraviolet sensors take up a staggering amount of bandwidth, as do both standard and high-speed, full motion video. Also, consider that to reach a geographically remote control station the unmanned system mission and control data must be retransmitted, usually via satellite, effectively doubling the bandwidth required. A Predator, Reaper or Global Hawk UAV, for example, can easily take up to a full transponder on a satellite to transfer data.

"The demand is huge because commanders no longer want pictures taken last week; they want streaming video with enough clarity and fidelity to anticipate the actions of the enemy," said retired Army Maj. Gen. Robert Scales, a military historian. "Thus, we are not even within five percent of what's really needed."

A Pentagon presentation in 2008 showed demand for video was more than four times the supply and increasing exponentially. Currently, tactical Predators and Reapers supply more than 400 hours of video daily. Some of these warfighter platforms have expanded to carry 10 cameras today and will mount up to 30 by 2011, adding to the profusion of video and further exhausting scarce electromagnetic assets.

Beyond the immediate issue of bandwidth and spectrum constraints, the ability to leverage the host of imagery and signals intelligence is quickly becoming unmanageable. Much of the imagery gathered during collection is either lost to information overload because humans cannot adequately process it in real time, or it serves little purpose since today's processing power and analytical algorithms are inadequate to meet either supply or demand. As data gathering exponentially increases, hiring more analysts is not a viable option.

Future development must not simply focus on greater autonomy in the unmanned vehicle. We must also recognize that both real-time and post-operation analyses are two sides of the same coin. Some type of autonomous analysis needs to take place on the vehicle if we hope to sever the contstant link

between platform and operator. The system could still keep a human in the loop for firing at urban ground targets. The vehicle would only need to share relevant imagery and wait for permission to fire.

The primary goal of autonomous unmanned systems must remain reducing the danger to the warfighter. But autonomous unmanned systems must have a secondary goal of increasing the efficacy of our forces as a force multiplier of intelligence, surveillance and reconnaissance (ISR) assets. And by cutting the electromagnetic umbilical cord, autonomous unmanned systems will be much more spectrum efficient.

Lastly, there will be eventual cost savings of autonomous over manned and unmanned based systems — something we must consider in a budget constrained environment. The MQ-1 Predator's role as a force multiplier usually goes unquestioned until one considers the footprint that accompanies the system. The U.S. Air Force fact sheet notes that the typical "fully operational system consists of four aircraft (with sensors), a ground control station, a Predator Primary Satellite Link, or PPSL, along with operations and maintenance crews for deployed 24-hour operations."

For those four aircraft, this involves 55 or more personnel. And while some personnel would be needed for logistics and maintenance of any system, roughly half of that 55-person footprint is made up of flight crew. As vehicle control becomes autonomous, so too must the analysis and maintenance.

While the full realization of autonomous systems may be decades away, we need to take steps toward developing technology in this direction today. First and foremost are the mathematical, software and processing developments allowing automated systems the necessary onboard intelligence to be autonomous. In the same way, with the likely wide dispersion of these platforms, and the need to work in concert with a host of other varied platforms, development toward secure interoperability standards for the autonomous systems is also a must.

The sum of human regulation has been based on managing the actions of people or the consequences of those actions. Ultimately a person is held accountable because it is generally understood that machines cannot be responsible for their actions. Some of these rules and regulations will require significant, if not total, overhaul to accommodate the productive coexistence of people and autonomous systems.

But if the world is to progress beyond remote control and overcome the spectrum constraints limiting unmanned vehicles, we must address these larger challenges. CHIPS

Mr. Tom Kidd is the director of Strategic Spectrum Policy for the Department of the Navy. For more information, contact Kidd at DONSpectrumTeam@navy.mil.

Mr. Mikel Ryan is the head of the Mid-Atlantic Area Frequency Management Office at Naval Air Station Patuxent River, Md.

Mr. Antonio Siordia is an analyst with the Space and Naval Warfare Systems Center Pacific.

Operation of 700 Megahertz Wireless Microphones Prohibited after June 12, 2010

Under a new Federal Communications Commission (FCC) rule, anyone who uses a wireless microphone (or similar device) that operates in the 700 MHz band will have to stop using it no later than June 12, 2010. Similar devices include wireless intercoms, in-ear monitors, audio instrument links and wireless cueing equipment.

When these microphones were first designed, they used frequencies that were located in between broadcast television channels. With the completion of the digital television transition, these frequencies are now used for public safety, such as police, fire and emergency services, and by commercial wireless services, such as wireless broadband services. Wireless microphones operating on these frequencies can cause harmful interference to these users.

The FCC is only prohibiting the use of wireless microphones (and similar devices) that operate between 698 and 806 MHz (the 700 MHz band). You may continue to use devices that operate on other frequencies. Also, this change only affects operations within the United States. Operators outside the United States may be allowed to use devices in the 700 MHz band with host nation and combatant commander approval.

Microphones and similar devices using electrical power cords are not affected by the FCC's decision. CHIPS

For more information, go to www.fcc.gov/cgb/wirelessmicrophones, or contact Mr. Tom Kidd, DON director for Strategic Spectrum Policy, at DONSpectrumTeam@navy.mil.

Department of the Navy: Current and Future

PUBLIC KEY INFRASTRUCTURE and PUBLIC KEY ENABLING ACTIVITIES

By James Mauck

The Secretary of Defense has embraced public key cryptography as a critical component of defense-in-depth and contributor to the overall Department of Defense (DoD) information assurance (IA) strategy for protecting its information and networks. DoD Instruction 8520.2, "Public Key Infrastructure (PKI) and Public Key Enabling (PKE)" establishes the requirements for PK-enabling all e-mail, private Web servers and networks.

This article outlines some of the Department of the Navy's current and future activities related to implementation of DoD and DON PKI policies — specifically in the areas of public key enablement of DON networks and personal electronic devices (PEDs); DON private Web servers and applications; and future PK-enablement of Secret Internet Protocol Router Network workstations using SIPRNET hardware tokens.

Public Key Enablement of DON Networks and E-mail

Today, approximately 85 percent of all DON enterprise network users authenticate their identity to their workstations using their Common Access Card (CAC) and its embedded PKI certificates through a process we call cryptographic logon or CLO. CLO provides two-factor strong authentication and provides a higher level of assurance than traditional passwords. Multiple network defense exercises have shown that passwords are a weak link because they are easy to share, not hard to gather through social engineering efforts, and are easy to break using advanced password cracking tools. CLO mitigates many of the risks associated with passwords because to masquerade as a user, a potential attacker must physically have control of a user's CAC and know his or her personal identification number (PIN).

The department is fielding solutions that will help reduce the number of "CLO exception" user categories like afloat users, system administrators, and Navy and Marine Corps reservists. Deployment of Real-Time Automated Personnel Identification System (RAPIDS) infrastructure to the shipboard environment will enable issuance, maintenance and replacement of damaged CACs for personnel while underway. Issuance of the "alternate token," which is a non-CAC smart card, is enabling cryptographic logon for higher privileged secondary accounts used for system administration. Also, previous technical limitations are being eliminated, which will enable all Navy and Marine Corps reservists to authenticate their identity via CLO to their reservist accounts using their reservist Common Access Card.

Use of digital signature and encryption capabilities are critical to the DON's efforts to protect sensitive information while in transit over e-mail. Digital signature capability reduces our adversaries' ability to gather information through the use of targeted malicious e-mail messages known as "spear phishing." By validating the digital signature associated with an e-mail message, DON users can read and review the message and any attachments with a higher level of confidence, knowing that the e-mail was sent by the author as indicated and that the message contents were not altered during transmission.

Through a series of PED policy messages beginning in August 2007, the DON CIO directed the migration to PED models that are PKI-compatible, like the BlackBerry. The combination of modernized PED handheld units, along with installation of smart card readers that communicate wirelessly with PEDs via an encrypted Bluetooth link, provide mobile workers with the capability to send signed and/or encrypted e-mail while on-the-go. This extends e-mail signature and encryption capabilities from the desktop environment to the edges of our enterprise networks, enabling the protection of sensitive information on mobile devices and helps prevent spear phishing attempts directed at mobile workers.

Public Key Enablement of DON Private Web Servers and Applications

In 2009, the DON CIO provided updated PKI and PK-enablement guidance via two naval messages. The September message defined at a high level, the department's PK-enablement waiver request process. The December message contained guidance on how to properly PK-enable DON private Web servers, portals and applications. The DON Deputy CIOs (Navy and Marine Corps) will be providing service-specific guidance on PK-enabling and PKE waiver request processes.

A DoD private Web server is defined as any DoD-owned, operated or controlled Web server that provides access to sensitive information that has not been reviewed and approved for public release. Properly PK-enabling private Web servers, portals and applications requires that user authentication be accomplished using properly validated PKI certificates instead of usernames and passwords.

In addition to certificates issued by the DoD or a DoD External Certificate Authority, recent DoD policy changes have expanded the categories of acceptable PKI certificates to include certificates issued by any DoD-approved external public key infrastructure operated by a non-DoD organization. Non-DoD organizations include U.S. federal agencies that issue Federal Information Processing Standards Publication (FIPS PUB 201-1) compliant personal identity verification (PIV) cards under direction of Homeland Security Presidential Directive 12 (HSPD 12), in addition to other DoD-approved state/local/tribal government organizations, and external DoD business partners approved by DoD.

PKI provides a mechanism for strongly authenticating identities on which authorization decisions may be made. Improper use of PKI as an access control mechanism may inadvertently allow unintended users to gain access to systems and information for which they are not authorized. In many cases Web

server, portal and application owners need to implement and configure access controls, as necessary, to enforce need-to-know requirements. Examples of access control mechanisms include access control lists, mapping of users' PKI certificates to their individual account, and dynamic authorization decisions based on user attributes.

SIPRNET PKI

In early fiscal year 2011, SIPRNET users will begin seeing familiar Non-classified Internet Protocol Router Network (NIPRNET) PKI capabilities employed on the SIPRNET to enhance security. These enhancements will include issuance of SIPRNET smart cards, implementation of a SIPRNET CLO, PK-enablement of SIPRNET Web servers, and signature and encryption of SIPRNET e-mail. Although there is currently a DoD SIPRNET PKI deployed and in operation, its use is limited and most commonly associated with authentication to Web servers and applications via SIPRNET software certificates or enforcement of communities of interest.

The foundation for the future SIPRNET PKI is already being laid, and key initiatives of the DoD-wide program are being led by recognized subject matter experts from within the DON and its services. The DoD is in the process of replicating the DoD authoritative identity repository, called Defense Enrollment Eligibility Reporting System (DEERS), from the NIPRNET to the SIPRNET. To ensure PKI interoperability across federal Secret level networks, the Committee on National Security Systems (CNSS) is standing up a PKI root under which all federal Secret level PKIs, including DoD's, will be subordinated. DoD's SIPRNET root and issuance certification authorities will then be deployed, enabling issuance of SIPRNET PKI certificates to Web servers, portals, applications, and the SIPRNET smart card that will be used for logon.

In spring 2010, representatives across the department will be participating in a DoD pilot that will validate SIPRNET smart card issuance processes and test SIPRNET cryptographic logon capabilities. After successfully completing the pilot under the current SIPRNET Public Key Infrastructure, SIPRNET token roll out will begin in increasingly larger phases under the newly deployed CNSS-subordinated DoD PKI.

PKI technology is key to the DON's defense-in-depth strategy and protection of DON sensitive information. It provides the foundation for robust authentication to enable accurate access control decisions made within DON networks, private Web servers and applications. Increased acceptance of PKI credentials issued by federal and non-DoD external business partners is enabling secure information sharing within the DON and DoD. Deployment of the DoD SIPRNET PKI, implementation of SIPRNET CLO, and PK-enablement of SIPRNET Web sites and applications will transform how we control access and share sensitive information in the classified environment in the future. CHIPS

James Mauck supports the DON CIO Cybersecurity and Critical Infrastructure Team. He is a subject matter expert on PKI and PKE.

References

Public Key Infrastructure

- DoD Instruction 8520.2 Public Key Infrastructure (PKI) and Public Key (PK) Enabling – http://www.dtic.mil/whs/directives/corres/html/852002.htm
- DoD CIO Memo for Approval of External Public Key Infrastructures – http://www.doncio.navy.mil/PolicyView.aspx?ID=1582
- DoD PKE – Working with External PKIs – http://iase.disa.mil/pki/pke/documents/slick_sheet1-pki_interoperability_final.doc
- Homeland Security Presidential Directive 12 – http://www.idmanagement.gov/documents/HSPD-12.htm
- Federal Information Processing Standards Publication (FIPS PUB 201-1) Personal Identity Verification (PIV) of Federal Employees and Contractors – http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf
- Authorization & Attribute Services Tiger Team – https://www.intelink.gov/sites/ictg/IdAM/AAS/AATT/default.aspx

DON CIO Guidance for Public Key-Enablement of PEDs

- DON Security Guidance for Personal Electronic Devices DTG 202041Z AUG 07 – http://www.doncio.navy.mil/PolicyView.aspx?ID=347
- DON Policy Updates for Personal Electronic Devices Security and Application of Email Signature and Encryption DTG 032009Z OCT 08 – http://www.doncio.navy.mil/PolicyView.aspx?ID=782
- Amplification Guidance for Purchase and Installation of Personal Electronic Device Smart Card Readers DTG 281919Z JAN 09 – http://www.doncio.navy.mil/PolicyView.aspx?ID=865
- Modification to Personal Electronic Device Smart Card Reader Compliance Mandate DTG 231919Z NOV 09 – http://www.doncio.navy.mil/PolicyView.aspx?ID=1458

DON CIO Guidance for Public Key-Enabling of Web Servers and Applications and PKE Waiver Request Process

- Public Key Enablement of DON Unclassified Private Web Servers and Applications DTG 291445Z DEC 09 – http://www.doncio.navy.mil/PolicyView.aspx?ID=1506
- DON NIPRNET Public Key Enablement Waiver Request Process DTG 262302Z SEP 09 – http://www.doncio.navy.mil/PolicyView.aspx?ID=1355

DON Enterprise Architecture v1.1.000 Released: Continues to Support Investment Decision Making

By Victor Ecarma

The Department of the Navy Chief Information Officer recently released the DON Enterprise Architecture v1.1.000. The DON EA v1.1.000 provides authoritative reference information, which can be used in developing solutions to support and fulfill DON mission and capability requirements. In addition, this update contains administrative changes associated with two DON EA laws, regulations, policies, and guidance (LRPGs). The administrative changes are as follows:

1. The wording of the two records management artifacts (Rules No. 4 and No. 5) has been updated to provide additional clarification about these requirements.
2. The two public key infrastructure/public key enablement (PKI/PKE) artifacts have been merged into a single new artifact (Rule No. 9).

In addition, as of the release of DON EA v1.1.000, the process for requesting a PKI/PKE waiver has been automated in the DON variant of the DoD Information Technology Portfolio Registry (DITPR-DON) as part of the DON EA compliance waiver process.

These administrative changes to the DON LRPGs have already been incorporated into the DON EA compliance assessment process. Compliance assessments for all other updates to the DON EA shall be implemented on Oct. 1, 2010, following the next formal release of the DON EA in July.

A listing of the content contained in the DON EA v1.1.000 is provided as an enclosure to the DON EA v1.1.000 release memo. The detailed content, as well as other current information about DON EA policy and procedures, can be viewed at https://www.intelink.gov/wiki/DONEA. CHIPS

Victor Ecarma provides support to DON CIO to advance enterprise architecture throughout the DON. The DON EA point of contact is the director of enterprise architecture & emerging technology, Mr. Michael Jacobs.

Updated DON DoDAF V2.0 Implementation Guidance Released

By Kimberly N. Brooks

The Department of the Navy Chief Information Officer (DON CIO) has released updated DON DoD Architecture Framework (DoDAF) v2.0 Implementation Guidance. This guidance clarifies what it means to be compliant at the current time with the requirements of DoDAF v2.0, within the DON.

The DON's DoDAF v2.0 implementation guidance clarifies the policy associated with using DoDAF v1.5 versus DoDAF v2.0 "views" and discusses the use of DoDAF v2.0 compliant commercial off-the-shelf (COTS) tools. It also provides direction on the use of "fit for purpose" views which are a new concept released as part of DoDAF v2.0.

A key element of compliance with DoDAF v2.0, which is discussed in the implementation guidance memo, is that all architectures developed within the DON should focus on the underlying data and information associated with the program or solution, as opposed to simply focusing on the graphical representation of the required architectural views. In addition, the memo discusses the requirement for this underlying architectural data to be compliant with the new DoDAF v2.0 Meta Model (DM2).

Style and format changes associated with DoDAF v2.0 views will be incorporated into the next release of the DON Architecture Product Guide (APG). The full guidance memo can be found at www.doncio.navy.mil. For Official Use Only (FOUO) information about current DON EA policy and procedures can be found at http://go.usa.gov/leF. CHIPS

Kimberly Brooks provides enterprise architecture support to the DON CIO. The DON EA point of contact is the director of enterprise architecture & emerging technology, Mr. Michael Jacobs.

CONGRATULATIONS TO DON AWARD WINNERS

DEPARTMENT OF THE NAVY FEDERAL 100 AWARD WINNERS

Ten information technology leaders from the Department of the Navy were among this year's Federal 100 Award winners. Federal Computer Week magazine presents the award to 100 professionals from government, industry and academia for their efforts in effecting change, progress and efficiency in determining how the federal government acquires, develops and manages IT.

The winners' accomplishments were recognized in the March 22 issue of Federal Computer Week magazine, and the awards were presented at a black-tie gala held on March 22 at the Grand Hyatt Hotel in Washington, D.C.

The 2010 DON Federal 100 Award winners are:

- CAPT Danelle Barrett, Carrier Strike Group Two, Assistant Chief of Staff for Command and Control, Communications, Computers and Combat Systems;
- Peter Gillis, Community Manager, Marine Corps IT Management Community of Interest;
- RADM John Goodwin, Assistant Chief of Naval Operations, Next Generation Enterprise Network;
- David Green, Chief Technology Advisor, Headquarters Marine Corps Command, Control, Communications and Computers;
- Mr. Terry Halvorsen, Deputy Commander, Naval Network Warfare Command and Deputy Assistant Chief of Staff, U.S. Fleet Forces N6 and Command Information Officer;
- Jeff Huskey, Command Information Officer, Commander, Navy Installations Command;
- Tom Kidd, Director, Strategic Spectrum Plans & Policy, Office of the DON CIO;
- Jim Knox, Director, Information Sharing, Knowledge and Records Management, Office of the DON CIO;
- Ronald Simmons, Director, Knowledge Management, Marine Corps Combat Development Command; and
- Sonya Smith, Director, Cybersecurity and Critical Infrastructure, Office of the DON CIO.

DON IM/IT EXCELLENCE AWARD WINNERS

Three individuals and five project teams were honored at the Department of the Navy Information Technology Conference in San Diego for their outstanding contributions toward transforming the Navy and Marine Corps through information technology. The following teams and individuals were recognized during an awards ceremony, Feb. 2, 2010, by Rob Carey, DON Chief Information Officer; Jim Craft, Deputy Director, C4, Headquarters Marine Corps; and Joyce Dawkins, Head, Information Architecture Branch, Assurance and Compliance Directorate, DCNO for Information Dominance (N2/N6).

TEAM AWARDS

Cyber Asset Reduction and Security Task Force

Over the past year, the Cyber Asset Reduction and Security (CARS) Task Force has delivered a common, well-defended infrastructure, implemented several enterprise security solutions, and provided unprecedented visibility into IT inventories, expenditures and operational capabilities across the Navy. By rapidly migrating legacy infrastructure to enterprise networks, instituting a rigorous excepted network approval process, and enforcing Navy-wide enterprise consolidation, excess capacity was eliminated, security posture was improved, and the Navy is better positioned to attain the vision of the Naval Networking Environment. Through their efforts, the CARS team heightened the Navy's enterprise IT perspective, dramatically improved network security posture, and made a lasting impact on Navy cyber readiness.

Team Members

Mr. Neal Miller
Mr. Brian Koman
Mr. Byron Parker
CAPT Sam Sumwalt
CWO2 Alan Bollinger
PS1 Dawn Demacos
Mr. Charles Kiriakou
LCDR Travis Rauch
Mr. Gibby Sorrell
Mr. Mukesh Barot
Ms. Janet Smith
Mr. Matthew Swartz
Mr. Clifford Bussey
Mr. Allen Blackburn
Ms. Mary Lou Hoffert
CWO4 Michael Clark
Mr. Huey Dennis

Commander, Navy Installations Command Security Assessment Team

The Commander, Navy Installations Command Security Assessment Team (CNIC SAT) was instrumental in developing and implementing an innovative approach to information assurance compliance. The CNIC SAT has been able to work with our IA workforce and management to reduce potential security vulnerabilities, develop lessons learned and best practices, and achieve external compliance verification for CNIC networks, servers and systems. Their innovative approach, technical knowledge, and commitment to excellence have changed the way we ensure a high standard of, and continually improve, information security across the Navy.

Team Members

Ms. Carol Lee
Mr. Steven Farmer
Ms. Terry Merz
Mr. Timothy Rogers
Mr. Robert Diestel
Ms. Denise Madison
Mr. Brett Osborne
Mr. Andrew Erne
Ms. Gail McGilvary
Mr. Raymond Reese

OPNAV CIO Team

The OPNAV CIO Team conducted operations, maintenance, and technical upgrades for the entire OPNAV staff consisting of more than 3,000 personnel. As a result, significant cost savings were achieved for both information technology and information management. Their diligence in the area of information assurance has ensured 100 percent compliance with Federal Information Security Management Act mandates. The team has conducted several high visibility projects within OPNAV, such as PKI implementation, which requires 100 percent Common Access Card authentication from all network users; blade server stand up, which replaces obsolete hardware on the SIPRNET; and the E-form Paperless Initiative, which leverages Adobe products to employ digital signatures.

Team Members

CDR Randy Darrow
Ms. Wanda Joynes
Mr. Jonathan Gerard
Mr. Julius Pfeifle
CWO2 Jacqueline Clifton
LCDR Albert Seeman
Mr. Kenneth Robertson
Mr. Ryan Johnson
Mr. Robert Przydzial
ET1 Joshua Hansell
Mr. Mark Bowers
Ms. Denise Morales
Mr. Kevin Young

Naval Supply Systems Command Network/Server Consolidation Team

The Naval Supply Systems Command (NAVSUP) Network/Server Consolidation Team has achieved significant results in streamlining and reducing the Navy's legacy network and server infrastructure. Their actions resulted in a 90 percent reduction in NAVSUP's legacy network footprint (from 30 to 2 networks) and a 70 percent reduction in the legacy server footprint (from 716 to 218 servers).

Team Members

Mr. Tom Heasley
Ms. Laurie Shugrue
Ms. Lynn Briggs
Mr. Bob Park
Ms. Lila Tonsic
Mr. Mark Estes
Mr. Dan Aparis
CDR Tom Graebner
Mr. Brian Pontius
Ms. Tennille Good
Ms. Linda Gardner
Mr. Frank Swallow
Mr. Brian Zirbel
Mr. Gary Steele
Ms. Vicki Hardy
Mr. Shannon Rothermel
Ms. Amanda Johnson
Ms. Pam Wenner

Tactical Training Group, Pacific Network-Centric Warfare Syndicate

The Tactical Training Group, Pacific Network-Centric Warfare (NCW) Syndicate made significant improvements to the Navy IM/IT workforce by training more than 600 personnel on knowledge and information management. Additionally, their development of the Post Deployment Interview Process has directly improved the readiness of deploying strike groups by allowing the quick collection and turnaround of lessons learned. The NCW team also conducted in-depth mentoring and evaluation of five strike groups in 2009, directly enhancing the warfighting readiness of Pacific Fleet Strike Groups.

Team Members

LTJG Jeffrey White
Ms. Jill Robertson
Mr. Chris Simpson
Mr. Dennis Schulz
Mr. Tim Snyder

INDIVIDUAL AWARDS

Mr. Len Blasiol

Director of MAGTF Integration
Combat Development Directorate
Marine Corps Combat Development Command

Mr. Len Blasiol is recognized for his strategic visionary leadership in the transformation of operational processes by leveraging technology to optimize more efficient knowledge transfer in support of U.S. Marine Corps mission goals. He has demonstrated a willingness to evaluate shifting technological advancements; learn their capabilities and limitations; and translate those advances that show potential into innovative paradigm shifts such as agile commands and decentralized intelligence. His efforts have demonstrated significant improvements to the efficiency and effectiveness of his organization to accomplish its mission. These efforts have also improved the strategic use of knowledge in support of decision making and accelerated mission task accomplishments. Mr. Blasiol continues to provide critical visionary leadership to the U.S. Marine Corps.

Ms. Theresa Reed

Navy Enterprise Resource Planning Implementation

While serving as Data Management Lead for Naval Supply Systems Command's (NAVSUP) Enterprise Resource Planning (ERP) Single Supply Solution implementation, Theresa Reed ensured the successful migration of NAVSUP's legacy master data and transaction data from the old, disparate systems into the new Navy ERP solution. Ms. Reed led one of the major critical areas for any successful ERP implementation — data management. Her team has loaded more than 85 million data elements with an accuracy exceeding 98 percent — a truly impressive statistic. Navy ERP is a transformational event and Theresa Reed's dedication and hard work are critical to its success.

Mr. Paul Skopowski

Deputy Plans Officer, Marine Corps
Network Operations and Security Center

Mr. Skopowski is responsible for the planning, synchronization and effective delivery of new and improved capabilities that satisfy enterprise level operational and technical requirements directly impacting the Marine Corps Network Operations and Security Center's (MCNOSC) mission. He demonstrated superior leadership, managerial skills, technical acumen and forward-thinking ingenuity by guiding multiple working groups chartered to project future Marine Corps Enterprise Network needs at the command, service, Department of the Navy and Global Information Grid levels.

JOHN J. LUSSIER AWARD for ELECTROMAGNETIC SPECTRUM LEADERSHIP

The John J. Lussier Electromagnetic Spectrum Leadership Award is named for the DON Principal Deputy Chief Information Officer who lost his courageous battle with cancer in June 2009. Mr. Lussier was an advocate for protecting the DON's equities in the electromagnetic spectrum and advanced the DON's strategic vision for spectrum. This award is presented to an individual who demonstrates superior leadership and achievement in Navy and Marine Corps electromagnetic spectrum management and use.

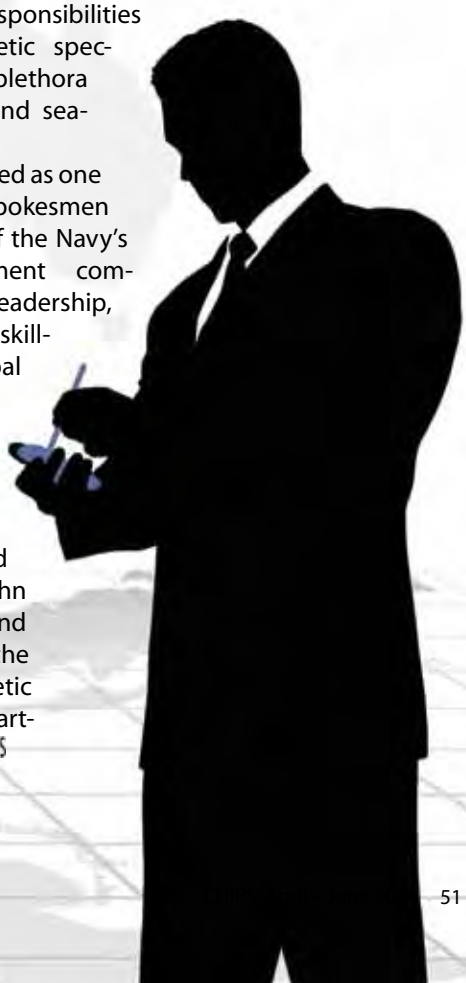
Recipient for 2010: Mr. Mikel R. Ryan

Head, Mid-Atlantic Area Frequency Management Office
Naval Air Station Patuxent River

As the Vice Chair of the International Consortium for Telemetry Spectrum, Mr. Mikel Ryan was instrumental in the development and support of a complex initiative that resulted in the global reallocation of a frequency band to support harmonized flight test telemetering. The reallocation provides an additional frequency band for critical aircraft testing and includes unmanned air vehicle (UAV) testing and monitoring.

Mr. Ryan also spearheads the efforts of the Mid-Atlantic Area Frequency Management Office at Naval Air Station Patuxent River where his responsibilities include electromagnetic spectrum support for a plethora of aviation, ground and seaborne testing.

Mr. Ryan is recognized as one of the preeminent spokesmen for the Department of the Navy's frequency management community. Mr. Ryan's leadership, determination, and skillful support of a global spectrum reallocation initiative will significantly benefit naval telemetry capabilities for decades to come, and is in keeping with John Lussier's leadership and strategic vision for the use of electromagnetic spectrum in the Department of the Navy. CHIPS



Web Portals and Shared Drives Must Be Continually Monitored

The following is a recently reported data breach involving the disclosure of personally identifiable information (PII) on the Navy Knowledge Online (NKO) Web site. Incidents such as this will be reported in each CHIPS magazine to increase PII awareness. Names have been changed or omitted but details are factual and based on reports sent to the Department of the Navy Chief Information Officer Privacy Office.

Background

When used properly, Web portals and shared network drives do a great job of facilitating information sharing and collaboration. They are indispensable to commands that are forward deployed, and for drilling Reservists and other communities that rely on virtual access to information. However, PII breach incidents have been reported with increasing frequency in this area and must be given command attention to ensure strict access controls are in place.

The Incident

In December 2009, a DON command received a heads up that PII data had been discovered in a file on the NKO Web site without security controls. The data was displayed on two spreadsheets containing names, addresses and other PII. While the site requires users to log on or use a CAC card to access the site, it should have also required the user to have file access permission. In the past, NKO was used extensively by the command as a staging area where mobilization information was posted so that Navy entities could access this information to use in the mobilization process.

More recently, and due to heightened PII awareness from annual refresher training, the command removed this type of information from the site, and it was used for general information purposes only. It appeared that the two spreadsheets inadvertently remained on NKO since their original posting in September 2008. Both spreadsheets were removed from the NKO Web site immediately after discovery.

Lessons Learned

The most valuable lesson learned from this incident was the importance of placing controls on documents that contain PII, even when those documents are protected behind CAC-enabled Web sites. Similar to dealing with classified information, one must analyze who should have access to PII. ONLY THOSE WITH A NEED TO KNOW should have access to PII.

Positive controls (e.g., password, encryption, etc.) must be placed on documents containing PII to ensure that only approved personnel have access. Lastly, spot checks must be performed on a routine basis to ensure that controls that were put in place still remain.

Of special note, numerous incidents regarding lack of access controls have been reported after network maintenance has been performed. Software tools are commercially available to run periodic checks on shared drives and portals that key in on PII elements such as a Social Security number.

Aggressive use of the DON PII compliance spot checklist also has been a useful tool. Go to the DON CIO Web site at www.doncio.navy.mil for specific policy guidance on this subject. CHIPS

Additional privacy information can be found on the DON CIO Web site at www.doncio.navy.mil. Steve Muck is the DON CIO privacy team lead.

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 Web site at http://www.esi.mil/.

Software Categories for ESI:

Asset Discovery Tools

Belarc

BelManage Asset Management Provides software, maintenance and services.

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

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

Ordering Expires: 30 Sep 11

Web Link: https://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: 18 May 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

Patriot

BigFix Asset Management – Provides software, maintenance and services.

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

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

Ordering Expires: 08 Sep 12

Web Link: https://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.

Contractor: *Computer Associates International, Inc.* (W91QUZ-04-A-0002); (813) 612-7352

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 57.

Oracle (DEAL-O)

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

Contractors:

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

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

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

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

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

Ordering Expires:
Oracle: 30 Sep 11
DLT: 1 Apr 13
immixTechnology: 26 Aug 11
Mythics: 18 Dec 11
TKCIS: 29 Jun 11

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

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

Special Note to Navy Users: See the information provided on page 58 concerning the Navy Oracle Database Enterprise License under Department of the Navy Agreements.

Sybase (DEAL-S)

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

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

Ordering Expires: 15 Jan 13

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

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

Enterprise Application Integration

Sun Software

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

Contractors:

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

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

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

Ordering Expires: 24 Sep 12

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

Enterprise Architecture Tools

IBM Software Products

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

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

Ordering Expires: 2 Jul 10 (Please call for extension information.)

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

Citrix

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

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

Ordering Expires: 25 May 10 (Please call for extension information.)

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

Ordering Expires: 01 Jun 14

Web Link: http://www.it-umbrella.navy.mil/contract/planet_assoc/planetassoc.shtml

Quest Products

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

Contractors:

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

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

Ordering Expires:

Quest: 30 Sep 10

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 54.*

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.it-umbrella.navy.mil/contract/enterprise/erp_software/rwd/rwd.shtml

SAP

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

Contractors:

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

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

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

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

Ordering Expires: 14 Sep 13

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

Information Assurance Tools

Data at Rest Solutions BPAs offered through ESI/SmartBUY

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

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

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

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

The DON CIO issued an enterprise solution for Navy users purchasing DAR software. See the information provided on page 58 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 Web site at https://chess.army.mil/ascp/commerce/contract/FA8771-07-A-0301_bpaorderinginstructions(2)_ARMY.jsp.

As of press time, other DoD users are not authorized to purchase DAR software because service-specific guidance has not been issued.

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

Safeboot/McAfee ***Rocky Mountain Ram*** (FA8771-07-A-0302)

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

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

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

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

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

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

CREDANT Technologies ***GTSI Corp.*** (FA8771-07-A-0309)
WinMagic, Inc. ***Govbuys, Inc.*** (FA8771-07-A-0310)
CREDANT Technologies ***Intelligent Decisions*** (FA8771-07-A-0311)
GuardianEdge Technologies ***Merlin International*** (FA8771-07-A-0312)
Ordering Expires: 14 Jun 12 (If extended by option exercise.)
Web Link: http://www.esi.mil

McAfee

McAfee Provides software and services in the following areas: Anti-Virus; E-Business Server; ePolicy Orchestrator; GroupShield Services; IntruShield; Secure Messaging Gateway and Web Gateway.
Contractor: ***En Pointe*** (GS-35F-0372N)
Ordering Expires: 16 Sep 10 (Please call for extension information.)
Web Link: http://www.esi.mil
Antivirus Web Links: Antivirus software available at no cost; download includes McAfee, Symantec and Trend Micro Products. These products can be downloaded by linking to either of the following Web sites:
NIPRNET site: https://www.jtfgno.mil/antivirus/antivirus_index.htm
SIPRNET site: https://www.cert.smil.mil/antivirus/av_info.htm

Securify

Securify Provides policy-driven appliances for network security that are designed to validate and enforce intended use of networks and applications; protects against all risks and saves costs on network and security operations. Securify integrates application layer seven traffic analysis with signatures and vulnerability scanning in order to discover network behavior. It provides highly accurate, real-time threat mitigation for both known and unknown threats and offers true compliance tracking.
Contractor: ***Patriot Technologies, Inc.*** (FA8771-06-A-0303)
Ordering Expires: 04 Jan 11 (If extended by option exercise)
Web Link: http://www.esi.mil

Symantec

Symantec Symantec products can be divided into 10 main categories that fall under the broad definition of Information Assurance. These categories are: virus protection; anti-spam; content filtering; anti-spyware solutions; intrusion protection; firewalls/VPN; integrated security; security management; vulnerability management; and policy compliance. This BPA provides the full line of Symantec Corp. products and services consisting of 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*** (FA8771-05-0301)
Ordering Expires: 12 Sep 10
Web Link: http://var.immixgroup.com/contracts/overview.cfm or www.esi.mil
Notice to DoD customers regarding Symantec Antivirus Products: A fully funded and centrally purchased DoD enterprise-wide antivirus and spyware software license is available for download to all Department of Defense (DoD) users who have a .mil Internet Protocol (IP) address.

Contractor: ***TVAR Solutions, Inc.***
Antivirus Web Links: Antivirus software can be downloaded at no cost by linking to either of the following Web sites:
NIPRNET site: https://www.jtfgno.mil/antivirus/antivirus_index.htm
SIPRNET site: http://www.cert.smil.mil/antivirus/av_info.htm

Websense (WFT)

Websense Provides software and maintenance for Web filtering products.
Contractor: ***Patriot Technologies*** (W91QUZ-06-A-0005)
Authorized Users: This BPA is open for ordering by all DoD components and authorized contractors.
Ordering Expires: 31 Aug 11
Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

Xacta

Xacta Provides Web Certification and Accreditation (C&A) software products, consulting support and enterprise messaging management solutions through its Automated Message Handling System (AMHS) product. The software simplifies C&A and reduces its costs by guiding users through a step-by-step process to determine risk posture and assess system and network configuration compliance with applicable regulations, standards and industry best practices, in accordance with the DITSCAP, NIACAP, NIST or DCID processes. Xacta s AMHS provides automated, Web-based distribution and management of messaging across your enterprise.
Contractor: ***Telos Corp.*** (FA8771-09-A-0301); (703) 724-4555
Ordering Expires: 24 Sep 14
Web Link: http://esi.telos.com/contract/overview

Lean Six Sigma Tools
iGrafx Business Process Analysis Tools

iGrafx Provides software licenses, maintenance and media for iGrafx Process for Six Sigma 2007; iGrafx Flowcharter 2007; Enterprise Central; and Enterprise Modeler.
Contractors:
Softchoice Corporation (N00104-09-A-ZF34); (416) 588-9002 ext. 2072
Softmart, Inc. (N00104-09-A-ZF33); (610) 518-4192
SHI (N00104-09-A-ZF35); (732) 564-8333
Authorized Users: These BPAs are co-branded ESI/GSA SmartBUY BPAs and are open for ordering by all Department of Defense (DoD) components, U.S. Coast Guard, NATO, Intelligence Community, authorized DoD contractors and all federal agencies.
Ordering Expires: 31 Jan 14
Web Links:
Softchoice
www.it umbrella.navy.mil/contract/enterprise/igrafx/softchoice/index.shtml
Softmart
www.it-umbrella.navy.mil/contract/enterprise/igrafx/softmart/index.shtml
SHI
www.it-umbrella.navy.mil/contract/enterprise/igrafx/shi/index.shtml

Minitab

Minitab Provides software licenses, media, training, technical services and maintenance for products including Minitab Statistical Software, Quality Companion and Quality Trainer. It is the responsibility of the ordering officer to ensure compliance with all fiscal laws prior to issuing an order under a BPA, and to ensure that the vendor selected represents the best value for the requirement being ordered (see FAR 8.404).
Contractor: ***Minitab, Inc.*** (N00104-08-A-ZF30); (800) 448-3555 ext. 311
Authorized Users: This BPA is open for ordering by all Department of Defense (DoD) components, U.S. Coast Guard, NATO, Intelligence Community and authorized DoD contractors.
Ordering Expires: 07 May 13
Web Link: http://www.it-umbrella.navy.mil/contract/minitab/minitab.shtml

PowerSteering

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

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

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

Ordering Expires: 14 Aug 13

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

Office Systems

Adobe Desktop Products

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

Contractors:

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

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

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

Insight Public Sector, Inc. (N00104-08-A-ZF36); (301) 261-6970

Ordering Expires: 30 Jun 13

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

Adobe Server Products

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

Contractor:

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

Ordering Expires: 14 Jan 14

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/adobe-srvr/carahsoft/carahsoft.shtml

Microsoft Products

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

Contractors:

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

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

Dell Marketing L.P. *(formerly ASAP)* (N00104-02-A-ZE78); (800) 248-2727, ext. 5303

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); Large Business; (877) 333-7638

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

Ordering Expires: 31 Mar 10 (The follow-on agreements are in process for an April 1 start date. The ESI and DON IT Umbrella Program Web sites will have the current information.)

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

Red Hat/Netscape/Firefox

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

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

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

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

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

Sun (SSTEW)

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

Contractor: ***Dynamic Systems*** (DCA200-02-A-5011)
Ordering Expires: Dependent on GSA schedule until 2011
Web Link: http://www.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 Web sites and analyst support for the number of users registered. In addition, the services provide independent advice on tactical and strategic IT decisions. Advisory services provide expert advice on a broad range of technical topics and specifically focus on industry and market trends. BPA listed below.

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

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 DON Information Technology (IT) Umbrella Program Office. The Navy Oracle Database Enterprise License provides significant benefits, including substantial cost avoidance for the department. It facilitates the goal of netcentric operations by allowing authorized users to access Oracle databases for Navy internal operations and permits sharing of authoritative data across the Navy enterprise.

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

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

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

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

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

Navy Enterprise BPA for DAR Users:
Mobile Armor ***MTM Technologies, Inc.*** (N00104-09-A-ZF30)
Web Link: http://www.it-umbrella.navy.mil/contract/mtm/mtm.shtml

Visit our Web sites:

www.it-umbrella.navy.mil

www.itec-direct.navy.mil

www.esi.mil

www.chips.navy.mil

Page Intentionally left blank

the Pulse

Join the conversation.

https://www.doncio.navy.mil/pulse

A collaborative site for members of the DON IM/IT community.

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

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