SHARING INFORMATION TECHNOLOGY EXPERIENCE

CHIPS

October - December 2011

Creating IT efficiencies without sacrificing operational effectiveness will be a tough challenge, but we cannot afford to fail.

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

CHIPS October – December 2011 | Vol. XXIX Issue IV

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

Department of the Navy
Deputy Chief Information Officer (Navy)
Vice Adm. Kendall L. Card

Department of the Navy
Deputy Chief Information Officer (Marine Corps)
Brig. Gen. Kevin J. Nally

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

Space & Naval Warfare Systems Center Atlantic
Commanding Officer Capt. Mark V. Glover

Space & Naval Warfare Systems Center Pacific
Commanding Officer Capt. Joseph J. Beel

Senior Editor/Layout and Design
Sharon Anderson

Webmaster
Department of the Navy Chief Information Officer

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

---

Contributors
Lynda Pierce, DON Enterprise IT Communications
Michele Buisch, DON Enterprise IT Communications

CHIPS is sponsored by the Department of the Navy Chief Information Officer (DON CIO), the DoD Enterprise Software Initiative and the DON's ESI software product manager team at SPAWARSYSCEN Pacific. CHIPS (USPS 757-910) is published quarterly by SPAWARSYSCEN Atlantic, 1837 Morris St., Suite 3311, Norfolk, VA 23511. Periodical postage paid at Norfolk, VA and additional entry offices. POSTMASTER: Send changes of address to CHIPS, SSC Atlantic, 1837 Morris St., Suite 3311, Norfolk, VA 23511-3432.

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, 1837 Morris St., Suite 3311, Norfolk, VA 23511-3432, or call (757) 443-1775; DSN 646. Email: chips@navy.mil; Web: www.doncio.navy.mil/chips.

Disclaimer: The views and opinions contained in CHIPS are not necessarily the official views of the Department of Defense or the Department of the Navy. These views do not constitute endorsement or approval by the DON CIO, Enterprise Software Initiative or SPAWAR Systems Centers Atlantic and Pacific. 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.

ISSN 1047-9988

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

Cover

Network and cyber leaders across the departments of the Navy and Defense discuss the urgency to standardize and consolidate networks and data centers, reduce information technology costs and secure the IT enterprise — without sacrificing mission effectiveness.

Interviews

"Well, first off, if you're ever going to be in government, I think this is the time to be in government. Whenever you have big changes afoot — like in 1993, when we did the first post-Cold War bottom-up review, or now when we are facing a major reallocation of our nation's resources — it's cool to be part of a process that will have big ramifications for a long time. It's a time when good ideas matter, and good people are the source of good ideas."

– Under Secretary of the Navy Robert O. Work

Navigation

In Every Issue

Highlights

Please update your bookmark, the CHIPS website address has changed to www.doncio.navy.mil/chips.

From the DON CIO

From Around the Fleet and Program Offices

Editor's Notebook

Signs of the severity of the economic crisis are all around us — we are reminded daily in the news, by our leadership and in our workplace, at the gas pumps and in the grocery store, but the news isn't all bad because challenges often come with opportunities to make changes that can make a difference. I am especially inspired by Under Secretary of the Navy Robert O. Work's comment that we are in "a time when good ideas matter, and good people are the source of good ideas."

I had the honor and pleasure of interviewing Mr. Work in September. You will find his discussion about the budget process, restructuring the naval force and finding efficiencies in department business information technology motivating.

Thought provoking discussion and decisive action are ongoing across the departments of the Navy and Defense. In August I attended the Army's LandWarNet conference where the Army's network and cyber leaders and DoD CIO Teri Takai explained efforts to reduce IT costs and build an enterprise infrastructure that will enable information sharing across the globe, linking warfighters and joint and coalition partners — securely.

At LandWarNet, Adm. Bill McRaven, commander of U.S. Special Operations Command, defined the unique communications requirements of Special Forces. Really, they have many of the same basic needs that we all do: fast, reliable, cost-effective, secure mobile communications.

Joining the discussion in this issue are Commander, Navy Cyber Forces Rear Adm. Gretchen Herbert and Commander, Space and Naval Warfare Systems Command Rear Adm. Patrick Brady who outline their roles and responsibilities and share their strategies for mission success.

Arctic affairs officer from Task Force Climate Change, Cmdr. Blake McBride, explains the Navy's Arctic environmental assessment and steps the Navy is taking to operate in the warming waters of the Arctic.

Oct. 7, the Department of the Navy Chief Information Officer Terry Halvorsen and David Weddel, Assistant Deputy Chief of Naval Operations for Information Dominance, were keynote speakers when SPAWAR Systems Center Atlantic unveiled a new data center that will play a key role in consolidating more than 100 Navy data centers to increase effectiveness and efficiency and reduce costs while still meeting the Navy's security and operational requirements.

The DON CIO explained how the center fits into the Navy's future plans.

"This data center will be part of the Navy's data center consolidation effort. Not only is this data center efficient, it's green — that is another big piece of what we want to do. We need to protect the environment and the resources that we have. This data center will help us do that," Halvorsen said.

As you know the DON CIO is the department lead for IM/IT/cyberspace efficiency and effectiveness.

Welcome new subscribers!

Sharon Anderson

Department of the Navy Data Center Consolidation

CHARLESTON, S.C. (Oct. 7, 2011) Space and Naval Warfare Systems Center Atlantic cuts the ribbon on a new data center in Charleston, S.C., with Mr. Gary Armstrong, vice president, Suffolk Construction; Lt. Cmdr. Steve Fichter of NAVFAC SE ROICC; Commanding Officer SPAWARSYSCEN Atlantic Capt. Mark V. Glover; DON CIO Mr. Terry Halvorsen; Deputy Commander SPAWAR Mr. Rod Smith; Assistant Deputy Chief of Naval Operations for Information Dominance Mr. David Weddel; Executive Director SPAWARSYSCEN Atlantic Mr. Christopher Miller; and Ms. Pennie Bingham from the Charleston Metro Chamber of Commerce.

CHARLESTON, S.C. (Oct. 7, 2011) Distinguished visitors attending the data center ribbon cutting ceremony at SPAWARSYSCEN Atlantic hear about data center capabilities from Lt. Cmdr. John Lukacs joined by Capt. Mark Glover, Mr. David Weddel, Mr. Terry Halvorsen and Mr. Bruce Carter.

Construction began on the 20,220 square-foot facility on Joint Base Charleston-Weapons Station Oct. 15, 2010 and was recently completed. The $9.498 million data center was designed to the U.S. Green Building Council's Leadership in Environmental and Energy Design silver rating standard.

The Navy's data center consolidation initiative will provide cost savings due to reductions in physical locations, power and data center management contracts.

A MESSAGE FROM THE

DON CIO

Finding IT Efficiencies:
Challenging but Necessary Work

It has been a busy year for the Department of the Navy Chief Information Officer staff and the information technology efficiencies integrated product teams (IPT) as we analyze how the DON can improve the way business IT is purchased, managed and operated. This hard work will enhance the department's effectiveness, as well as result in real savings, as we grapple with shrinking budgets. As a result of these efforts, several processes have been updated to improve the way the department manages business IT by providing better visibility into what is being spent, optimizing resources and acting in a centralized manner as one enterprise to improve our ability to negotiate the most favorable contracting terms. Those new processes are detailed in the following memos.

"Department of the Navy Information Enterprise Governance Board (IGB) Charter" established the IGB to serve as the department's single, senior information management (IM), information technology, cybersecurity and information resources management (IRM) policy and governance forum. The IGB reviews and approves DON IM/IT/cyberspace and IRM enterprise initiatives.

"Required Use of Department of the Navy Enterprise Information Technology Standard Business Case Analysis (BCA) Template" mandates the use of a BCA template for all DON IT investments of $1 million or more. Its use ensures consistency, facilitates comparisons of proposed alternatives to the status quo, and clearly defines expected costs, benefits, effects on operations and risks, thereby ensuring the best course of action is taken.

"Department of the Navy Information Technology Expenditure Approval Authorities (ITEAA)" requires approval by the designated ITEAA of any IT software, hardware or service with a projected life cycle cost or purchase price totaling $1 million or more. The ITEAAs will ensure that IT projects are aligned with DON IT goals and conform to the DON and Department of Defense (DoD) enterprise architectures. The three ITEAAs for the Navy, Marine Corps and secretariat are: Deputy Chief of Naval Operations for Information Dominance/DON Deputy CIO (Navy) OPNAV N2/N6; Headquarters Marine Corps Director for Command, Control, Communications and Computers (HQMC C4)/DON Deputy CIO (Marine Corps); and the DON CIO for the secretariat. All three ITEAAs have set approval thresholds that are lower than required by the memo.

"Department of the Navy Data Center Consolidation Policy Guidance" established a moratorium on DON investment in increased data storage capacity without first determining that existing capacity is insufficient to meet needs. The policy states that DON organizations must use existing Navy Marine Corps Intranet (NMCI), Space and Naval Warfare Systems Command (SPAWAR) and Marine Corps data centers. They may also explore the use of Defense Department and commercial data centers that meet or exceed required standards and show proven savings.

More recently, the memo, "Efficiency and Effectiveness Review of DON Information Technology Systems" issued by the Under Secretary of the Navy, tasked the DON CIO to analyze and assess the DON's IT/National Security System investments for efficiency and effectiveness. All these memos, which you can find on the DON CIO website at www.doncio.navy.mil, were published to ensure better control of the money spent on business IT investments and to gain efficiencies. By operating in a more centralized manner, the department will be able to optimize its resources and reduce redundancies. In fact, the IPTs are exploring other areas in which the department should act in a more centralized manner. These areas include: enterprise licensing for software, hardware and services; telecommunications; workforce training; and the Navy Marine Corps portal environment.

As we work through this process of finding and analyzing potential efficiencies in the DON, we must also consider and explore what efficiencies may be gained by consolidating IT resources or investments at the DoD level. It is important to be prepared to have the conversation and do the analysis to determine which joint solutions make sense for the DON to adopt. This may include cloud services offered by the Defense Information Systems Agency (DISA). While DISA's enterprise solution may not always be the right solution for the DON, we will conduct a business case analysis to make that decision.

The federal government is also making changes in the way IT is managed. The Office of Management and Budget released the memo "Chief Information Officer Authorities" in August 2011 to strengthen and clarify the role of agency CIOs from policymaking to true IT portfolio management. These authorities enable federal CIOs to ensure IT solutions support the organizational mission and align with organizational goals. This change will also help CIOs overcome bureaucratic obstacles to deliver enterprise-wide solutions. Additionally, the "25 Point Implementation Plan to Reform Federal Information Technology Management" published December 2010 named the CIO as the lead in four main areas: governance, commodity IT, program management and information security.

Although it's challenging to reform how our business IT is managed, we cannot afford to fail. Simply put, cuts to business IT will prevent cuts to operational IT.

Terry Halvorsen

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

INTERVIEW WITH THE UNDER SECRETARY OF THE NAVY *ROBERT O. WORK*

Transforming the Naval Enterprise to Support the Warfighter

Robert O. Work was confirmed as the Under Secretary of the Navy May 19, 2009. In this capacity, Work serves as the deputy and principal assistant to the secretary of the Navy and acts with full authority of the secretary in the day-to-day management of the Department of the Navy.

In response to the national economic crisis and the president's directives for a drawdown in the Defense Department budget due to a gradual withdrawal of U.S. military forces in Afghanistan beginning later this year, the DoD and the military departments reduced overhead costs, eliminated duplicative force structures and underperforming acquisition programs, and streamlined processes.

Mr. Work is leading strategic reviews and efficiency efforts across the department in areas of force structure, warfighting capabilities, shipbuilding and acquisition. In December 2010, the Under Secretary issued a memorandum, "Department of the Navy (DON) Information Technology (IT)/Cyberspace Efficiency Initiatives and Realignment," directing the DON Chief Information Officer, Mr. Terry Halvorsen, to find efficiencies and cost savings in how the department delivers IT/cyberspace capabilities and information resources management.

At Naval IT Day in June, in Northern Virginia, Mr. Work discussed how the most recent defense buildup is different than any other U.S. military surge, and why the subsequent restructuring of the naval force and its warfighting capabilities will be challenging. CHIPS asked Mr. Work to discuss his analysis and IT efficiencies Sept. 1, 2011.

CHIPS: Some have said that reductions in the defense budget could reach $1 trillion. Is the DON working on worst case scenarios so the department can still maintain a force and achieve cost savings and efficiencies?

Mr. Robert O. Work
Under Secretary of the Navy
r

Under Secretary Work: Well, a trillion dollars would be the absolute worst case, and not something we are worried about — yet. Let me explain. We've benefited from a long buildup in defense spending that started back in FY (fiscal year) 99. The buildup first started because there was a consensus that the bottom-up review strategy — which called for a force capable of fighting two regional wars — was being underfunded. The buildup then accelerated and expanded as we fought wars in Iraq and Afghanistan. So we've seen over 10 years of steadily increasing defense spending.

OCO (overseas contingency operations) funding began to go down after FY10, as we started to pull out of Iraq. At that point, Secretary Gates said we needed to prepare for a future in which our base defense top line would also stop growing, and maybe even decline. We all recognized we needed to start tightening our belts. This thinking led to the big effort to find departmentwide efficiencies in our FY12 program and budget.

After the FY12 budget was submitted to the Hill, and in support of his broader deficit reduction effort, the president told DoD that future defense spending would be reduced by $400 billion over a 12-year period. As you might expect, this announcement started a series of 'what if' drills within the department. These efforts were well worth it because our savings target has now stabilized at more than $450 billion over a 10-year period. We are in the process of trying to determine our share of the cuts, how fast they will occur and how we will accommodate them in our program.

The only reason we would take a bigger hit is if the 'Gang of 12' — the Deficit Reduction Committee set up by the president and Congress — decides we need to take more defense cuts to reduce the deficit further. Alternatively, if the Gang of 12 is unable to come up with a plan, a sequestration reduction automatically kicks in which could cut defense spending by as much as a trillion dollars. So a trillion dollars is the absolute worst-case scenario.

Let me be clear, however. We are not focused on the worst case right now. We are focused on working the $450 billion cut. And the only thing we know for sure is that IT will be affected, as will every other major and minor program in the DON. To achieve these types of savings targets, every single program in the DoD and DON is being looked at as a potential source of savings.

CHIPS: What makes the drill different this time? Budgets have been cut in defense before.

Under Secretary Work: Well, it's certainly true we've faced cuts in defense before. In fact, since the end of World War II, and prior to the most recent buildup we just talked about, there were three big buildups and build-downs. The first buildup between FY48 and FY52 saw a big spike in peacetime baseline funding, first because of the onset of the Cold War, and then to pay for the Korean War. This

sharp spike was followed by a sharp post-war drawdown, which bottomed out in FY55 — well above the FY48 level. In other words, the requirements for our baseline strategy jumped as we were fighting the Korean War.

A second Cold War buildup started in FY55 to fund the Cold War strategy of containment. It continued until about FY64, and then accelerated because of the Vietnam War. The Vietnam post-war drawdown actually began in FY69 and continued until FY75, when the defense budget reset to FY64 levels. In other words, the requirements for our base strategy basically remained steady as we fought the Vietnam War.

The third Cold War buildup started in FY76 and topped out in FY85, when concerns about national deficits caused a reduction in defense spending. The following build-down was then accelerated by the collapse of the Soviet Union, and the subsequent dramatic reduction in our baseline strategy requirements. In other words, after we won the Cold War, base defense requirements went down.

So now we face another build-down. It's happened three times before. What's the big deal? The big deal is that this build-down promises to be different from those before it, for three reasons. To begin with, this is the first long war fought with an All-Volunteer Force. And, although the Army and Marines grew to fight the wars in Iraq and Afghanistan, Air Force and Navy end strength actually came down. As a result, overall DoD end strength remained relatively flat over the war. In the past, manpower would jump during the war, and you'd save money by quickly shedding wartime draftees once the war ended. But since we didn't grow much in manpower during the most recent build-up, we can't cut personnel without cutting into force structure dedicated to our baseline strategy.

Second, in past wars, wartime production would jump as you bought ships and airplanes and tanks to fight the war, and we'd cut this production upon war's end, saving big money in the process. But with the exception of MRAPs (Mine Resistant Ambush Protected vehicles) and UAVs (unmanned aerial vehicles), we purchased relatively little during this buildup. Consequently, our airplanes, ships and tanks are older and more worn out than they were before the war started, and we should be ramping up in production. So cutting production now would not be wise.

Finally, in the past, we'd save money by cutting direct wartime costs, such as ammunition, supplies, fuel and support contracts. But since we've paid for the wars in Iraq and Afghanistan with supplemental funding, any savings generated as we wind down these wars do not count as part of the president's savings target — all the cuts must come out of the base budget. So, the bottom line is that the entire $450 billion cut will come out of our base — and not wartime — budget, and we will lack many of the levers normally available to accommodate them.

Moreover, did the requirements for our base budget rise during the war as they did in Korea, or stay static as they did during the Vietnam War, or drop like they did after the end of the Cold War? A good case can be made that the demands on our base budget have been rising, and continue to rise. So we are faced with a much different challenge than those faced by past defense planners, and this will require us all to be very creative as we tackle the cuts.

CHIPS: One of the areas that you've asked the DON CIO to focus on is IT efficiencies and cost savings. You've identified 25 percent in cost savings to be achieved over the next five years. What are you anticipating coming out of that?

Under Secretary Work: When we participated in the [Secretary of Defense's] efficiencies drill last year, we were told to try and shift about $30 billion from departmental overhead, or 'tail,' to warfighting capabilities, or 'tooth.' We actually exceeded our target. Altogether we identified $42 billion in efficiencies and were able to divert that money to get all sorts of new capabilities. But it's important to note that IT was not a big part of that first round of efficiencies. It essentially took a pass. So when Mr. Terry Halvorsen came aboard as the DON CIO in November 2010, one of the first things I asked him to do was to look very hard at IT from a strategic perspective, and to reduce overall business IT costs by about 25 percent.

I wasn't really certain that a 25 percent reduction was the right target because I didn't know exactly how much we were spending on IT. You see, there is no budget line that says 'DON Business IT.' Instead, business IT spending is decentralized within both the Navy and Marine Corps budgets and hidden in so many different contracts. All I knew was that we were probably spending a lot on IT business services, easily more than $5 billion a year. So I asked Terry to first figure out what we were actually spending on IT and to then try to reduce those costs by 25 percent. Based on all the literature I read on IT cost reductions in the commercial world, and using IBM's IT cost-cutting program as a model, I thought a 25 percent reduction was a good target to start the IT efficiency train rolling.

"Business IT includes things like NGEN (Next Generation Enterprise Network), enterprise licensing, data centers, and the like. That is where we hope to achieve 25 percent savings."

The long and the short of it is that Terry has a mandate from Secretary Mabus and me to look at business IT spending from a strategic, enterprise-wide perspective and to save as much money as he can. Terry has the tasking and authority to try to squeeze every dime out of this enterprise. This is a cultural shift that, quite frankly, is meeting some resistance. But the Secretary and I are firm in our belief that there is money to be saved in business IT, and we want Terry to go and find it.

CHIPS: Do these savings targets apply also to tactical IT programs of record?

Under Secretary Work: Tactical IT programs include programs like CANES (Consolidated Afloat Networks and Enterprise Services) and JTRS (Joint Tactical Radio System). For the moment, we plan on keeping tactical IT programs and spending decentralized and tracked by the two services. So when the Marine Corps buys a radio to put inside an MRAP, or the Navy develops a radio that goes inside a new helicopter, it is left to service program managers and ASN RDA (Assistant Secretary of the Navy Research, Development

and Acquisition) to manage costs and save money.

Where Terry gets involved on the tactical side is when and where the tactical and business IT systems and networks connect. At these important points, we want Terry to enforce standards across the two services so that they can talk with each other and to joint units. For now, however, we think the real savings to be had are on the business side of IT, and that is Terry's main focus. Business IT includes things like NGEN (Next Generation Enterprise Network), enterprise licensing, data centers, and the like. That is where we hope to achieve 25 percent savings.

CHIPS: I see. Do you want to address what you're doing to focus on business IT now?

Under Secretary Work: Sure. Like I said, there is no single budget line that says: DON Business IT. So the first thing Terry is trying to do is to determine how much we are spending on business IT. To help us figure this out, Terry recommended two key policy changes. First, he asked that any IT spending project that exceeded $1 million have a solid business case analysis (BCA) to support it. This BCA would have to compare alternatives and clearly define expected costs, benefits, risks, and so on. Second, he recommended that only one person in either the Navy or Marine Corps be authorized to approve the BCA. At first, I felt that this was going to be really hard to do, but the more I thought about it, I thought he was exactly right. These two policies would help us get a handle on what we are spending, and they were the right things to do.

So now both the Navy and Marine Corps have a single ITEAA, or Information Technology Expenditure Approval Authority, who approves every business IT project that costs more than $1 million. Business IT spending is no longer decentralized; any service IT expenditure over this threshold has to be approved by either N2/N6 (Deputy Chief of Naval Operations for Information Dominance/ Director of Naval Intelligence and Deputy CIO for the Navy), Vice Adm. Kendall Card, or the Marine Corps Director of C4 and Deputy CIO, Brig. Gen. Kevin Nally.

By requiring these IT projects to go through a BCA and by having a single service approval authority, we are soon going to find out exactly what our total business IT bill is. Additionally, as we go through this process, we are going to find what kind of additional policies and safeguards we should put into place.

The second thing Terry did was to strengthen the DON's IT governance. Terry recommended that we establish an Information Enterprise Governance Board, or IGB, as the department's single senior information management/information technology/cyber governance board. It's run by Terry, and includes all of the IT stakeholders in the DON.

When the IGB needs to get an enterprise-wide business operation policy or decision approved, Terry brings it to the IGB's board of directors, which includes me, the Vice Chief of Naval Operations (VCNO) and the Assistant Commandant of the Marine Corps (ACMC). We approve or disapprove everything that Terry or the IGB recommends, so Terry automatically gets the support he needs from both Navy and Marine Corps leadership once a decision is made.

Establishing the IGB for IT governance, using BCAs to evaluate projects before spending, and establishing Navy and Marine Corps ITEAAs are the three key things that Terry has set up to help us get a handle on business IT spending, and I endorse them fully. I think they are working well. If we find we need more safeguards or additional governance bodies, we will establish them as well.

The third, and perhaps most important thing Terry is doing, is reducing DON business IT costs. He's already making good progress. One of the first things he tackled was better managing applications across the department. We've made a half-hearted attempt in the past to keep applications under control. For example, right now we have every single version of Microsoft Office ever made, and we are trying to maintain all of them. That makes no sense whatsoever. So we gave Terry the authority to scrutinize all departmental applications and get them down to a manageable and affordable level.

The second thing Terry is looking at to save money is in data center consolidation. This was one of the areas that IBM tackled aggressively and saved big money on, and it was one of the first things Terry and I discussed at length. Again, because business IT was so decentralized in the department, data centers sprouted up all over the place. Organizations were setting up data centers to store their own data, and it was very inefficient and expensive. Terry is going after this problem hard, and he has established policies aimed at consolidating data centers from a DON enterprise view.

A third area of focus for Terry is enterprise licensing. It turned out that the Marine Corps had the best enterprise licensing for Microsoft [products] in the department. Terry asked why shouldn't we just use the one that is the most advantageous to the department? Simple question, simple answer, big payoff.

CHIPS: I know that the department is also looking at cloud computing and email as an enterprise service by a commercial handler. Are you looking at implementing enterprise email as just a dot-mil email address?

Under Secretary Work: Terry has a lot of ideas about this, and we are still exploring all the different options. For example, OSD (Office of the Secretary of Defense) would like us to look at DISA (Defense Information Systems Agency) as an enterprise email carrier. Terry is exploring whether we could use commercial providers. We haven't made a final decision, but we know this is an area that we might be able to save big money.

Regardless of who ultimately provides the service, we want a strategic, enterprise-wide network. In other words, what we want is for anyone in the DON, no matter where they are, to be able to place their CAC card into a DON computer and pull up their email and be able to get the email address of anybody in the DON, whether it's a Sailor, Marine, or civilian. Right now we can't do that. We've given Terry the tasking to make that vision a reality.

Terry hasn't made a final recommendation yet because there are issues that still need to be worked out. But Terry has carte blanche to look at every single opportunity and to pursue the one that saves us the most money. As he goes through this process, he must look at a variety of issues. For example, if we went to a commercial carrier, there would be some security concerns. Will we be able to satisfy those concerns?

As things stand now, if we went with DISA, it would be a little bit more expensive than going with a commercial carrier.

Could we maybe get them [DISA] to bring their prices down? He is looking at all these things. This is a rather long answer to your question, but we are looking at this particular initiative very hard, because we hope to find significant savings.

"Now there are those inside the department who think we are being too optimistic in our savings projections. But in my view, in this budget environment, you have to set your savings targets aggressively."

CHIPS: When you talk about the business IT network, are you talking about NGEN?

Under Secretary Work: Yes, when talking about business IT I am primarily talking about our NIPRNET, which now resides on the NMCI (Navy Marine Corps Intranet) CoSC (Continuity of Services Contract), and in the future the Next Generation Enterprise Network, or NGEN. We consider NGEN and NMCI to be parts of the DON enterprise-wide business IT network, and we are doing everything possible to reduce the costs of providing these networks and services.

CHIPS: When you named Mr. Halvorsen as the IT efficiencies lead he established eight IPTs to examine some areas for savings. Do you have a status on the work they've done so far?

Under Secretary Work: Well, the first thing I can tell you is that for the last eight months they have been very hard at work. I think it's safe to say that Mr. Halvorsen is one of the most data driven CIOs the department has ever had. He demands good data for decisions, and he demands that all IT BCAs be supported by good data. These IPTs are responding to questions he is asking them, and they are becoming very good idea generators for the business IT enterprise.

For example, the DCC (Data Center Consolidation) IPT recommended we set a moratorium on purchasing more data center capacity because they think we have more data centers than we need. It's time to consolidate them and save some big money.

Now there are those inside the department who think we are being too optimistic in our savings projections. But in my view, in this budget environment, you have to set your savings targets aggressively. In essence, we want the burden of proof, that the savings targets are too aggressive, to be on IT managers. And if they can't achieve the savings by doing business the old way, we want them to think of a new way to conduct business that does.

Similarly, the Enterprise Licensing (Enterprise Software/Hardware and Software Commodity Purchases/IT Services) IPT was the one that said, 'Why don't we just exploit the Marine Corps? They've got a great enterprise licensing agreement with Microsoft so let's just use that across the DON to save money.' Made perfect sense, and we are moving in that direction.

The Navy and Marine Corps Portal Environment IPT is looking at all of our Web services and all of our portals and trying to come up with a single standardized Web portal service rather than having customized Webs and portals all over the place. At the very least, we want to have standards for each of them. A perfect example is in our sexual assault prevention and response program. If a young Sailor or Marine is the victim of one of these traumatic events, no matter where they are, we want them to be able to go to a website that has clear and easy links that connect them with the people who can help them.

All of our sexual assault and prevention websites need to be standardized and interoperable so when people need information — they can get it. We are trying to do that throughout the whole department on all of our programs.

The DON Telecommunications Environment IPT is trying to standardize our video teleconferencing (VTC) capabilities. We have video teleconferencing [equipment] all over the place, but it is unevenly spread. Some people have access to exquisite VTC capability, other people don't have access to any; some people have multiple VTC facilities throughout their organization, and other people just have one VTC facility. What IPT members are trying to do is figure out what kind of standardized VTC equipment units should have, and to what degree, and at what cost. We don't want to 'gold plate' it; we want a VTC [capability] across the department that works and is relatively inexpensive to operate.

We are also working on several IT workforce training and education initiatives. We are especially interested in improving our cyber warfare training capabilities. One of the most exciting things in this regard is called the Cyber Range, which is currently in use, as well as under continuing development. We envision it as a training and exercise environment that will provide our Sailors, Marines and civilians with the ability to improve their skills individually and as teams in cyberspace.

This doesn't cover everything we are doing. But I hope it conveys to you that the IPTs have been both busy and productive. We have eight now; we might need more in the future — or we might need less. Regardless of how many we have, they will continue to serve as the idea generators for Mr. Halvorsen and his CIO team. And they will continue to have to prove their ideas have merit before Mr. Halvorsen will present them to the IGB to get buy-in from the VCNO, ACMC, and me.

CHIPS: Will the DON portal environment eventually eliminate the individual portals that commands have?

Under Secretary Work: I don't know if that's going to be the final case, but I believe that in the future, instead of everybody spending a lot of money to customize their own portals, there might be more standardization of portals throughout the department. However, I don't want to say something that would foreclose Mr. Halvorsen's choices in this regard.

CHIPS: When you talked about the Cyber Range, is that tangible right now, sir?

Under Secretary Work: The DoD Information Assurance Range, which simulates the Global Information Grid, and Marine Corps Range are in place and functional right now. The Navy Cyber Range has initial authority to begin operation. DON CIO will be designating the Marine Corps as the DON Cyber Range lead to coordinate and combine Navy and Marine Corps efforts. The goal is a DON Cyber Range comprised of Marine Corps and Navy Cyber Range programs that will

serve as the cyberspace training environment within the DON by providing simulated Marine Corps and Navy network environments, which support test and evaluation, education, and major service and joint exercises.

CHIPS: Do you think the BCA templates are applicable outside of IT? Could other programs benefit from them?

Under Secretary Work: Yes, absolutely. I have a deputy under secretary, named Eric Fanning, who is my deputy chief management officer. He demands BCAs for essentially everything that is not a tactical or an operational system that comes up in our budget process. We are trying to use BCAs in as many ways as we possibly can in order to make sure we are getting the best return on every dime we spend and are reducing waste and duplication. BCAs are a great way to do that.

CHIPS: In a brief you gave at the Naval IT Day you mentioned comparisons between costs of personnel in 1998 and personnel costs now, and you said it would be difficult to garner savings from a reduction because the Navy and the Marine Corps didn't really build up. Have you identified any other cost savings related to personnel in the force?

Under Secretary Work: Although we've cut the number of people on active duty since FY98, our manpower costs have gone up by over 20 percent. We need to get a handle on rising personnel costs, or by the 2020s we will be in big trouble. The first thing we are doing in the department — and by this I mean the Department of Defense, led by the deputy secretary — is to review all of the different types of entitlements and pay benefits in a holistic way.

We are then trying to figure out where it might make sense to pursue savings. Our efforts are guided by the SECDEF, who has said he doesn't want to do anything that might be harmful to a strong All-Volunteer Force.

So it gets down to this: Are there areas that we might be able to achieve some savings that have no major negative impact on the recruitment and retention of quality people in the All-Volunteer Force? For any changes we recommend, we have to satisfy ourselves that we aren't going to upset the balance of what we consider to be the finest fighting organization that the United States has ever fielded. This effort is going to continue throughout the fall, and we expect to have some answers by next February when the president's budget is rolled out and made public.

CHIPS: The austere environment that the Defense Department is going to have to operate in can be pretty demoralizing to a workforce that is trying to do its best; should the workforce be encouraged by these reductions? Will they help the department?

Under Secretary Work: Well, first off, if you're ever going to be in government, I think this is the time to be in government. Whenever you have big changes afoot — like in 1993, when we did the first post-Cold War bottom-up review, or now when we are facing a major reallocation of our nation's resources — it's cool to be part of a process that will have big ramifications for a long time. It's a time when good ideas matter, and good people are the source of good ideas.

So you can react to what's happening in one of two ways. One is to say: 'Oh, my gosh! The sky is falling! How will we ever get through this?' And then shut down or sulk. The other way is to see this time as a great opportunity and be part of the solution.

When I was on active duty, we used to say you could either be someone who makes things happen or someone who wonders what the heck just happened. I've been in my job nearly two and a half years, and I think most in the Department of the Navy are those who want to make things happen. They realize what the Navy and Marine Corps offer to the nation, and that what the DON does everyday just cannot be duplicated by very many other organizations. But they also know we are going to have to keep being the best with fewer resources than we expected. I'm thinking most are going to help us identify ways to save money that might keep us from having to cut the workforce, or reduce force structure, or scale back on needed capabilities.

No matter what happens, the secretary, CNO, CMC, VCNO, ACMC and I are committed to taking care of both the men and women in uniform, as well as the men and women who make up our civilian workforce. While we are all probably going to have to take some cuts in the future of some kind, I don't think people should be demoralized. They should know that their leaders are fighting for them at every level of the department. And they need to get in the fight themselves.

"When I was on active duty, we used to say you could either be someone who makes things happen or someone who wonders what the heck just happened. I've been in my job nearly two and a half years, and I think most in the Department of the Navy are those who want to make things happen."

CHIPS: In some of the notes, you mentioned looking at acquisition, ship maintenance and shipbuilding plans. Is the department going to be able to protect resources to fund these areas because the fleets are getting older and there are concerns about the number of ships available for tasking?

Under Secretary Work: There is a common view among the DON's senior leadership that while the future Navy-Marine Corps team may be a little smaller than it is today, it is going to be a ready force. The last thing any of us want is a return to the hollowed-out Navy and Marine Corps team we saw in the late 1970s. So the one thing I can guarantee to everyone who works inside the department is that we are going to place great attention on maintenance, spares and logistics so that we avoid hollowing the Navy and Marine Corps from the inside out.

CHIPS: Is there anything else that you would like to add, sir?

Under Secretary Work: Just this: I am really proud of everybody in the DON. It's a great comfort knowing just how good our people are and how dedicated they are to the department and to our nation. To everybody out there I'd just like to say: Thank you for what you are doing. You inspire me every day. Keep up the great work. CHIPS

The DoD Information Enterprise

By Teresa Takai
Department of Defense Chief Information Officer


Teresa Takai

The DoD CIO serves as the principal adviser to the Secretary of Defense for information management/information technology and information assurance, as well as non-intelligence space systems, critical satellite communications, navigation and timing programs, spectrum and telecommunications. As the DoD CIO, Ms. Teresa Takai provides strategy, leadership and guidance to create a unified information management and technology vision for the department and to ensure the delivery of information technology based capabilities required to support the broad set of department missions.

Ms. Takai spoke about some of the challenges, efforts and efficiencies that she is leading at the Army's LandWarNet conference Aug. 24, 2011. Ms. Takai's remarks have been edited into an article and include additional information about the DoD information enterprise strategy.

I would like to give a bit of a backdrop in terms of what my job is. Because there has been concern about the changes that are planned for the Assistant Secretary of Defense for Networks and Information Integration and Department of Defense Chief Information Officer (ASD (NII)/DoD CIO) organization and what that means for the DoD CIO's role and responsibilities. First, the NII office has been part of the study for efficiencies across the Office of the Secretary of Defense. One of the key challenges that Secretary Gates gave us was to look for any and all efficiencies that we could take at the Pentagon to ensure that we had adequate funding, and so that we have as much funding as possible for the missions of the military departments.

We have reduced overhead in the number of personnel and the budget. We have removed redundancies in OSD, particularly across my organization and the Under Secretary of Defense for Acquisition, Technology and Logistics (USD AT&L). We are transferring some functions to AT&L because that's the most efficient way to do them. We will have a very close working relationship. As you know, we do a significant amount of our work with the Defense Information Systems Agency (DISA), and we will continue to do so.

My office will move from being titled as the Assistant Secretary of Defense for Network Information and Integration/DoD CIO, which was very difficult for the organization to have two roles, into the title of DoD CIO. That doesn't mean that we aren't going to continue to perform the functions, but what we need for our organization is to have a much tighter integration.

Another part of the importance of the organization moving forward is that we will have a very close working relationship with U.S. Cyber Command. Between my organization and the policy organization, we will be playing an oversight role with CYBERCOM, particularly as it relates to understanding the operations that it will do and looking at those from a policy perspective.

Lastly, one of the important roles for the DoD CIO is looking across the technology landscape and making sure that we are doing several things. First of all, for instance, we play the lead role for spectrum because one of the challenges is the growing need for all the services to have more and more spectrum to be able to conduct operations. On the other hand, we have increasing pressure from the commercial sector for that same use of spectrum, and so some of you may have been involved in studies we are doing to look at the future uses of spectrum and how we can ensure that the interests of the Department of Defense are protected and that federal government needs are met.

The second area is for us to play a role on the international stage with our partners and also with NATO to look at the technology standards that we need. Then lastly, we look at the technology and dollars that we need to provide the communications technologies that operational commanders need.

What we need to do is have a single look at the technology, not as a service-by-service or a COCOM-by-COCOM (combatant command), but to recognize that for the warfighter, what's really needed is a single look at the way we operate.

The Challenges Ahead

The warfighter expects and needs access to information — from any device, anywhere, anytime… But the challenge is how to get it there in the best way possible, how to get it out in a secure fashion, and also in a way that is quickly usable for the mission. As you look over time, we are no longer going to be able to do that from the devices that we have traditionally used. We are going to be moving to commercial devices, which is another challenge

If you look at the DoD IT landscape (Figure 1), it is easy to see why it is so difficult for us to get to a single secure, authoritative database and single search engine that warfighters need. It is tough to do when you have more than 10,000 operational systems with databases spread all over the world and more than 772 data centers, and by the way I think that number is pretty conservative. I think we have probably a lot more than that. In fact, every time we do an inventory, we find a few more data centers.

Then those 15,000 networks make it not only difficult for us to get information, but they are pretty tough to secure. So our points of vulnerability are considerable. If you tally up the num-

Figure 1. DoD IT Landscape	
IT Systems	**DoD IT User Base**
~ 10,000 operational systems (20% mission critical) > 772 data centers ~ 67,000 servers ~ 7+ million computers and IT devices ~ 15,000 networks	• 1.4 million active duty • 750,000 civilian personnel • 1.1 million National Guard and Reserve • 146 + countries • 6,000 + locations
Total IT budget > $38 billion in FY12	

bers, with more than 3 million individuals in the organization, it is difficult to effectively use a tool which is pretty straightforward like email, when you can't get email from one end of the department to the other without looking at it from an overall perspective.

The estimated $38 billion a year the department spends on technology is actually conservative. It was interesting; we were in a meeting earlier this week talking with the Air Force about some of the efficiencies that it is doing. The Air Force found a significant amount of more money than it even knew it was spending on technology. So I would submit to you that while we have a lot of efficiencies drills coming at us, we have a lot of money that we can take and utilize in a different way to get to our end objective.

Other challenges ahead include exploding technologies, shrinking budgets and the growing cyber threat. I don't think this is new to you, but I want to add a different context around the actions that DoD will be taking.

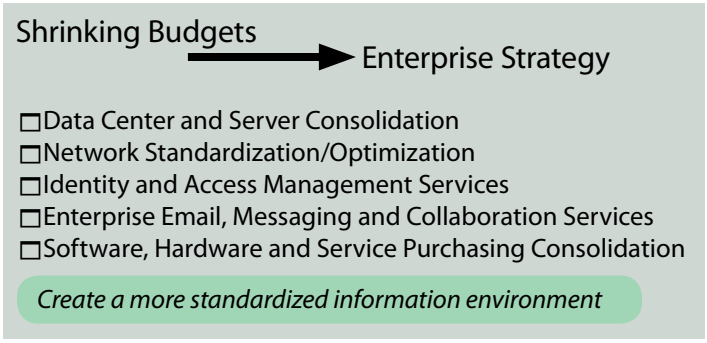


Figure 2.

Shrinking Budgets: Enterprise Strategy

It's easy to say, we either can have efficiencies or we will be effective, or we have to respond to the cyber threat, because those things won't work together. I submit to you that they do, and that the actions that we will take (shown in Figure 2) to effectively make the changes are, in many cases, the same actions.

The first piece is shrinking budgets, and each of the DoD organizations has been very aggressive in identifying IT efficiencies. Clearly, some of the things you are working on now are the data center and server consolidations. But data center consolidation isn't just about getting the footprint down. It is really getting to how we move to more standardized ways of operating, not just because it costs less, but because it gives us the ability to more quickly field new capabilities on a standard infrastructure.

The second piece is the number of networks and email systems that we have, and we will need to change for the way that we will operate in the future. To access the network of the future, identity management will allow you to get the information that you need. This includes the ability, not only to identify you, but to be able to link your identity to the information you need.

"The warfighter expects and needs access to information — from any device, anywhere, anytime… But the challenge is how to get it there in the best way possible, how to get it out in a secure fashion, and also in a way that is quickly usable for the mission."

Cyber Threat: Exploitation, Disruption and Destruction

Now put the challenges against the backdrop of the growing cyber threat. [Former] Deputy Secretary William Lynn uses this lexicon: "We are in the midst of a strategic shift in the cyber threat…moving up the ladder of escalation."

Clearly, all of you who protect and defend IT systems recognize the threat. But what we see now is the exploitation of DoD networks. We see the theft of email addresses. We see utilization of that information to get in, not only DoD systems, but those of our industry partners to look at intellectual property and information. The next escalation of exploitation will be disruption. We saw it occur in Estonia; we have seen it in other areas of the world.

We are moving away from just purely the concept of the need to protect at the perimeter of the network. We are concerned about the potential for disruption to lead to destruction. We are concerned about the juxtaposition of the cyber threat with the kinetic threat.

The services are conducting a number of exercises to look at the resiliency of networks and IT systems, as well as defense and protection. This becomes very much a public/private requirement, it's something the DoD cannot do alone; we must include industry partners.

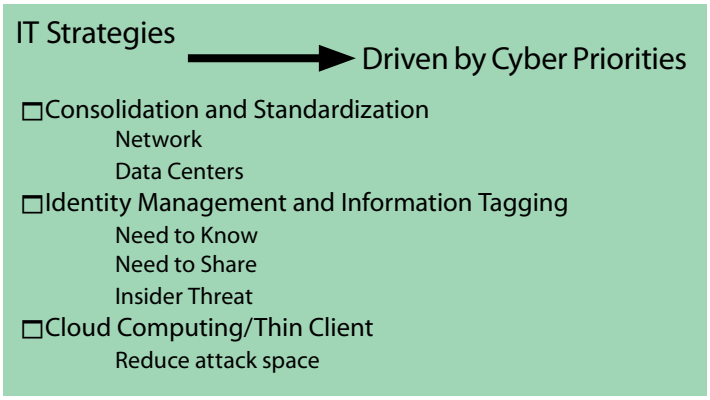
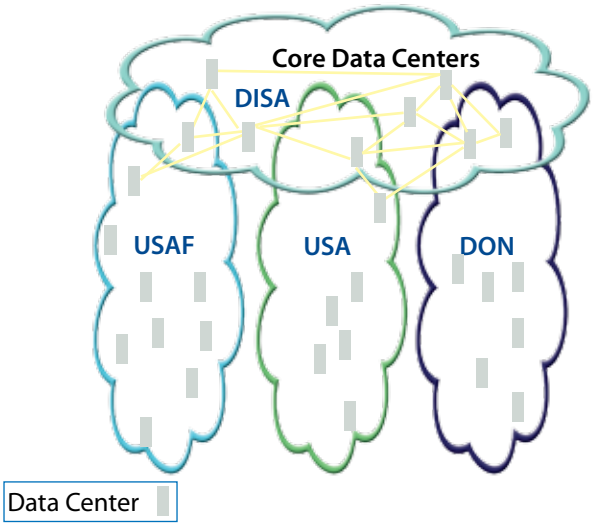


Figure 3.

IT Strategies: Driven by Cyber Priorities

The IT strategies that I described (shown in Figure 3) are part of our efficiencies strategies, and the same strategies we need to use to address the cyber challenge. Consolidation and standardization will give us a much better way to decrease attacks on DoD networks and IT systems and can improve network defense. Now the challenge that everybody points to is that if there is one network the department is more vulnerable. That is

Figure 4. The Community Must Change to This Model.



true. But, we will never have one network. We have many legacy networks and systems, and we don't want one network or one way to protect and defend it. At the same token, there is a big difference between one network and 15,000 networks.

Our challenge is, and we are smart enough to figure it out, the right mix to be able to defend much better than we can today, and also ensure that we are engineering and managing technology in a way that decreases threats. IT strategies, like identity management and information tagging, allow us to more easily control the need-to-know and need-to-share, not only from the standpoint of external intrusions, but also to address insider threats.

Lastly, as we move to cloud computing, we will be able to move information into more standardized ways of accessing it. At the same time, a thin client infrastructure, in certain instances, is going to decrease our attack surface in the field. We will have the ability to share information more easily because it will not be traversing multiple networks and multiple data centers. Instead, DoD networks and IT systems will be configured in a way to share information. Operational commanders will be able to get to unclassified, classified and top secret information as it relates to a particular mission as dynamically as they need to.

Figure 4 is a great visual perspective of what the department is working to achieve. It is important to see that as we talk about enterprise and doing things together, there is still the need for the Army, Air Force, Navy and Marine Corps to have operational effectiveness within their operations, but to be able to come together for a core sharing of information and core use of DoD networks more effectively.

Effectiveness and efficiency do not always go hand in hand, there's a yin and a yang in terms of the push and pull. But, there is a way for us to be able to preserve the services' individual requirements and yet look at the broader perspective. That is what I really see as an important role for the DoD CIO office to play — to really bring us all together in the broader mission.

Exploding Technologies: Mobile Devices, Thin Client and Cloud Computing

We have to recognize changes in technology development; it is driving the need to change and standardize. As we look

"We have to recognize changes in technology development; it is driving the need to change and standardize."

at commercial mobile devices, there are two factors that are really a challenge for us: we do not control their development and understand how to fit these devices into our networks. In the past we developed our own wireless communications. We developed radios and used commercial off-the-shelf technology to some extent, but we were able to influence the market because we were the largest customers. That's no longer true.

Some of the things that the Army is doing will be a big part of what we will do in the future, to ask questions like: Do you have a radio that is longlasting? Should every Soldier have the same radio or are the radios specific to a function? Is it necessary to have only one device for information?

To accommodate commercial technology, we have to move to a much more standardized infrastructure, so that we can secure it, so that we can lock it down, so that we can understand where the information is going, and we can look at ultimately how we communicate in a cross-domain environment.

A mobile device is a small thin client, and as we move toward thin clients, we are going to be thinking about how we use them on a more broad-based standpoint.

And then of course the term that all of us love, it is sometimes maligned and sometimes misunderstood, is cloud computing. Cloud computing is a service model of the way that our IT services will be provided. We don't all need to own our box, we don't need to see the server lights blinking. We need to know that we can get services from a standardized place and be able to build and innovate to the next level.

Cyber Challenges Beyond DoD: Supply Chain Risk, Attack on Defense Industrial Base and Critical Infrastructure Protection

There are cyber challenges in what we are doing. First, we are looking at the risks in the supply chain. In a global marketplace, we are seeing less and less of an ability to control the components that are in the technologies that we buy — for both hardware and software. We are working on a study with telecommunications providers to understand where our risks are throughout the supply chain.

The results will be to No. 1, understand where we have to take more control of the supply chain, and secondly, to better understand our vulnerabilities, which will impact the way we look at resiliency. Knowing that we have risks in our infrastructure, we can determine what we can do to combat the risks and be able to, in case of a breach or disruption, come back online very, very quickly.

I mentioned, we are seeing more attacks on the defense industrial base. One of the things we are working on is to form partnerships with defense companies. We have about 36 companies, and we are looking to expand that to the next set of companies that came to us through U.S. Transportation Command (TRANSCOM) so they can share information about the threats they are facing.

We are looking at the importance of critical infrastructure

"It doesn't do us any good to be protected inside the DoD if the critical infrastructure that we depend on is not protected as well."

protection. It doesn't do us any good to be protected inside the DoD if the critical infrastructure that we depend on is not protected as well. This is a joint effort with the Department of Homeland Security, particularly as it relates to the continental United States, to make sure that we are working with the energy providers, that we are working with critical infrastructure officials to be sure that the DoD is looking at the cyber threat on a broader stage.

Figure 5. Enterprise Email

As Is	To Be
• Lack of permanent email address. • Inability to view a Global Address List for all components. • Lack of an integrated email messaging platform. • Unnecessarily dissimilar security processes.	• Access from anywhere, at any time and from any place (stationary or mobile). • Easily discoverable contact information within the DoD enterprise. • Continue mission critical operations when disconnected from the enterprise email network.

Army Enterprise Planning

I want to thank and congratulate you for the work that you are doing to push forward the Army IT enterprise. Lt. Gen. Susan Lawrence, Army CIO/G-6, has been an absolutely fantastic partner in looking at where the department should go. One of the challenges of being at OSD is to understand the important policies we need to make your operations easier across DoD.

I have to make sure that the policies the DoD issues are implementable and that they are going to make a difference for all of you. I will use a couple of examples because I think these are things that are affecting you sometimes in a good way, sometimes in a very disruptive and difficult way, and to give you a perspective on why working to an enterprise approach is so important across DoD.

Figure 6. Enterprise Email — *Keys to Success*

- Optimize email solutions to the least number of platforms.
- Ensure that all DoD users have stable identities.
- Develop and implement a strategy to unify collaboration mechanisms, including email, chat, voice, video and data exchange.

So I picked the beloved enterprise email example (shown in Figure 5). Across the DoD there are multiple email addresses. Quite frankly, I am sure you have challenges identifying who is where and how to communicate. Second, we are unable to understand the global address list and move to an integrated email platform because organizations within DoD have very dissimilar security practices.

Enterprise Email — Keys to Enterprise Success

Figure 6 illustrates the advantages of enterprise email; it is a forcing function to make the kinds of infrastructure changes we need. By moving to enterprise email, we are beginning the journey of getting to a single identity — and of having that identity linked to information. So email is a part of getting us to a common directory and the kind of identity management that we need so we can share information more effectively.

Second, it gets the department on a more common infrastructure. We will move to a standard gold disk so that we can get to a common configuration, not only in the Army, but across the services, and that's one of the things that we have been working on with the Army. A standard gold disk is one of the policies we will be issuing in the future.

Lastly, this effort isn't just about email. All of you want to be able to use SharePoint, to use text and instant messaging across the services and combatant commands, and without having to stand up multiple instantiations of these environments for the specific missions that are necessary. So the objective and what the Army is doing in terms of email is to really drive that forward.

The Army has taken a big, bold step that we have challenged the other CIOs in the other services to do: *to move from an email address that is army-dot-mil to an address that is mil-dot-mil.*

Seems like a pain in the neck? But what it will do is give us the ability to share information. Can you imagine the administrative burden that it reduces to change your email address every time you change positions?

But more important, one of our collective efforts is with the Department of Veterans Affairs for electronic health records. The connection is if we can get to a common identifier, then as a service member you will have a common identifier from the time that you enter the service throughout your military career, and when you leave service and are provided services by the Veterans Affairs system. So enterprise email has far reaching advantages.

Figure 7. Joint Enterprise Network

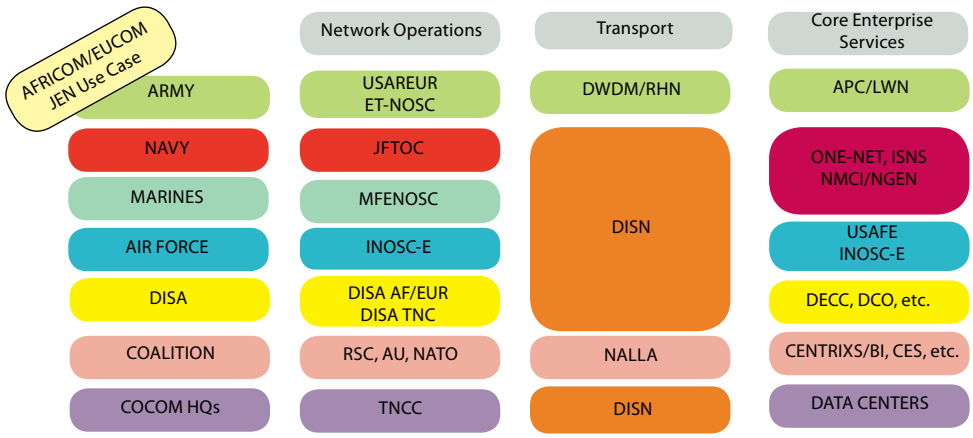
As Is	To Be
• Unique communications, data processing and security posture in USEUCOM and USAFRICOM. • Huge challenges in connectivity and collaboration. • Not efficient or effective. • Security problems and inconsistencies.	• Joint governance supporting USEUCOM and USAFRICOM. • Provide: – Net-centric enterprise services – Consolidated IT service support – A common NetOps architecture – Redundant transport and connectivity • Meet DoD and NSA requirements, improve security, and maximize investments. • Collapse ~ 50 Army sites into the DISN theater infrastructure.

The Joint Enterprise Network

The next initiative which is important is the Army's role in an effort between U.S. Africa Command (USAFRICOM) and U.S. European Command (USEUCOM) to stand up common data centers and infrastructure from a network perspective. AFRICOM and EUCOM came together, with the support of the Army, to standardize the unique communications, data processing and security posture in the European and Africa commands.

Their efforts to improve the Joint Enterprise Network are

Figure 8. Network Optimization
Joint Information Environment (JIE)



"For the DoD, it's about understanding the needs across the department and looking at policies, processes, standards, and the things that we need to do from an OSD perspective to allow you to be able to do your jobs and move the entire organization forward."

shown in Figure 7. Figure 8 illustrates how we operate today. I am sure you will recognize the boxes. From network operations and transport perspectives, this is effectively our case for changing how we need to optimize the network in the future and how we need to institutionalize what EUCOM and AFRICOM have been able to do.

The objective is to move toward an integrated joint NetOps, joint transport, and then consolidated enterprise services, like collaboration tools, as shown in Figure 9.

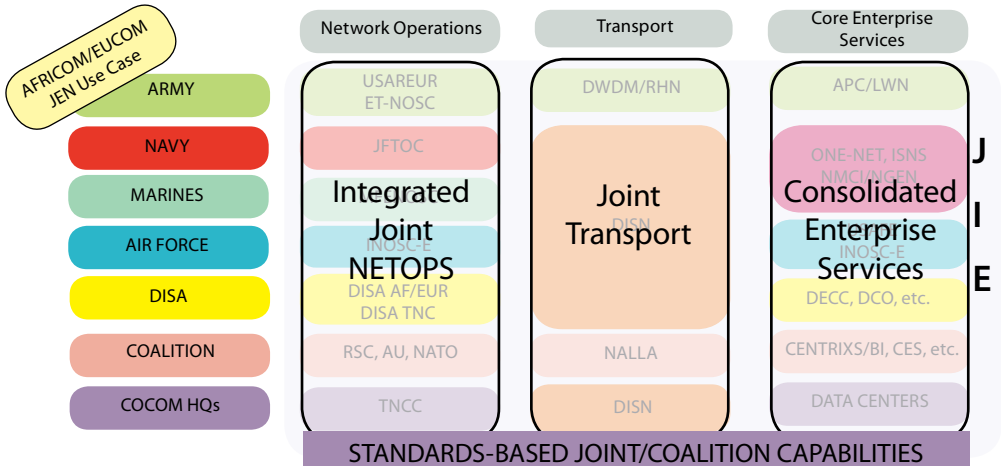
We have to think about how this example can be extended into the way that we support the COCOMs in the future. Bringing together all the services and COCOMs into an infrastructure that allows the necessary applications to be built very quickly, fielded very quickly, and quite frankly, if we can build and field them quickly, we can also get rid of them and move on to what the next set of needed applications is for the next area of conflict and next area that we have to provision.

We really see the DoD, DISA and Army in a partnership. We are working very hard to make sure that No. 1, the Army is well supported. DISA Director Lt. Gen. Carroll Pollett and I are working very hard. DISA is working very hard for the success of the shared services model. DISA is moving beyond the backbone network into broader use of its Defense Enterprise Computing Centers (DECCs).

DISA is working to provide enterprise services, not only for Army, but across the DoD. In many ways, it isn't just about providing the services, it's about DISA looking at the technical directions that the department wants to take in the future and being a part of setting those technical directions. For the DoD, it's about understanding the needs across the department and looking at policies, processes, standards, and the things that we need to do from an OSD perspective to allow you to be able to do your jobs and move the entire organization forward.

Lastly, the department wants to take advantage of the great work all of you are doing — whether it's in enterprise email, your role in the joint environment or whether it's the work that you're doing at Fort Bliss to set the stage for fielding new technologies — all these efforts are going to be cornerstones to pull the technology infrastructure together and provide these capabilities, not only now and tomorrow, but five years from now with new mobile technologies, and 10 years from now with technologies like cross-domain sharing, a universal search engine and getting the information in a protected way to those individuals that need it. CHIPS

Figure 9. Network Optimization
Joint Information Environment (JIE)



The Challenge:

Information is a strategic asset. It must be given the same priority and protection as any mission critical system or platform. Success in day-to-day peacetime functions, during stability and support operations, and armed conflict will be dependent upon our ability to connect people with information and create an information advantage for our team and our mission partners.

Our transformation to a 21st century, net-centric force is dependent upon ultimate delivery of the critical enabling capabilities.

The ASD NII/DoD CIO provides the leadership that is turning the vision, *Deliver the Power of Information*, into reality.

– http://cio-nii.defense.gov/.

The Communications Special Forces Need

By Adm. William H. McRaven
Commander, U.S. Special Operations Command

Robust, reliable, trusted communications are in high demand by Special Operations Forces, and Adm. McRaven, commander of U.S. Special Operations Command, talked about their specialized communications needs at the Army's LandWarNet conference Aug. 24, 2011, in Tampa, Fla. The admiral's remarks were edited into an article to focus on the communications and information technology needs of Special Forces.

The mission of U.S. Special Operations Command is to provide fully capable Special Operations Forces to defend the United States and its interests, and to synchronize planning of global operations against terrorist networks.

Adm. William H. McRaven assumed command of USSOCOM Aug. 8, 2011. McRaven, has been called "one of the most experienced terrorist hunters in the U.S. government." A SEAL himself, McRaven, as the commander of the Joint Special Operations Command (JSOC), selected the special unit of Navy SEALs (Sea, Air and Land teams) that killed Osama bin Laden in Abbottabad, Pakistan, May 1, and in which, communications played a pivotal role.

I want to talk about special operations. I want you to know who we are, and I think who we are might surprise you a little bit. I want to talk about how we communicate, why we communicate, and then I am going to reach out and ask you to help me solve some problems within the Joint Special Operations communications arena.

As special operations folks, we like to think of ourselves as at the tip of the spear. We are generally the first ones in and the last ones out. In this case, the spear that is part of our insignia has three bands — that's for air, sea and land — and our heritage traces us back to the days of Maj. Gen. "Wild Bill" Donovan, who was the head of the OSS (Office of Strategic Services). And we like to think that those same qualities that the OSS had — that imagination, that creativity — is part of what makes SOCOM who we are today.

Yin and Yang of Operations

We have what my predecessor, Adm. Eric Olson, called the yin and yang of operations. When you think of special operations, most of the time folks think about kinetic operations, the direct action, the raids. That's generally what makes it in to the newspaper. But frankly, the harder part of our job is engagement. When you look at the young Special Forces NCOs (non-commissioned officers) and officers downrange, in terms of engaging with the tribal leaders in Afghanistan, building the Afghan police — this is the much harder part of the job.

But the thing about the yin and the yang is that if you are going to conduct a direct action mission, you better know how to do engagement because at the end of that operation you are going to have to talk to the village elders and explain to them why you came into that compound. Conversely, if you are doing engagement, you darn well better know how to fight because invariably the fight comes to you.

SOF as an Organization

First, we are global. Right now we are in 76 countries around the world. Normally, on any day, 365 days a year, you will find special operations forces in somewhere in the neighborhood of about 70 countries. Sometimes there are just one or two guys, sometimes there is a hundred, sometimes there are a couple thousand, but we cover the globe.

We are joint. We are raised joint. Joint Special Operations Command has component commands, United States Army Special Operations Command, which is at Fort Bragg. Lt. Gen. John Mulholland has the job to man, train and equip the Special Forces, the Rangers, the 160th Aviation (160th Special Operations Aviation Regiment (Airborne)), 4th Military Information Support Group, and he's got the JFK Special Warfare Center and School.

On the Air Force side, out in Hurlburt Field, the Air Force Special Operations Command (AFSOC) maintains all the fixed wing and tilt-rotor wing aircraft. They have a special tactics squadron, and they also have an Air Force Special Operations school. In California, at Coronado, the Naval Special Warfare Command has the SEAL teams, the special warfare combatant-craft crewman, or our special boat guys. They have our SEAL Delivery Vehicle teams — these are little wet submersibles, and then they have the Naval Special Warfare Center.

Then our newest component is the Marine Corps Special Operations Command out of Camp Lejeune. They have the special operations regiment, battalions and support groups. They have a school as well, and then the command I just came from, the Joint Special Operations Command [is another].

We are raised in a joint environment. If you are a young Ranger, you have jumped out of an Air Force aircraft, and you have spent time with Navy SEALs. If you are a Navy SEAL, I guarantee you have spent time with an Army ODA [Operational Detachment Alpha, a standard 12-man team composed of U.S. Army Special Forces operators]. It is about the "jointness," and this is one of both the advantages of our organization, and frankly, when it comes to communications, one of the tactical challenges we have.

We are interagency, and this really began for the most part since 9/11. I don't conduct a single operation any day of the year that does not have some interagency component — CIA, NSA (National Security Agency), DIA (Defense Intelligence Agency), NGA (National Geospatial-Intelligence Agency), FBI and others. We have somewhere in the neighborhood of a couple of thousand interagency personnel that are working with our units downrange every day.

We (USSOCOM) are both a COCOM and a service. As a combatant commander, I have a responsibility globally to synchronize the war on terrorism; that is my COCOM responsibility. In

my service-like responsibility, I have the requirement to man, train, equip, deploy and, when called upon, employ forces. I, unlike any other COCOM, have a budget. I have acquisition authority. I have the responsibility to make sure that promotions and advancements for our officers and enlisted are taken care of. SOCOM is a very unique organization.

We are distributed. So I talk about our global footprint, our joint footprint, our interagency footprint. We have a very distributed communications architecture — 560 nodes. These are generally the folks downrange that have the SDN lights, the SDN mediums [broadband satellite communications connectivity; core Ku band (SHF) 0.95 to 12.75 gigahertz link].

Of course, from there we branch out even further. About 54 garrison nodes, that's Fort Bragg, Fort Campbell, Hurlburt, five soft strategic entry points around the globe, 59,000 global users. We use both government and commercial satellites and any other infrastructure we can find that can pass information, that's part of our distributed network.

Adm. Bill H. McRaven, commander of U.S. Special Operations Command, addresses the audience at the AFCEA International LandWarNet conference in Tampa, Fla., Aug. 24. The conference is designed to bring both government and industry together to discuss best business practices. McRaven outlined the role of USSOCOM and the communications challenges the command faces, while also challenging those in attendance to develop cutting-edge communications capabilities for Special Operators.

Cost Effective

I like to think that we are the most cost effective capability that the U.S. government has. I have about $10 billion a year as my annual budget. That is only in fiscal year 2011, only 1.4 percent of the Department of Defense budget. This next year (FY12) we will be 1.6 percent of the Department of Defense budget. We are only 3 percent of DoD personnel, but right now we are 7 percent of the forces in Iraq and Afghanistan.

If you take a look at what Special Operations, Special Forces, SEALs, Rangers, etc., have been doing in Iraq and Afghanistan since 9/11, I think the return on the government's investment, on the American citizens' investment, has been well worth it.

About 11.2 percent of my budget is spent on C4IAS (command, control, communications, computers and information automation). So a large amount of what I do is about command and control.

Special Forces Profile

As you would expect, overall strength and a large portion of Special Forces are military, but we have a pretty good slice of both contractors (8 percent) and government (9 percent) service. The interesting thing about the 83 percent of military is they are not what we would call "badged" special operations. They're not SEALs, not Rangers, not SOF guys. They are general purpose forces that come to SOCOM. But very quickly when they come on board, we make them special operations folks. We make them think like SOF operators. We make them act like SOF operators. We make them move at the speed of war, and this is what makes this organization as agile and as good as it is.

The average SOF operator is about 34 years old. That's not to say we don't have younger SOF operators in the Rangers and the SEALs, but the average guy is about 34 years old. He is college educated, married and has at least two kids. So this idea that the SOF operator is out there and he's some lone wolf "Rambo" guy who lives alone in an apartment by himself just isn't borne out by this.

Most of these guys are thinking athletes, somewhere in their childhood they played football. They ran track. They wrestled. But a very interesting statistic — we pulsed 1,000 guys entering some of the various schools at the SF center at basic underwater demolition SEAL training, and as we looked across their resumes, the one thing that popped out more than anything else was that they played chess. Not something you would think of as a guy coming into a special operations career, but again these guys are not only athletes — they are thinking athletes.

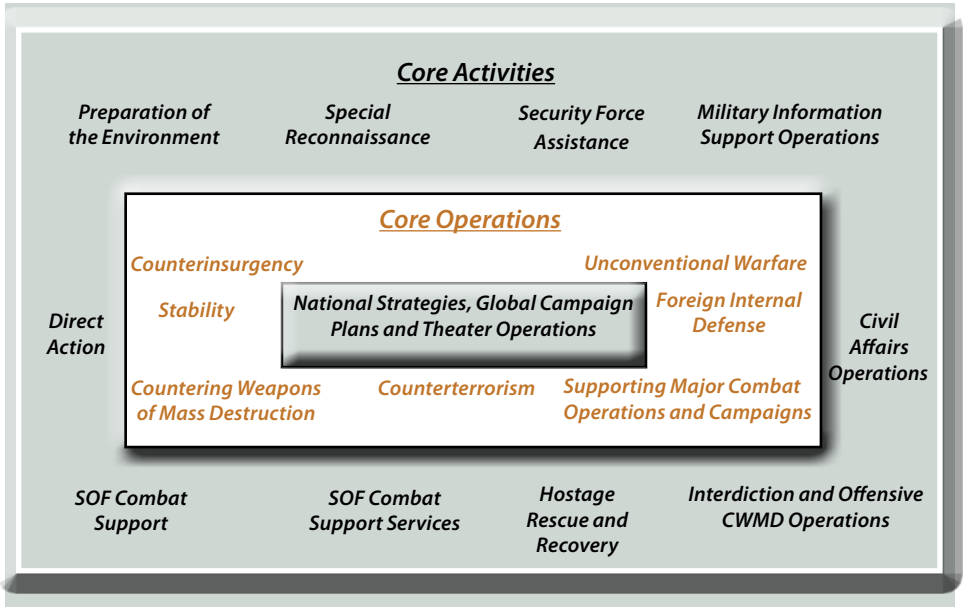
Eight years of time with the general purpose force so they come in with an understanding, particularly on the Army side, of what the conventional forces can do for special operations, and they bring the great part of that conventional thought process into SOF — and we need that. Multiple advanced tactical schools and most of them speak at least one foreign language. I would be the exception.

SOF Scope of Operations

We've recently redefined how we look at SOF operations and activities. We do core operations so the two that most people think about are counterinsurgency and counterterrorism. But there are supporting missions. So, for example, in a counterinsurgency, you will have preparation for the environment, special reconnaissance, direct action, combat service support, SOF combat support, military support information operations, civil affairs, conventional weapons management and disposal (CWMD).

You may do a hostage and recovery mission in the middle of counterinsurgency. So these activities support the core missions, and this has really helped us think about how we do our business, and it's been a very helpful construct for us. (See Figure 1.)

Figure 1. SOF Core Activities/Operations



Daily Communications

We communicate through 321,000 emails per day across this global distributed network. Video teleconferences: 210 per day. When I was a JSOC commander, I did six video teleconferences a day; each one lasted about an hour. And those video teleconferences were my opportunity to pass information to my force and to receive information. So the criticality, the clarity of that information, of that communication network, was absolutely critical to how I got my job done. And I only did six of those 210 per day. Today, communications are Web-based: 72,000 portal hits per day, and then 424,435 phone calls per day.

And, of course, now guys are on chat and any sort of instant messaging that you can think of. You see people using those in lieu of email today. So we have a fairly robust SOF enterprise network.

Why We Communicate

Command and Control. There are times in our communications process where we need to be able to communicate more clearly than others. First, we obviously communicate to command. So as a commander, and for any of my 06 or 05 commanders, we put out commander's guidance.

Now frankly, in the world of communications, I would contend this is probably the easiest part of how we communicate. For those of you who are commanders, you know you want to work very hard to make that command statement very succinct, very clear, that can be put out in a single sentence, in a single paragraph, and it generally communicates across a variety of mediums pretty well.

Now you have to be able to control. Control is now a different level of communication; it requires a different level of fidelity. So as we control, that young colonel, or that young lieutenant colonel, who now has unmanned aircraft, manned aircraft, he's got troops on the ground, and he's maneuvering those troops in combat to control them.

Send and Receive Intelligence. With each step we require more and more clarity, so if we are sending and receiving intelligence, I guarantee you what I need is high definition video from a UAV. I need still pictures that are crystal clear. I need to make sure the information that's coming across the radios, or mIRC chat, is as clear as it can be so we don't misinterpret what the guy in the field is seeing or how we are relaying intelligence.

Target the Enemy. Now of all these, targeting the enemy becomes the one where we need the most precise information. So as you are looking at a high definition video of a guy on the ground, is that a Taliban fighter with a RPG (rocket-propelled grenade) or is that an old man, a wood cutter, that's just carrying a load of wood on his shoulders? Are those 15 military-age males or are those women and children? Because if you make that mistake, you are going to inadvertently kill civilians, and that's the last thing you want to do in a counterinsurgency.

Counterinsurgency operations are about making sure that you are supporting the population. So our targeting and how targeting information flows is absolutely critical.

Pass Information to Higher Headquarters. So after we target the enemy, then we have to be able to pass information to higher headquarters. This kind of cycle, this ebb and flow, really goes from command where we have got to have some degree of clarity to returning that information back to higher headquarters, and then that bell curve in the middle is where we need our peak communications clarity.

So as soon as an operation is over, we are moving information back to higher headquarters, and they've got to have essentially the same level of fidelity we had as they continue to pass it up. A lot of times in Afghanistan and Iraq when we conduct an operation, it will become an international media hit within about 30 minutes. So if we have conducted an operation, whether it has gone well or poorly, it will be on CNN within 30 minutes and, therefore, the information that we have to get back to our boss has got to be as accurate as we can make it. And sometimes, that is a pure function of the communications architecture we have to support our troops.

Build Trust and Establish Relationships. Everybody that's been to the battlefield in Afghanistan knows that you have to build trust and relationships with the local population. Frankly, we build a lot of trust and relationships with people through video teleconferences. So the real question is, as I'm doing a video teleconference with one of my allies, coalition partners, or with one of my Afghan allies, am I getting everything he's trying to tell me? Am I seeing his body language?

Do I understand exactly what he's saying because that communications medium becomes critical to my understanding of the situation and my ability to build a relationship, establish trust and, in fact, get the job done.

Crisis Management. Now what you have is all of those things except in a very compressed environment. So when we have a crisis situation, which for some reason we seem to have crisis situations every day, when you are in places like Iraq and Afghanistan, we have to look at all these needs as compressed in time and

space. *And therefore, everything we have in terms of how we communicate has got to move at the speed of war.*

Pass Assessment. This is a continuous communications cycle. We are not a linear organization, so everything is going on 24 hours a day, 7 days a week, 365 days a year. We are communicating in the ways I described, and in a thousand other ways across the globe, across the joint environment, across the interagency, across the coalition, across all possible networks. (Summarized in Figure 2.)

Special Operations Communication Needs

A Universal Domain. I would like to be able to pick up my iPhone or my Android, or whatever smart phone, and be able to communicate with all of the folks I talked about, but not worry about the security protocol or device. Do I have the right crypto on the other end? How do you tag the information so that if I'm going to write an unclassified email, it has a green border, or the text is green, and when it is sent, it can go to everybody that can receive green text? And if it's secret, there is a blue border, and only those people that have the ability to receive blue text get it, and if it is top secret it's red.

How do you use artificial intelligence to tell me whether or not that information is classified based on a number of screening criteria, and it allows me to use whatever medium I have to transfer or translate that information? That to me is a universal domain. We talk a lot about the problems of cross-domain solutions; it is hard for me to take information from my crypto-side and transfer it to my unclass-side. But this is a problem, and it slows up in the way we communicate.

Improved Reception. I'm new on the job as USSOCOM commander, and for about the last three years I've been overseas most of the time. So we are about to move into our new house, and I've decided I want a television. I just don't want any television; I want the biggest television out there. I saw a 70-inch television and that's what I want. So I was looking at televisions, and it's kind of like that commercial, I was fixated on this TV.

And this young man comes by and sees me looking at the TV and he says, "You know, that TV has yellow." I said, "Really?" He said, "Yeah, it's got yellow in it." And he looked at me like where have you been for the last couple years? Of course, I began to understand what he was saying, that most TVs display a picture in blue, green and red and this one also had yellow. As I looked at the TV, of course, the quality of the picture was a lot better because it had yellow. Who knew? But the fact of the matter is that made a difference in how I perceived the information.

[Another example] When I was in Afghanistan in a gymnasium on the treadmill doing my four-minute mile and watching Wolf Blitzer, the volume was low (as in most gyms) so there is a speech-to-text scroll. But we don't have that capability in our VTCs — but maybe we could.

So my challenge to the "6" community for those that manage information, is: Help me receive and understand information better. I've used some great products, perceptive pixel, telepresence, and they are light-years better than some of the other products in terms of my ability to receive information, but it is still not good enough.

Enterprise Cloud. On those six video teleconferences that I did a day — I can tell you that most of the time I only received about 50 percent of the information, or I'm only ingesting about 50 percent of the information. Therefore, I am losing a lot of information. We can't afford that. We need to have a SOF enterprise cloud that allows me platform independent ability to reach out and get the information I need from wherever I am on the globe because both in law, and as the SOCOM commander, I have the responsibility to synchronize the global war on terrorism, and because I am distributed across 76 countries daily, it is important that any of those individuals that are part of the 59,000 global users can access the cloud.

Full Spectrum Search Engine. We have stovepipes within our databases, but what I'm looking for is a universal or a full spectrum search engine that allows me to find what is in my top secret, secret and unclass databases, something that can work across domains to get the information I need.

Ironclad Protection. Then, as always, we need ironclad protection. With most of our systems, we have three means of protection: the Common Access Card, a password, and in a lot of cases, biometrics. But at the end of the day, I'm not sure any [of these security measures] gives me the ironclad protection I need as part of the SOF enterprise.

Figure 2.
How and Why Special Forces Communicate

How

- ☐ **Email – 321,000 per day**
- ☐ **VTC – 210 per day**
- ☐ **Portal Hits – 72,000 per day**
- ☐ **Phone Calls – 424,435 per day**

Why

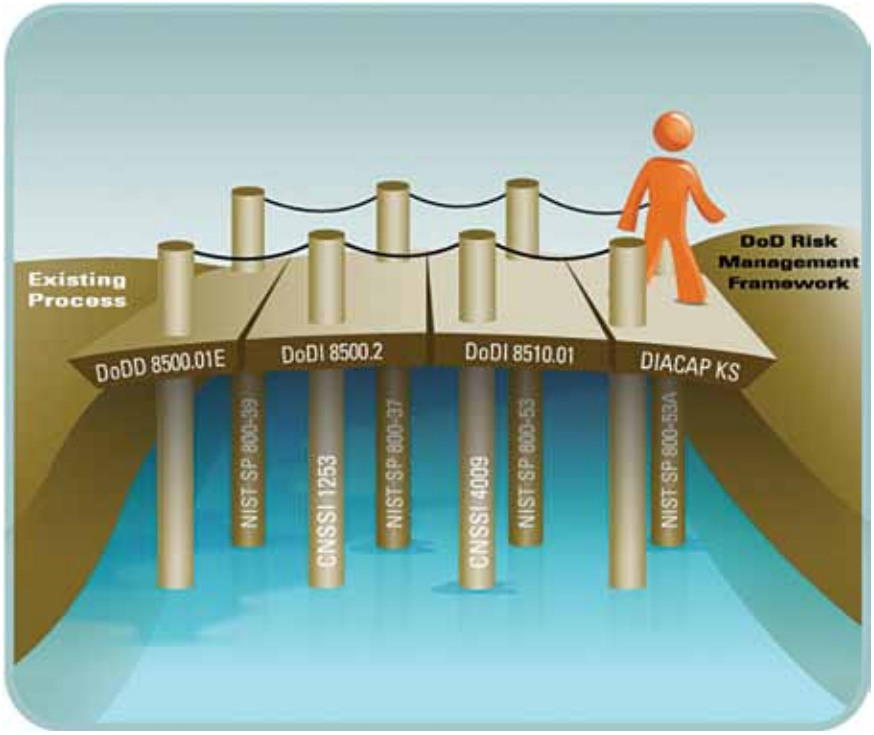
Command and Control.
Send and Receive intelligence.
Target the Enemy.
Pass Information to Higher Headquarters.
Build Trust and Establish Relationships.
Crisis Management.
Pass Assessment.

When you take a look at special operations, it is the global nature of SOF that makes us unique. It is not that the Army isn't global, clearly it is, and the Air Force, and the Marine Corps, but our 24/7 cycle, from command and control and operations, is not a linear process for us. It is happening every single minute of every single day across the entire globe. It is managed at smaller and smaller levels as you move from Afghanistan up to the SOCOM commander. These are the things I need your help in fixing. CHIPS

For the latest news and information about U.S. Special Operations Command, visit www.socom.mil/.

Certification & Accreditation Transformation

By Jennifer M. Ellett



While DoD continues to develop updates to the DoD 8500 series, it is clear there will be a number of changes for the DoD cybersecurity community — some significant.

Certification and accreditation (C&A) transformation is an initiative to align processes, terminology and frameworks for assessing information security risk across all federal agencies, including the defense and intelligence communities. This effort will provide efficiencies, standardization and support to reciprocity.

Reciprocity is an agreement among participating entities to accept each other's security assessment to reuse information security resources and accept each other's assessment and security posture to share information. This reduces rework and cycle time when deploying and receiving information systems from outside a single Department of Defense (DoD) component. Reciprocity between DoD components is based on transparency, uniform processes and a common understanding of expected outcomes.

The initial set of transformation goals, set by the DoD Chief Information Officer and the Director of National Intelligence (DNI) in 2007 is shown in Figure 1. The DoD worked with the Committee on National Security Systems (CNSS), DNI and the National Institute of Standards and Technology (NIST) in the years since to align guidance and policy across the federal government.

DoD is an active participant in updates to NIST and CNSS documents, including:

- NIST Special Publication 800-53 Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations," (http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf);
- NIST SP 800-37 Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems," (http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf); and
- CNSS Instruction No. 1253, "Security Categorization and Control Selection for National Security Systems" (www.cnss.gov/Assets/pdf/CNSSI-1253.pdf).

Now DoD is updating the following guidance to provide the DoD transformation to the federal framework:

- DoD Directive (DoDD) 8500.01E, "Information Assurance" (IA) (www.dtic.mil/whs/directives/corres/pdf/850001p.pdf);
- DoD Instruction (DoDI) 8500.2, "Information Assurance Implementation" (www.dtic.mil/whs/directives/corres/pdf/850002p.pdf); and

Figure 1. C&A Transformation Goals

1. Define a common set of trust (impact) levels and adopt and apply them across the intelligence community (IC) and DoD. Organizations will no longer use different levels with different names based on different criteria.
2. Adopt reciprocity as the norm, enabling organizations to accept the approvals issued by others without retesting or reviewing.
3. Define, document and adopt common security controls, using NIST Special Publication 800 53 as a baseline.
4. Adopt a common lexicon, using CNSS Instruction 4009 as a baseline, thereby providing DoD and the intelligence community a common language and common understanding.
5. Institute a senior risk executive function, which bases decisions on an "enterprise" view of risk considering all factors, including mission, IT, budget and security.
6. Incorporate information assurance into enterprise architectures and deliver IA as common enterprise services across the IC and DoD.
7. Enable a common process that incorporates security within the "life cycle" processes and eliminate security specific processes. The common process will be adaptable to various development environments.

- DoDI 8510.01, "DoD Information Assurance Certification and Accreditation Process" (DIACAP) (www.dtic.mil/whs/directives/corres/pdf/851001p.pdf).

While DoD continues to develop updates to the DoD 8500 series, it is clear there will be a number of changes for the DoD cybersecurity community — some significant. Specifically, the revised DoD 8500 series will include aligning DoD terminology with NIST terminology, expanding the scope of information technology that falls under the 8500 series, incorporating interim policy memorandums (e.g., directive type memorandum and DoD CIO memos), and changing the security control catalog and categorization process.

At the earliest, the DoD 8500 series updates are expected in spring 2012. Once the policy updates are released, DoD will transition over a period of years, similar to the DoD Information Assurance Certification and Accreditation Process (DIACAP) transition period, to the updated risk management processes and controls.

The change to DoDI 8510.01 will align risk management processes with NIST SP 800-37. It will also establish an overarching risk management process that will be applicable to all forms of DoD IT and information, including DoD information systems, platform IT, applications, IA components (e.g., IA products, crypto solutions, cross domain solutions, etc.) and DoD information on non-DoD information systems. This will increase the number of areas with a DoD-specified risk management process, but the framework and risk management process are not expected to have the same level of breadth and depth of review for each type of DoD IT and information.

The name of the DoD risk management process will change from DIACAP to the DoD Information Assurance Risk Management Framework, and the term C&A will be replaced with the NIST term assess and authorize. Other examples of DoD to NIST terminology changes are listed in Figure 2.

One of the most significant changes under C&A transformation will be the replacement of mission assurance category (MAC) and confidentiality level categorizations with the CNSS Instruction 1253 categorizations of low, medium and high risk for each security objective (confidentiality, integrity and availability). The resulting determination of high, medium or low risk for each of the three security objectives determines the initial baseline of IA controls.

A second significant change will be the removal of the DoD security control catalog from DoDI 8500.2. Instead, DoDI 8500.2 will point to NIST SP 800-53 for controls. This change is a result of NIST's collaboration with the intelligence community, DoD and the Committee on National Security Systems to ensure the NIST SP 800-53 control catalog included security controls that meet the requirements for national security systems.

DON program managers will find that with the new categorization and security control catalog there will be a significantly increased number of controls and enhanced controls with which systems must comply. The DON will mitigate the added workload demands of the increased requirements by providing a departmental prioritization of controls to assist program managers, engineers and security managers when building and assessing new systems, especially during this period of budget cuts.

Once the initial DoD security baseline is determined using the CNSS methodology and NIST controls, there may be additional overlays to apply. Overlays are structured additions or subtractions of security control to the established baseline reflecting an information type, or application of environmental or operational considerations regarding tactical systems, standalone systems, platform IT, cross domain solutions, personally identifiable information, or compliance with the Health Insurance Portability and Accountability Act, and other laws and requirements.

The overlays may also change the value in a control. For example, an electromagnetic frequency in an audit control might require too much tactical bandwidth so the value would be adjusted by an overlay. Not every system will require an overlay, but for a certain major category of systems or environ-

Figure 2. DoDI 8510.01 Roles and Acronyms Compared with NIST SP 800-37

DoDI 8510.01 DIACAP	NIST SP 800-37 Revision 1 Security Authorization
Heads of the DoD Components	Head of Agency (CEO)
Principal Accrediting Authority (PAA)	Risk Executive (Function)
Chief Information Officer (CIO)	Chief Information Officer (CIO)
No Equivalent	Information Owner/Steward
Senior Information Assurance Officer (SIAO)	Senior Information Security Officer (SISO)
Principal Accrediting Authority (PAA)	Authorizing Official (AO)
Designated Accrediting Authority (DAA)	
No Equivalent	Authorizing Official Designated Representative
Program Manager (PM)/Systems Manager (SM)	Common Control Provider
Program Manager (PM)/ Systems Manager (SM)	Information System Owner (ISO)
Information Assurance Manager (IAM)	Information System Security Officer (ISSO)
Information Assurance Officer (IAO)	
No Equivalent	Information Security Architect
Information Assurance Officer (IAO)	Information System Security Engineer (ISSE)
Certifying Authority (CA)	Security Control Assessor (SCA)
Validator	
User Representative (UR)	No Equivalent
Certification and Accreditation (C&A)	Assess and Authorize (A&A)

ments, such as personally identifiable information, cross domain or space based, an aligned overlay will be produced.

To support consistent security controls throughout DoD, a working group defined for the DoD enterprise *"organizationally defined"* values for the more than 250 NIST controls that require organizational specific values, such as password length, session time-out period and frequencies. The DON was a participant in this effort, which supports the DoD transition to the NIST 800-53 controls, further enables reciprocity and reduces variations for security control requirements in small organizations.

The DON has been an active participant in much of the DoD C&A transformation work, including developing the baselines, overlays, DoD enterprise specific values for security controls, and the NIST 800-53 to DoD 8500.2 controls crosswalk. These efforts are helping shape DoD C&A transformation and will ensure the DON's interests are represented and addressed in the DoD policies and processes. As a reminder, DON organizations should continue to follow current DoD instructions and directives for information assurance until they are replaced. This article is an introduction to the anticipated changes in DoD cybersecurity requirements as C&A transformation is implemented in the next few years.

To help organizations plan for the transition to the NIST 800-53 controls, the DON has completed a crosswalk of DoD 8500.2 controls to NIST 800-53 Revision 3 controls. The mapping is available from the DON CIO website: www.doncio.navy.mil/PolicyView.aspx?ID=1734. CHIPS

Jennifer M. Ellett is a Certified Information Systems Security Professional (CISSP) and a cybersecurity analyst on the DON CIO cybersecurity and critical infrastructure team.

NCTAMS LANT Embraces a New Online Training Program: "SHORE UNIQUE COURSEWARE"

Future looks bright for information systems technician training . . .

By Lt Chad A. Rogers

On Aug. 19, 2011, Naval Computer and Telecommunications Area Master Station Atlantic in Norfolk, Va., became the front-runner in a new online training program called, "Shore Unique Courseware." Working directly with the Center for Information Dominance (CID) in Pensacola, Fla., this courseware fills the knowledge gap for all new information systems technicians (IT) reporting to a NCTAMS from IT "A" School. The course significantly reduces the time required to train personnel on 30 intricate communications systems so they can begin working productively at their assigned duty station.

"It usually takes a new Sailor about 120 hours to complete even the most basic qualifications when reporting directly to the watch floor," said ITC (SW/IDW) Derrick Owens, leading chief petty officer for the NCTAMS LANT training division. "Now that time can be reduced by at least 50 percent, or more, allowing the new Sailor to report directly to the watch floor armed with the advanced knowledge of the communications systems they will be directly interacting with."

This reduction, in turn, means faster qualification times in a more efficient process allowing the "customer" in an afloat unit to receive quality technical support at all levels.

Using a facilitated Web-based curriculum tailored to four functional areas, such as satellite connectivity, messaging, network configurations and networking essentials, the Shore Unique curriculum provides 116 hours of instruction through 99 lessons. ITSN Dylan Carter, one of the first students in the program, said, "The most valuable part of the training was being able to have the material explained in the module and then see how it actually works on the watch floor. It made learning and qualifying on the equipment that much easier."

Using the abundance of navigational tools available in the courseware program also helps the students to perform multiple procedures in a simulated software environment. The Shore Unique Courseware is also followed up through instructor-led activities and on-the-job training, which involves participation by the student in a life-like set of complex cues and performance-based responses.

Since many systems and processes are unique to the NCTAMS, the Shore Unique Courseware utilizes real-time working documents to post and share correctable discrepancies on the system's technical or functional capabilities. Combined with assessment metrics and strategies, such as pre- and post tests with hands-on interaction between the student, the facilitator, and the technical support from CID, the Shore Unique curriculum can continue to evolve to the needs of the NCTAMS and the warfighter at sea.

"Before most of our Sailors would go straight to the watch floor before they even went through command indoctrination," said Lt. Chad Rogers, training division officer for the operations department. "Now, we can take them as soon as they get here and provide them the opportunity to go through indoctrination, get Electronic Key Management System qualified, and qualify in watch floor fundamentals before even being placed in their work space. Combine that with the multitude of courses available to them in Shore Unique, and our return on investment is invaluable not only to the command, but the Sailor standing watch out on the deckplates at sea!"

ITSA Erik Tellin and ITSA Alexandra Scott, two NCTAMS LANT students who had the rare opportunity to be the first to go through the two-week Shore Unique pilot program, said they look forward to being of great value to their divisions and look forward to becoming the "go-to" person in any NCTAMS LANT communications system.

Thanks to the interactive laboratories in each module, students can practice what they have learned on virtual equipment that is exactly the same as what they will use when they move to the watch floor.

The pilot program successfully kicked off at NCTAMS LANT and will soon be used at other communications facilities throughout the fleet. The future looks even brighter for ITs because NCTAMS LANT intends to bring shipboard personnel into the virtual world of Shore Unique Courseware. CHIPS

Lt. Chad A. Rogers is the training division officer in the NCTAMS LANT operations department.

First row bottom: Shore Unique Courseware students: ITSA Erik Tellin, ITSN Dylan Carter, IT3 Kirstie Trangata and ITSA Alexandra Scott

Second row top: Team Oscar/ N37 training division: Lt. Chad Rogers, IT1 Bennie Askew, IT2(SW) Gilberto Villarreal, IT3 Chastdy Lewis and IT2 Charles Robison.

Q&A with Rear Adm. Gretchen S. Herbert Commander, Navy Cyber Forces

Rear Adm. Gretchen S. Herbert

Among her varied assignments, Rear Adm. Gretchen S. Herbert, has been commanding officer of Naval Computer and Telecommunications Station Washington; branch head, Naval Networks for OPNAV N6; and assistant chief of Naval Operations for the Next Generation Enterprise Network. She also served as director of the Communications, Networks and Chief Information Officer (CIO) Division on the staff of the Deputy Chief of Naval Operations for Information Dominance.

Fleet assignments include combat systems officer embarked in USS George Washington (CVN 73), where she deployed to the Arabian Gulf in support of Operations Southern Watch, Enduring Freedom and Iraqi Freedom; and assistant chief of staff for Communications and Information Systems (N6) to commander, Carrier Strike Group 7 embarked in USS Ronald Reagan (CVN 76), where she deployed to the Western Pacific and Arabian Gulf with the Ronald Reagan Strike Group.

In June, 2011, Herbert assumed command of Navy Cyber Forces at Joint Expeditionary Base Little Creek-Fort Story, Virginia Beach, Va.

Navy Cyber Forces (CYBERFOR), as delegated by Commander, U.S. Fleet Forces, is the global C5I type commander responsible to man, train and equip all C5I forces afloat and ashore to generate required levels of current and future cyber force readiness. With a headquarters staff of nearly 600 located at Joint Expeditionary Base Little Creek-Fort Story, CYBERFOR provides ready forces and equipment in cryptology/signals intelligence, cyber, electronic warfare, information operations, intelligence, networks and space.

Rear Adm. Herbert responded to CHIPS questions about CYBERFOR's mission in writing in September.

CHIPS: Can you discuss NAVCYBERFOR's role as the global C5I type commander (TYCOM)?

Herbert: Similar to the role of the Navy's platform TYCOMs (surface, submarine, aviation), the role of Navy Cyber Forces is to adequately man, train, equip and assess the readiness of fleet C5I forces — East Coast, West Coast, Forward Deployed Naval Forces (FDNF) and shore C4I commands. Navy Cyber Forces professionals ensure operational readiness and mission assurance throughout the cyberspace domain.

More fundamentally, NAVCYBERFOR's type commander role is to assess, train and certify cyber forces for basic phase and integrated training, ensuring that our Sailors and systems are fully ready for joint and coalition operations. We work very closely with the platform TYCOMs to ensure that the numbered fleet commanders have the required capabilities and trained cyber forces to meet all missions.

Our networks, sensors, combat systems, intelligence and communications systems all rely on unfettered access to the electromagnetic spectrum and the Global Information Grid. Mission success requires us to have information dominance — manifested in our freedom to operate, maneuver and enable decision superiority in and through cyberspace. Our cyber forces need to be trained to provide the right level of expertise across the full spectrum of operations from humanitarian assistance/disaster relief through major combat operations.

The Navy's cyber workforce is also known as the Information Dominance Corps. The IDC is comprised of nearly 50,000 professionals — officers, enlisted and civilians — serving as specialists in information-centric fields, including intelligence, information warfare, information technology, oceanography and space. Navy Cyber Forces works to build, train and maintain a strong IDC with unique skills and capabilities for delivering innovative solutions, expanding decision space, delivering kinetic and non-kinetic effects, and successfully operating and winning in the cyberspace domain.

CHIPS: How would you assess force readiness in cyber operations, and what is Navy Cyber Forces doing to improve force readiness?

Herbert: On a monthly basis the Navy Cyber Forces, in conjunction with Fleet Cyber Command (FCC), assesses the readiness of the afloat/ashore C5I units. The review starts with the commander's assessment of readiness and continues with a review of resource pillars — personnel, equipment, supply, training, ordnance and facilities, or PESTOF. Any shortfalls identified by the unit commander or identified in the PESTOF pillars are addressed and mitigated by NAVCYBERFOR and FCC personnel or, for longer range solutions, addressed in the POM (program objective memorandum) budget process. Specific areas of focus include the following.

- **Cyber Workforce**

Provisioning a cyber workforce capable of addressing the challenges of information-centric operations is a top priority of NAVCYBERFOR. We work very closely with stakeholders throughout the Navy — including the office of the Chief of Naval Operations (OPNAV), both in the Manpower, Personnel, Training and Education (MPT&E OPNAV N1)) organization and Deputy CNO for Information Dominance (N2/N6). Our manpower team also collaborates with U.S. Fleet Cyber Command/U.S. 10th Fleet at Fort Meade, Md., the Bureau of Naval Personnel in Millington, Tenn., Naval Education and Training Command in Pensacola, Fla., and our two primary schoolhouses: Center for Information Dominance in Pensacola, and the Center for Naval Intelligence, Dam Neck, Va.

Navy Cyber Forces also incorporates fleet feedback on shortfalls and gaps in IDC manning, and periodically conducts Human Performance Readiness Reviews (HPRRs) to ensure that fleet Sailors receive the training and education required to meet current and emerging mission requirements.

Recently, Navy Cyber Forces was designated as the executive agent to help lead and execute a Navywide cyber workforce zero-based review (ZBR). Led by a task force commissioned through OPNAV N2/N6, the ZBR will baseline our current cyber work and workforce, and identify gaps in skill sets and positions. The results of this study will assist the Navy in making strategic decisions on how to align limited resources and talent capacity, by putting our critical skill sets where they are needed most.

• Training our Fleet

NAVCYBERFOR is responsible for C5I readiness assessments of Navy ships and submarines, as well as multiple IDC-related shore commands (i.e., such as the Naval Computer and Telecommunications Area Master Stations, Navy Information Operations Commands, Fleet Intelligence Detachments (FID) and Fleet Intelligence Adaptive Force (FIAF)).

In order to quantify C5I material readiness and cyber forces readiness for tasking, NAVCYBERFOR solicits and incorporates fleet feedback. We analyze C5I performance metrics from returning strike groups and independent deployers, and we routinely conduct assist visits to provide C4I training and assistance. We take our fleet customers through a certifying process to prepare them for the integrated training phase, and certify ashore units for basic phase operations. Tenth Fleet, in turn, certifies the units for continuous operations. Together, we monitor all units throughout the Fleet Response Training Plan (afloat units) and Cyber Shore Training Plan (ashore units).

• Electronic Warfare

In our role as the Fleet Electronic Warfare Center, NAVCYBERFOR is leading a critical EW readiness improvement campaign to build a robust and relevant fleet EW capability. Specific efforts include establishing EW as a primary mission area, breaking out EW visibility in DRRS-N (Defense Readiness Reporting System-Navy), conducting Tactics Seminars at the Surface Warfare Officers School (SWOS), performing technical assist visits for surface units, and establishing an electronic warfare officer training continuum.

Additionally, Navy Cyber Forces and the Navy Marine Corps Spectrum Center have been leading efforts to protect Navy's operational equities in [the] National Broadband Initiative and associated efforts to relocate operating radio frequencies for critical Navy combat systems. SMEs (subject matter experts) from NAVCYBERFOR also work to identify and preserve Navy frequency assignments for Aegis missile defense and CVN (carrier) air traffic control radars.

• Network Warfare

In coordination with the platform TYCOMs and Fleet Cyber Command/10th Fleet, and the Defense Information Systems Agency (DISA), we are assessing, training, inspecting and certifying networks of afloat and ashore units. Navy Cyber Forces has two distinct roles in this effort. First, as the global C5I type commander, we are assessing and training units in conjunction with the platform type commanders to ensure afloat units are certified in the basic phase of training and can advance to integrated training. With Fleet Cyber Command/10th Fleet and DISA, we are helping prepare units for the Command Security Inspection and Certification Program (CSICP). This inspection program measures the effectiveness of our information technology programs of record and their integration with the afloat and ashore units they support.

Navy Cyber Forces is also leading a performance review of Navy afloat software applications. The fleet functional area manager (FAM) effort was established to review all afloat software applications for performance and accreditation issues, fixing those apps that are underperforming or removing them from the afloat inventory. We've also been working with PEO C4I to employ their Sailor 2.1 tool (https://sailor.nmci.navy.mill) to provide updated information on authorized apps and software patching procedures to improve application functionality and security.

The fleet FAM is a partnership of stakeholders from across the fleet, platform TYCOMS, systems commands and resource sponsors. We each have equities and responsibilities in ensuring that the systems and products that we are employing on our networks are secure, interoperable and are value added to the fleet.

• Intelligence

Navy Cyber Forces continues to receive positive feedback from the tactical commanders regarding the increased readiness of our Fleet Intelligence Detachments and Fleet Intelligence Adaptive Force. FID personnel are receiving comprehensive training at two Centers of Excellence prior to deployments. The FID at the Office of Naval Intelligence, Nimitz Operational Intelligence Center, hosts "all-source" intelligence officers and intelligence specialists (IS) trained in imagery interpretation, while the FID at Naval Strike and Air Warfare Center (NSAWC) hosts IS strike intelligence analysts.

FID augmentation is event-focused and driven by specific skill sets for validated operational requirements levied by numbered fleet, carrier strike group (CSG) and amphibious readiness group (ARG) commanders. FIDs are designed to augment aircraft carriers and large deck amphibious ships. They were created to provide better trained, more operationally ready intelligence professionals to the fleet in the critical, high demand skill areas of all-source operational intelligence, imagery interpretation and strike support.

The FID concept was developed after examining lessons learned from other Navy communities that deploy in detachments or provide direct support ship riders. This DCNO for Information Dominance approved concept called for transitioning a portion of ship's company intelligence billets, with the most highly perishable skill sets, from aircraft carriers and large deck amphibious ships (CVN/LHA/LHDs), to intelligence centers, where their unique skill sets were tested and employed more routinely.

The remaining ship's force intelligence personnel would maintain and sustain organic intel systems and provide robust intel support to the combat systems training teams.

One of the unique attributes of the FID model is that it is designed to produce teams that will stay together from their first embarkation during basic phase to the final at-sea event in the deployment/sustainment phase of the Fleet Response Training Plan (FRTP).

When not embarked, FID personnel provide remote real-time intelligence support to deployed operating forces, receive sustainment training/qualifications and share lessons learned.

The FIAF detachments are collocated at the maritime operation centers (MOC) at the six numbered fleets and Pacific Fleet to meet new fleet and operational requirements with rapidly adaptive intelligence capability. The FIAF is designed to fill validated combatant command (COCOM) information assurance (IA) requirements, support Navy Cyber Forces and numbered fleet missions, maintain fleet intelligence readiness throughout the FRTP, and enable Navy operations by supporting MOC operations.

The FIAF constitutes the "flexible" portion of the intelligence manpower plan, giving Navy Cyber Forces the ability to rapidly redistribute resources (from MOC to MOC) and address in theater crisis/emergent intelligence demand signals for missions, such as maritime interception operations intelligence exploitation teams (MIO-IET), small tactical unmanned aerial system (STUAS) detachments, nuclear-powered cruise missile submarines (SSGN) detachments, and similar requirements or priorities as identified by operational commanders. The long-term FIAF approach is to build a flexible capability that will give Navy Intelligence the ability to respond to validated current and emergent IA requirements, provide forward MOCs on-site expertise to increase intelligence readiness of deploying naval forces, and enhance enterprise-wide intelligence readiness by creating the capability to do remote support from multiple locations.

The FID and FIAF are maturing and providing a better prepared Sailor to the operational and tactical commanders. To measure the effectiveness of these new models, Navy Cyber Forces will be hosting an Augmentation Planning Board this fall to evaluate the current state of the FID and FIAF, identify any shortfalls, and determine what course adjustments are needed to better position the force to meet current/future operational demands.

CHIPS: In June, the Defense Department released its first strategy for operating in cyberspace in the fight to protect the nation from potentially devastating network attacks. This is just one of the several building blocks, such as the stand up of U.S. Cyber Command, designed to allow U.S. military forces to operate in cyberspace and protect critical national infrastructure. Does the continuing national discussion regarding how the military should operate in cyberspace affect CYBERFOR's man, train, equip role?

Herbert: Absolutely. One of the core tenets of the new strategy is that we need to treat cyberspace as a domain, and with that comes all of the associated responsibilities of defining how we operate, train and equip our forces to prevail and win in this domain. There is increased emphasis on the development and certification of relevant, reliable and enduring cyberspace and information dominance skills at the individual and unit level, through the operational, and ultimately, strategic level of war.

As we continue to develop metrics and Navy mission essential tasks to evaluate our warfighting readiness and effectiveness, we're also learning that we may need to incorporate variations in training and certification methods. Existing structures, boards and processes are not necessarily nimble, flexible or responsive enough to meet the fast-paced requirements and operational demands of the cyberspace domain. We need to work through those issues to ensure we can deliver the right personnel, with the right skill sets and the right tools to do the job, before we're "in extremis" in cyberspace-related mission areas.

Another area of focus is on developing a holistic continuum of training and education for not only the immediate cyber workforce, but for anyone who works and operates in the domain — and that includes just about everyone in the Navy. In this domain, more so than any other, it's vitally important that the "customer" understands the inherent risks, threats and vulnerabilities of operating in a battlespace that is not separate and distinct from our adversaries' battlespace — and that the cost of entry into this domain is unprohibitively low.

The national discussion about how the military will operate in cyberspace may also inform resource allocation decisions which, in turn, would impact personnel and equipment decisions that will source the fleet. Additionally, the national discussion includes issues, such as how the law of armed conflict applies to military actions in cyberspace. Both legal and policy decisions will be made that will clarify our understanding of the law and inform the development of various rules of engagement. Ultimately, the policies and rules developed at the national and service levels will influence training provided to operators.

CHIPS: What are your thoughts about the future of Navy cyber?

Herbert: In light of the changing nature of operations in the information age, there is every reason to believe that the future of naval warfare will place increasing demands and expectations on the Information Dominance Corps. NAVCYBERFOR will be "front and center" in addressing those demands and meeting those expectations.

As we look at the emerging challenges and increasing complexity of modern warfare, it is clear that our Navy needs now, more than ever, a dedicated, technically skilled, engaged and innovative total workforce to fill the ranks of our cyber team. While these are challenging times, in terms of emerging mission requirements, combating blurry but persistent threat vectors and managing DoD-wide budgetary constraints, this is also an incredible opportunity to redefine the way we man, train, equip and sustain our Navy cyber workforce, now and in the future.

Much of our mission success will be driven by our ability to draw from the best of America — and in showcasing the Navy as an employer that values the talent, creativity, enthusiasm and ambitions of our nation's youth. Each of us has an incredibly important role in mentoring others and raising awareness of the great opportunities available in the Navy's Information Dominance Corps.

CHIPS: Is there anything you would like to add?

Herbert: I would just like to say that it is a profound honor to lead the exceptionally talented and dedicated professionals at Navy Cyber Forces. They inspire me each day, and I know that our Navy is stronger, and our nation safer, because of their dedication, focus and commitment to mission success. CHIPS

Navy Cyber Forces
www.cyberfor.navy.mil/.

Supervisor Sends PII Without Encrypting Email

By Steve Muck and Steve Daughety

The following is a recently reported personally identifiable information (PII) data breach involving a Department of the Navy support contractor who improperly handled PII. Incidents such as this will be reported in CHIPS magazine to increase PII awareness. Names have been changed or omitted, but details are factual and based on reports sent to the DON Chief Information Officer Privacy Office.

The Incident

A supervisor sent an unencrypted email containing full name, Social Security number, home address and phone number of 37 active duty personnel to dot-mil user accounts within a single command. All recipients had a "need to know" and routinely receive email like this to perform their assigned duties. The email was not digitally signed and did not carry the "For Official Use Only (FOUO)" privacy warning.

Actions Taken

Recipients were immediately contacted and asked to delete the email and all file copies and to reply with an email confirmation. The DON CIO Privacy Office was contacted a short time after this action was taken and was advised that all recipients had taken the appropriate action.

The DON CIO Privacy Office advised the accountable command/unit that because the email remained within the Defense Department firewall, had been sent to only those with a need to know, and the email was deleted from all files immediately after transmission, that the incident did not constitute a "high risk" breach. Accordingly, the DON CIO determined that notifying the personnel whose SSNs and other PII were emailed, without the required PII safeguards, was not required.

While this breach was considered low risk to affected personnel, it could easily have been determined high risk if:

- The email was sent to individuals who did not have a need to know; or
- The email was sent to a commercial account; or
- The email was stored on a personal computer or a personal removable storage device.

Lessons Learned

- All PII sent by email must be digitally signed and encrypted.
- When mistakes are made that result in theft, loss or compromise of PII, prompt corrective action can mitigate the potential risk of harm to affected personnel.
- Marking documents containing PII can be a simple but effective breach preventive measure.
- All attachments should be opened and read completely before email transmission to ensure there is no unintended PII contained within the document.

Encryption Guidelines

Guidelines for email encryption were issued in a naval message from the DON CIO: DTG 032009Z OCT 08, "DON Policy Updates for Personal Electronic Devices Security and Application of Email Signature and Encryption." This message can be found on the DON CIO website at www.doncio.navy.mil/PolicyView.aspx?ID=782. CHIPS

Steve Muck is the privacy lead for the Department of the Navy Chief Information Officer.

Steve Daughety is a privacy analyst supporting the DON CIO.

Q&A with Rear Adm. Patick H. Brady
Commander, Space and Naval Warfare Systems Command

Rear Adm. Patick H. Brady

Since the Chief of Naval operations combined the Office of the Director of Naval Intelligence (N2) and the Office of the Deputy Chief of Naval Operations for Communication Networks (N6), as well as other information-related elements from the N3 and N8 staffs, to form the Deputy Chief of Naval Operations for Information (N2/N6) in 2009, the Space and Naval Warfare Systems Command has been in lockstep with N2/N6 to elevate cyber into a Navy warfighting domain, much like the land, sea, air and space domains.

To this end, SPAWAR Commander Rear Adm. Patrick H. Brady leads a total force of approximately 8,000 engineering and acquisition professionals across the headquarters, System Centers Atlantic and Pacific and Program Executive Offices (PEO) for C4I, Enterprise Information Systems and Space Systems.

Through its engineering and acquisition excellence, SPAWAR delivers a portfolio of command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) capabilities to fleet customers. The command is also a key player in the Department of the Navy's Information Technology/ Cyberspace Efficiency Initiatives and Realignment Tasking mandate for the department to reduce its IT budget by 25 percent.

CHIPS asked Rear Adm. Brady to discuss SPAWAR's contributions to information dominance and enterprise IT efficiencies, and he responded in writing in late September — just before the stand-up of the Fleet Readiness Directorate Oct. 1.

CHIPS: Can you discuss the Fleet Readiness Directorate, an initiative for SPAWAR to provide the fleet with a flag focal point for fleet issues? I read on your blog that Assistant Secretary of the Navy for Research, Development and Acquisition Sean J. Stackley is pleased with the structure and capability SPAWAR will be able to provide in response to his tasking for "Information Dominance In-Service Sustainment/Coordination."

Brady: SPAWAR's Fleet Readiness Directorate (FRD) will be established Oct. 1 in response to Secretary Stackley's task to develop an in-service support organization within SPAWAR modeled after those in our partner systems commands. Our goal was to develop an organization that was solely focused on installation and sustainment support for our fleet's information dominance systems. To develop the FRD structure, we relied on several teams to analyze all the details of organization, personnel and mission requirements. As no new personnel or resources would be available to stand-up the FRD, we had to pay particular attention to how we could best arrange existing resources and expertise.

One of our major preparatory tasks was to evaluate all the systems that were being managed within the PEOs and to identify those systems that were at a sufficient maturity to be candidates for transition to the FRD. In the end, we identified 31 programs for transition Oct. 1 concurrent with the stand-up. In the future, additional programs will be evaluated for transition as they reach the appropriate stage of development within the product life cycle.

With the stand-up of the FRD, we are structured to provide that single focal point for installation and sustainment across SPAWAR and our intent is to continue to improve support to the fleet in these areas. The FRD will maintain strong coordination and mutual support with the PEOs, but now the program offices can provide increased focus on their acquisition activities. We see the FRD as a great opportunity across SPAWAR and the Navy.

CHIPS: How do you see establishment of the FRD affecting the typical fleet command and Sailor?

Brady: The central benefit to the fleet that flows throughout the FRD concept is consolidated accountability of SPAWAR systems installation and sustainment. The single focus nature of the FRD provides the fleet a common entry point to address SPAWAR system issues. By having in-service support reside under a single flag officer, Rear Adm. Chuck Rainey, it improves our ability to maintain a regular drumbeat with fleet leadership on issues ranging from install planning — to system maintenance processes and CASREP (casualty report) management. Ultimately, these efforts will help us better support fleet readiness.

CHIPS: Assistant Secretary Stackley issued a number of acquisition taskers. The guidance issued July 19, "Increased Use of Small Business Concerns," provides specific guidance to encourage use of small business in contracting because small businesses can provide the agility, innovation and efficiencies that are a win-win for government and industry. Can you provide an update?

Brady: Secretary Stackley's memo is focused on increasing the use of small businesses in Navy contracting processes. In my experience, small businesses, not only bring agility and innovation, but also help support more competition in our contracting. At SPAWAR, approximately 81 percent of all our contracts in fiscal year 2010 were competitively awarded, and small business obligations were an important contributor.

For fiscal year 2011, our goal for SPAWAR was 20 percent of eligible obligations for small business, and as of mid-September we exceeded that target. We also made strong progress this year in other small business goals, exceeding three of four socioeconomic specific targets.

In his memorandum, Secretary Stackley highlighted a number of specifics areas where we can focus our attention to con-

tinue to increase small business opportunities and participation in the acquisition process. Just one example was a review of the accuracy, currency and completeness of Web access for the future procurements forecast. In parallel with this action, SPAWAR is pursuing an additional, more qualitative and detailed approach to forecast future small business procurement opportunities that should not only identify more opportunities, but also help provide as much lead time as possible for their planning.

Active engagement with the small business community continues to be one of our best tools to increase awareness of business opportunities at SPAWAR, which ultimately increases the number of proposals, competition and small business utilization within our contracting.

Matchmaking sessions between program offices and providers promote that awareness of the new capabilities available in the marketplace that can support technology insertions or lead to small business innovation research or related initiatives. Our outreach activities to the small business community connect us to leading-edge technologies and processes that are critical for much of the work we do at SPAWAR.

CHIPS: Deputy Chief of Naval Operations for Information Dominance Vice Adm. Kendall Card said that SPAWAR is directly involved in the "Navy IT Way Ahead" strategy. Can you talk about what SPAWAR is doing in support of this effort?

Brady: Consolidating IT procurement under a single authority is a very important step toward maximizing efficient and effective delivery of the volume of information systems the Navy needs to conduct its missions. The DON Information Technology Expenditure Approval Authorities memorandum [issued by the DON Chief Information Officer July 19, 2011; available on the DON CIO website: www.doncio.navy.mil] highlighted this need for IT purchases greater than $1 million. There are also opportunities to make improvements to our IT procurements that are less than this amount.

SPAWAR is supporting the evaluation of all these opportunities. Moving IT procurement under the cognizance of a single authority can ease oversight and generally support better programming, planning and budgeting. A single purchasing authority will also achieve greater economies of scale for IT purchases and yield cost savings and operational efficiencies while limiting impact on staff and resources. These are great opportunities for the Navy, and SPAWAR looks forward to continuing our support to their development.

CHIPS: SPAWAR is also playing a pivotal role in the DON's Data Center Consolidation Policy, issued by the DON Chief Information Officer July 20. How is SPAWAR providing assistance in this regard? What other enterprise information technology efficiencies is SPAWAR executing?

Brady: SPAWAR was tasked by Secretary Stackley to take the lead and coordinate closely with PEO Enterprise Information Systems, the resource sponsors and DON CIO to build a plan that addresses architecture, resources, schedule, basis of estimates, technical feasibility, risks/opportunities, contract strategy and governance/responsibilities for data center consolidation.

This effort will look at the "gold standard" data centers we have in place today. In other words, those centers that meet or exceed all security and operational continuity requirements, and that reduce our cost footprint through consolidation into such facilities. Today, we have over 100 data centers serving the Navy, each with their own management structure, monitoring tools, facility costs and disaster response plan. As a Navy, we can do this more efficiently.

SPAWAR engineers have done this sort of work before. In the last five years we've transitioned a number of applications out of existing data centers and into SPAWAR hosting facilities. In work for the Commander of the Navy Reserve Force, we realized over $31 million of life cycle savings, and a savings to the Reserve force of over $6 million that would have been spent on contractor services and license fees.

We'll work with the other Echelon 2 commands in the Navy to help them choose the best alternatives for data centers and conduct the transitions identified that make sense and support an overall goal to reduce costs to the Navy. We're standing up a task force headed by Rob Wolborsky, our science and technology national competency lead, along with an engineering team, to work this important initiative.

CHIPS: The Consolidated Afloat Networks and Enterprise Services (CANES) program achieved a significant engineering milestone in July with the completion of critical design reviews (CDR) for the two competing CANES systems in development by Lockheed Martin Mission Systems and Sensors and Northrop Grumman Information Systems. CANES is a significant part of the Navy's enterprise network strategy. Can you discuss the strategy for implementing CANES?

Brady: CANES is a high visibility program that is of keen interest because of how it will modernize and standardize the tactical afloat system across the Navy.

CANES is the Navy response for providing operationally effective and cost-efficient networks for ships, submarines and maritime operations centers. CANES core tenets are to reduce network total ownership costs and increase operational relevance by employing constant competition, open architecture, government-owned data rights and an executable technology refresh framework that targets affordability.

The completion of [the] CDR marks a significant milestone in this phase of the program. At this point, we validated the design baseline for both developers, which was the last primary gating function leading to down-select. At downselect, the government will choose the winning design of the two developers and proceed to limited deployment with that design only. It is also important to note that at downselect the government will have no less than government purpose rights to the winning design.

I mentioned previously the importance of maximizing competition within our programs, and CANES is a solid example of this approach. There is competitive procurement for both the current EMD (engineering and manufacturing development) phase and the LD (limited deployment) phase. There will also be full and open competition for full deployment of the production units and engineering support services contracts.

The current schedule has the program down-selecting to a single CANES design in 2012. It is important for the CANES program to achieve its first installation due to the increasing costs of sustaining our existing systems.

The Chief of Naval Operations issued OPNAVNOTE 5400 May 31, 2011, which designates SPAWAR as the Navy's "Information Dominance Systems Command."

SPAWAR will provide dominance in the fields of intelligence, surveillance, and reconnaissance; cyber warfare; command and control; information and knowledge management; and meteorology and oceanography (METOC).

SPAWAR projects and programs will align with Office of the Chief of Naval Operations requirements and the operational needs of U.S. Fleet Cyber Command and l0th Fleet and Commander, Naval Meteorology and Oceanography Command. The fleet is the end user of SPAWAR products.

SPAWAR will work closely with the fleet, systems commands, and Navy partners to seamlessly and effectively deliver capability by acquiring and/or integrating sensors, communications, weapons, information and control systems for existing and future ships, aircraft, submarines, and unmanned systems.

To achieve this mission, SPAWAR will:

a. Support Assistant Secretary of the Navy (Research, Development and Acquisition) as the Navy Service acquisition executive;

b. Ensure the success of assigned Navy and Marine Corps programs of record;

c. Support affiliated program executive offices (PEOs) management of life cycle cost, performance, and schedule for assigned programs;

d. Balance current and future fleet readiness in the most efficient and effective manner to align with Chief of Naval Operations objectives;

e. Provide service within resource boundaries to Department of Defense; Department of Homeland Security; Joint and Coalition Command; control, communications, computers, intelligence, surveillance, and reconnaissance projects; and METOC projects in support of affiliated PEOs and those other agencies;

f. Serve as the technical authority and operational safety and assurance certification authority for assigned areas of responsibility; and

g. Provide in-service support for affiliated PEO programs as necessary.

CHIPS: Is there anything else you would like to tell CHIPS readers?

Brady: Our overarching objectives are to build an affordable information dominance capability for the fleet: maintain, modernize and integrate the existing fleet; and develop the premier information dominance acquisition workforce.

All the initiatives we discussed — especially the establishment of the Fleet Readiness Directorate and systems and acquisition process improvements — are key to accomplishing these objectives and will help us make the Navy's information dominance vision a reality. CHIPS

ASN RDA policy and guidance is available at https://acquisition.navy.mil/. Follow SPAWAR on Twitter and Facebook at http://twitter.com/SPAWARHQ; www.facebook.com/spaceandnavalwarfaresystemscommand.

ONR Exhibits Top Weapon Technologies at Modern Day Marine

From Office of Naval Research Corporate Communications

The Office of Naval Research (ONR) opened its Modern Day Marine Expo Sept. 27, demonstrating the very latest in technologies aimed at providing specialized capabilities for the Marine Corps. Cosponsored by the Marine Corps Systems Command, which acquires and sustains weapon systems and gear for Marines, the annual event in Quantico, Va., serves as the corps' premier equipment, systems, services and technology exposition.

"ONR's participation at Modern Day Marine is an important two-way stimulator for creative thought, discussions of ideas and situational awareness," said Dan Simons, who leads the fires thrust team, part of ONR's expeditionary maneuver warfare & combating terrorism department.

Modern Day Marine is billed as the world's largest military trade show directed at increasing capabilities for expeditionary forces. The exhibit presents thousands of attendees — including senior leaders, scientists and engineers from government and industry — with opportunities to directly interact with U.S. Marines and acquisition personnel responsible for equipping the corps. The following technologies were featured.

- Army Advanced Weapons Sight Technology – next-generation weapon sights for enhanced situational awareness, threat detection, range performance and target engagement.
- Awareness Lightweight Engagements and Remote Targeting – highly transparent polymer materials used for lightweight, high resolution military optical components.
- Azimuth and Inertial Microelectromechanical Systems (MEMS) – a handheld, highly accurate alternative to the Digital Magnetic Compass.
- High-Performance Alloys for Weapons Applications – a super alloy designed to withstand the high-temperature, high-pressure, erosive environments found inside machine gun barrels.
- Integrated Day-Night Sight Technology – weapon sights that discern friendly forces from hostile forces and noncombatants in environments ranging from daylight to darkest night and obscurants.
- Marksmanship and Small Arms Trainer – an interactive training simulation that documents individual task performance in real time and is suitable for both live-fire and virtual environments.
- MEMS-Based Fuze for Flight-Controlled Mortar – a newly developed fuze that is much smaller than the conventional M734A1 mortar fuze.
- MEMS Ignition Safety Device – a compact, low energy, low-cost igniter that actuates locks and provides a barrier to achieve "safe" and "arm" positions for rockets.
- Precision Universal Mortar Attack – a semi-active laser and GPS guidance-based system that offers precision, complex terrain insertion capability for mortars.
- Small-Caliber Caseless Ammunition – new propellant technology that eliminates the need for a cartridge case. CHIPS

SPAWAR's SAILOR 2.1 Now Available on a Navy Ship Near You

Online "Tech Tube" enhances fleet readiness and Sailors' skills

By Nicole Collins

In response to overwhelming fleet requirements and positive user feedback of the SPAWAR Acquisition Integrated Logistics Online Repository (SAILOR) 2.0, the Space and Naval Warfare Systems Command (SPAWAR) launched SAILOR version 2.1 Sept. 15.

Developed in collaboration with Program Executive Office Command, Control, Communications, Computers and Intelligence, the updated tool provides additional product features in anticipation of fleet demands for expanding the number of systems covered by this powerful tool.

"I see critical value with SAILOR in terms of a direct technical knowledge medium between the fleet and subject matter experts ashore," said Lt. Cmdr. Donald Wilson, force combat systems information officer from Commander, Naval Air Forces. "Having the documentation readily available at the click of a mouse allows Sailors to properly configure, operate and maintain equipment and software; in turn, you get improved system performance and support which equals increased fleet C4I readiness."

SAILOR was developed in November 2010 as an easy-to-use tool to assist the fleet in accessing current hardware and software configurations, as well as product support documents. SAILOR allows the fleet to exchange technical knowledge with subject matter experts through blogs and a technical exchange forum which ultimately increases transparency and decreases response time.

"Not only will the fleet have access to critical documents and configuration files for their C4I products, they'll have 'how-to' videos to help troubleshoot their equipment," said Margaret Fellenbaum, SPAWAR's technical director for product data management.

Originally designed for Sailors between ages 18 to 30, users can now navigate a comprehensive interface that includes video streaming capabilities, convenient document aggregation, a fleet feedback mechanism, consolidated navigation menus and enhanced user support areas.

"Bandwidth is limited out in the fleet. SAILOR 2.1 loads significantly faster and is more responsive," said Information Systems Technician First Class Justin Roysdon from the SPAWAR C4I help desk.

SAILOR 2.1 will offer the fleet an array of features such as "tech tube," updated navigation, an interface display and media center. Tech tube, a series of how-to videos, was created based on SPAWAR Commander Rear Adm. Patrick Brady's recommendation to display, track and report video tutorials to the fleet in an effort to proactively counter critical fleet issues, like readiness and technical support.

"SAILOR has become an essential tool for the fleet to enhance C4I readiness, and ultimately, the Navy's information dominance capabilities," Brady said. "SPAWAR continues to strive to meet fleet requirements, and SAILOR 2.1 provides additional features that the fleet has been asking for."

With an increasing response to the promotion of fleet readiness and ensuring warfighter efficiency, requirements are rapidly increasing for a faster, more efficient means of accessing online training, technical manuals and how-to videos for Sailors on board a Navy ship.

With a focus on fiscal efficiency, SPAWAR took the reins and pursued a more cost effective approach in quickly distributing logistics, training and instructional material to the fleet with version 2.1.

Trends have also shown systems leaning toward central online distribution points to provide an on-demand environment, where data can be instantly accessed without the need for physical media. SAILOR 2.1 significantly decreases program sustainment costs in maintaining, shipping and tracking training materials.

"Someone finally listened to the fleet Sailors and placed a majority of our C4I system information in a single location," said IT1 Christopher Tierney, aboard the USS John Paul Jones (DDG 53).

SAILOR 2.1 will maintain its current security and privacy methods and policies, and the new changes will not effect security measures.

As the Navy's information dominance systems command, SPAWAR and the SAILOR 2.1 team look forward to receiving feedback on the launch of a product that directly benefits the Sailor, increases fleet readiness and improves product data availability, accuracy and accessibility. CHIPS

To access SAILOR 2.1 go to https://sailor.nmci.navy.mil. For more information about SAILOR 2.1, email sailor@spawar.navy.mil.

Nicole Collins is a public affairs specialist with SPAWAR.

NUWC Newport Achieves IT Acquisition Efficiencies with DoD ESI

By Floyd Groce

The Department of Defense Enterprise Software Initiative, established in 1998 and sponsored by the DoD Chief Information Officer, was created to consolidate requirements for commercial software applications and negotiate with vendors to save time and money in the acquisition of software.

ESI's scope has since expanded to include information technology hardware and services. Since its inception, ESI has achieved cost avoidance of more than $4 billion off commercial IT prices compared with prices published on the General Services Administration (GSA) Federal Supply Schedules.

In 2009, Laura DiPaola, a systems engineer at Naval Undersea Warfare Center, Division Newport, R.I., was tasked with purchasing a commercial off-the-shelf software suite. As a result, she conducted research on the requirements and processes to use an ESI Enterprise Software Agreement (ESA).

Rather than limit scope to a single acquisition, DiPaola explored how the division could maximize savings by expanding the use of ESI agreements. Working with the NUWC Division Newport command information officer, Robert Bernardo, as well as Stephen Lamb of the division's contracts department, DiPaola coordinated a team to initiate a Lean Six Sigma event with the objective of implementing a division-wide DoD ESI employment policy to:

- Maximize cost savings during the first year of implementation, as well as during the future years defense program (FYDP);

- Comply with DoD and DON directives by updating IT procurement processes to take advantage of ESI's enterprise agreements with enhanced terms and conditions that support DoD IT objectives and industry best practices; and

- Follow the Federal Acquisition Regulation order of precedence (see DFARS 208.002 and DoD Instruction 5000.2).

As a result of this event, the team outlined how using ESAs can reduce software costs and determined a new workflow process that would ensure ESAs were reviewed and used whenever possible.

The benefits were clear from the beginning. During a two-month sampling of software contracts with a value of more than $3,000, not including purchase card transactions, the division achieved tangible savings by using ESAs.

Additional benefits were also achieved: (1) lines of communication were opened between departments; (2) a collaboration of ideas regarding the practical application of ESI's agreements verification was explored; and (3) mutual agreements were made that contribute to NUWC Newport's acquisition efficiency.

The team also created metrics to illustrate the ways in which NUWC is benefitting from ESI's software licensing strategy and its cost savings mechanisms.

The next step for NUWC Newport was to capture definitive savings metrics through a second Lean Six Sigma event to demonstrate ESI's advantages. This step focused on implementation and data gathering rather than on enforcing ESI use. The team hopes to achieve greater buy-in from the entire division and share the ESI metric reports across the organization so that all stakeholders understand the tangible savings available through ESI.

Since its inception, ESI has achieved cost avoidance of more than $4 billion off commercial IT prices compared with prices published on the General Services Administration (GSA) Federal Supply Schedules.

Under the DON information technology efficiencies initiatives, the department is focusing on ways to save on IT investments, including commercial software, hardware and services. While each Navy component must work within its own processes and requirements, the example set by the team at NUWC Newport illustrates the benefits that can be gained by investigating and using ESI contract vehicles.

These agreements benefit the defense and intelligence communities, and in some cases, the entire federal government, enabling better negotiating and purchasing power for the acquisition of IT software, hardware and services. CHIPS

To learn more, visit www.esi.mil.

Floyd Groce is director of enterprise commercial IT strategy in the office of the Department of the Navy Chief Information Officer.

The Spectrum Sharing and Reallocation Dilemma

By Thomas Kidd and Mark Rossow

The electromagnetic spectrum is a unique resource. While in some ways it is similar to other resources, like oil or water, in other ways, it is very different. The electromagnetic spectrum is typically defined as the set of all non-ionizing radiation electromagnetic frequencies.

The electromagnetic spectrum we are most familiar with is a finite collection of frequencies between about 3,000 cycles per second (kilohertz), or 3 kHz, and 300 billion cycles per second (gigahertz), or 300 GHz. These frequencies are used in radio frequency systems.

The electromagnetic spectrum is unlike any other resource we use. Not only is electromagnetic spectrum finite, it is also instantaneously renewable. The moment one system stops using a set of frequencies — another system can begin using it. As a finite resource, the electromagnetic spectrum is in short supply, but its instantaneously renewable properties provide a near perfect resource for sharing.

The electromagnetic spectrum is unlike any other resource we use. Not only is electromagnetic spectrum finite, it is also instantaneously renewable.

The electromagnetic spectrum is managed by allocating particular sets of frequencies, known as bands, to different uses. Some bands may be used for satellite communications while others may be used for radio astronomy. Without allocating different uses to different parts of the spectrum, one system may interfere with the operation of another.

Due to increased spectrum use, it has become difficult to obtain and use many frequency bands in the United States, as well as in many foreign countries. As such, increased electromagnetic spectrum sharing requirements are imposed on spectrum users worldwide. Sharing spectrum can be accomplished in several ways. Technological capabilities, policies and cooperation agreements among users are some of the broad sharing techniques implemented today to maximize the use of the electromagnetic spectrum.

While sharing spectrum has some challenges, it is often possible for some spectrum-dependent systems and equipment to share without causing interference with other systems using the same spectrum. The most common example of sharing is geographical separation, which has been used for nearly a century.

Use of early television frequencies could be shared because television stations were located hundreds of miles apart. Technology can also provide spectrum sharing opportunities. Equipment that transmits radio frequencies at very low power levels may create only a slight rise in background noise. This characteristic provides the ability to reuse radio frequencies efficiently over much shorter distances.

There are also more sophisticated sharing scenarios, including the use of information technology databases that provide detailed information about spectrum-dependent systems and equipment, and their geographical location and transmission media data, as well as what types of signals may cause interference.

Advanced technologies can also “sense” the presence of a radio frequency signal and wait to transmit until other equipment or systems cease use. In many cases, sharing radio frequencies can be accomplished with minimal encroachment for most spectrum users.

However, whether as a result of policy, physics or technology, not all systems can easily share spectrum. Some systems may require interference-free spectrum to ensure operation is not negatively impacted or degraded. Systems that are integral to public safety, such as air traffic control radars, often require very high levels of protection.

Radar generally transmits very strong spectrum signals and receives its own reflected signals, which are incredibly weak. These signals often travel hundreds of miles over their reflected path, and only a miniscule amount of the original transmitted signal is returned to the radar. The high transmission powers of radar are prone to affect spectrum use that is within the transmission areas of radar, and radar is very susceptible to radio frequency interference when it is receiving its very weak returned signal. As a result, radar is generally allocated spectrum solely

VIRGINIA BEACH, Va. (July 20, 2011) Information Systems Technician 2nd Class Michael Smith, assigned to Riverine Squadron (RIVRON) 3, and Operations Specialist 1st Class Robert McGill, assigned to Navy Expeditionary Combat Command, set up satellite communications equipment during Trident Warrior 2011 at Joint Expeditionary Base Little Creek Fort Story. Trident Warrior is an annual fleet experiment focusing on new technology. U.S. Navy photo by Mass Communication Specialist 2nd Class Steven Hoskins.

Reallocations of frequency bands that displace existing spectrum use can create a cascading effect that can be extremely challenging, especially if the displaced users cause the users in other bands to be similarly displaced.

for radiolocation purposes, and other uses of spectrum are not allowed within the same allocations.

While the preponderance of spectrum-dependent systems and equipment can share some use of the same radio frequencies, not every system can share with every other system. Some systems cannot successfully operate in the same allocated set of frequencies. Given the escalation of spectrum use throughout the world, the alternative to sharing is reallocation. Portions of the spectrum are reallocated to allow for multiple, new uses of the same spectrum.

Reallocations may be implemented by the relocation of existing spectrum use out of one frequency band and into other frequency bands or by adding additional allocations within the same band. Reallocations of frequency bands that displace existing spectrum use can create a cascading effect that can be extremely challenging, especially if the displaced users cause the users in other bands to be similarly displaced. The ripple of disruption can have unforeseen effects and costly consequences. Reallocation is very similar to rezoning a section of a city and forcibly relocating its residents. Even when done with the greatest skill, it can be a very disruptive process.

Electromagnetic spectrum is a finite resource in short supply. As the United States and many other countries are engaged in maximizing the efficient and effective use of spectrum, spectrum sharing and reallocation considerations and initiatives are addressed daily.

And, due to the importance of spectrum in commerce, national defense and public safety, spectrum sharing and reallocation will continue for many years to come. CHIPS

Thomas Kidd is the director for strategic spectrum policy for the Department of the Navy. Contact Mr. Kidd at DONSpectrumTeam@navy.mil.

Mark Rossow provides strategic spectrum policy support for the DON spectrum team.

The DON SSN Reduction Plan Continues

By Steve Muck

The Department of the Navy is eliminating the unnecessary collection of Social Security numbers (SSNs) to protect personally identifiable information (PII). The SSN, to include any form of the SSN, such as truncated, masked, partially masked, encrypted or disguised, is ubiquitous and a key data element used to commit identity fraud.

The DON is eliminating SSN use where it is not necessary, or replacing it with another unique identifier, such as the Department of Defense identification number (DoD ID), which is associated with an individual's name. This article summarizes the department's SSN reduction efforts.

Phase 1 began in August 2010 with the release of a naval message issued by the DON CIO DTG 192101Z JUL 10: "DON Social Security Number Reduction Plan for Forms Phase One."

The message states that all DON forms managers must:

- Identify and review all official forms that collect SSNs;
- Justify continued use of SSNs by a flag officer or senior executive service employee (SES) who will validate and sign a Secretary of the Navy (SECNAV) 5213/1 SSN Reduction Review form for each official DON form to be used;
- Eliminate the SSN component from the form or eliminate the form itself;
- Identify and eliminate, or make official all "bootleg" forms (see section below for information on this topic) that collect SSNs and consequently have not been approved by a forms manager;
- Post all official forms to the DON Naval Forms Online website at https://navalforms.daps.dla.mil; and
- Provide the date the justification is completed for forms that continue to collect SSNs.

Status: Two rounds of reviews initiated with work still in progress. In almost every command review, 50 percent of the forms found to collect SSNs were either eliminated or the SSN component was removed from the form.

Phase 2 began in June 2011. All DON information technology system owners were notified that they must: identify and review all DON IT systems that collect SSNs; justify continued use of SSNs by a flag or SES employee who will sign a memo for each IT system; post the signed memo to the DoD IT Portfolio Repository-DON (DITPR-DON); and ensure all SSN/PII questions are accurately reported.

Status: Early results of the review are positive. DITPR-DON privacy data accuracy improved. Each reporting command shows an average 20 percent reduction in the number of IT systems that collect SSNs.

Phase 3 implementation will result in the elimination of SSNs from forms, electronic collections, surveys, spreadsheets and hard copy lists that continue to rely on SSNs as a unique identifier. The DON is waiting for the release of a Defense Department instruction regarding reduction of SSN use in the DoD before implementing this next phase. The instruction will provide guidelines regarding the substitution of the DoD ID number for the SSN in many DoD and DON business processes. Phase 3 will also place restrictions on the use of memorandums, email, spreadsheets, electronic reports and hard copy lists that contain SSNs.

Status: The Defense Department is performing a final review of the instruction prior to publication in the Federal Register. The DON will announce implementation of Phase 3 after the release of the DoD instruction.

What is a bootleg form?

Have you ever wondered if a request for your SSN on a Defense Department form is an authorized collection? Forms that are not official are also referred to as bootleg forms. Here are some things to look for to determine if the form is official:

- Does the form have a form control number, such as "OPNAV 5211/13," on the bottom of each page?
- Does the form display the date it was created?
- Does the form, which has been pre-populated with PII, include the privacy warning, "FOR OFFICIAL USE ONLY – PRIVACY ACT SENSITIVE: Any misuse or unauthorized disclosure of this information may result in both criminal and civil penalties" within the body of the form?;
- Does the form, which requests PII directly from the user, have a Privacy Act Statement (PAS) within the body of the form on the last page? A PAS includes:
    - The authorizing authority (usually a law or statute) for collecting privacy information;
    - The purpose of the form (e.g., why the privacy information is being collected);
    - The routine users of the form and any system of record notice published, if applicable; and
    - Disclosure rules — such as what happens if the requested PII is not provided.

Bootleg forms should be sent to your forms manager for review. If you do not have a forms manager, contact your legal department or email the DON forms manager Barbara Figueroa at barbara.figueroa@navy.mil for assistance. CHIPS

Steve Muck is the privacy lead for the Department of the Navy Chief Information Officer.

Q&A with Cmdr. Blake McBride
Arctic affairs officer Task Force Climate Change

Cmdr. Blake McBride

The Navy released an Arctic environmental assessment and outlook report on Aug. 15, 2011 — which will be instrumental in developing future strategic plans and investments in a region that is becoming increasingly accessible to exploration and commercial enterprise.

Scientific evidence indicates that the Earth's climate is changing, with the most rapid changes occurring in the Arctic. While there is uncertainty about Arctic ice extent, scientists agree that the Arctic may experience nearly ice-free summers as early as the 2030s. This opening in the Arctic may lead to increased resource development, research, tourism, and could reshape the global transportation system. Because the Arctic is primarily a maritime environment, the Navy must consider the changing Arctic in developing future policy, strategy, force structure and investments.

CHIPS asked Cmdr. Blake McBride, Arctic affairs officer for Task Force Climate Change to talk about the Navy's assessment and he responded in writing in September.

CHIPS: According to the assessment, sea ice plays a crucial role in the Arctic climate. The amplified warming of the Arctic has been explained as due, in part, to a positive albedo feedback loop: as the air temperature increases, the sea ice cover (which presents a bright, white, highly reflective surface) melts and reveals the darker ocean surface. This dark surface absorbs more solar energy during the summer season when the sun never sets. This causes more heating, which causes more melting, creating a cycle that helps perpetuate warming conditions. For the average person trying to understand why sea ice is melting — is this too simple of an explanation?

McBride: Well, you have explained the feedback loop pretty well. As the darker waters absorb more heat, the ice melts.

But it's worth noting that the Arctic Ocean rapidly freezes back over in the fall and stays frozen for most of the year. The critical impact of the feedback loop is that it is reducing the thickness of the ice. Thin ice is more likely to melt each summer, so more of the water becomes ice free. We have been using satellite imagery to monitor the reduction in area ice coverage since 1979, but ice thickness has been more difficult to measure.

Navy submarines actually began noticing loss of ice thickness in the 1990s. In fact the Naval Ice Center even had a symposium in 2001 titled, "Naval Operations in an Ice-Free Arctic," to begin discussions on this issue and its impacts on the Navy.

Task Force Climate Change works with the Ice Center and the University of Washington's Applied Physics Laboratory to track the volumetric loss of sea ice in the Arctic. Current model projections indicate that by 2017 sea ice volume will be at 10 percent of its estimated 1979 value. Loss of ice volume is really a more significant indicator of environmental change, but it is the resulting reduction in ice extent that is making the region more accessible to maritime enterprise.

The shrinking ice cap is playing a triple role in warming the Arctic. The diminished ice is reflecting less solar energy; the open water is storing more energy that is released back to the atmosphere. This open water is also supplying greenhouse gas to the atmosphere in the form of water vapor. Those three factors combine to produce a strong regional greenhouse over the Arctic.

CHIPS: What does this mean for the Arctic region; does it have global implications as well?

McBride: The Arctic is not a vacuum. Arctic air and water interacts in very complex ways with global air and water circulations. For the reasons you have listed, the Arctic is experiencing a changing climate more rapidly than the rest of the Earth, but it presages what will happen later to the rest of the planet.

It's also worth noting that methane, which is a very strong, but short-lived greenhouse gas, may be released in great quantities from the sea floor in the Arctic and from melting permafrost.

CHIPS: The study states that ice thickness is also closely connected to ice strength, and so changes in thickness are important to navigability by ships, to the stability of the ice as a platform for use by indigenous people and marine mammals, and to light transmission through the ice cover. Studies indicate that polar bears are at risk, as wells as the ringed seals that bears eat, and humans hunt, which are also dependent on the sea ice to rest, give birth, nurse and feed. Is there any kind of human intervention that can mitigate the risks to indigenous people and polar animals?

McBride: The Navy and Coast Guard are aware that some of our operations could impact marine mammal migration routes and feeding patterns, as well as Alaska Native subsistence hunting. When we start doing surface ship and air operations up there, we will need to confer with tribal representatives and conservation authorities to ensure we minimize our impact.

CHIPS: It almost sounds like the Arctic region could become one big free-for-all with multiple nations staking claim to natural resources newly open to exploration. So far, Russia, the United States, Canada, Norway and Denmark have claimed territory. Is there a process or plan to address the multinational claims?

McBride: Multinational claims are adjudicated by the United Nations Convention on the Law of the Sea, or UNCLOS, and the Arctic Council. As a nation with Arctic territory, the U.S. is a member of the Arctic Council, but we are one of the few nations on Earth that has not ratified UNCLOS. The Navy has been on record for many years that accession to UNCLOS is in the best interests of the Navy and the nation.

While significant uncertainty exists in projections for Arctic ice extent, the current scientific consensus indicates the Arctic may experience nearly ice-free summers sometime in the 2030s. Models predict Arctic summer ice will decrease by 15 to 30 percent (3 percent per decade) and ice volume by 40 percent.

CHIPS: Twenty years seems pretty close, is there a list of priorities so that the Navy and U.S. can prepare for this eventuality?

McBride: The Navy's position is that the most likely scenario is that the Arctic will experience one month of conditions with less than one-tenth coverage of ice in the mid to late 2030s. We acknowledge that wild cards like meteorological variability, changes in ocean currents and rapid glacial ice melting could change the dynamics, but we believe a consensus of opinion supports that timeframe. But our first priority is to develop a better understanding of the changing environment and the many variables that impact it.

How we operationally prepare for an ice-free Arctic depends on what our mission requirements will be. Right now we are assessing environment changes and their corresponding strategic implications, what possible missions we may be called upon to complete, what we will need to do those missions, and what we currently lack.

The Coast Guard has regulatory duties and increased human activity in the region is a more immediate problem for them. They are already seeing some increase in human activity in territorial waters, including destination shipping, oil and gas exploration, and adventure tourism. However, the Navy still has time to approach this deliberately and responsibly.

CHIPS: The assessment discusses how various scientific reports will inform the program objective memorandum process, specifically POM 14. This allows the Navy's decisions to be based on a consensus of accepted scientific sources. How will POM 14 be affected? What decisions must the Navy make to ensure national security?

McBride: We have much to learn before we start investing in Arctic capabilities. We certainly do not wish to spend money before need. Aside from getting a better understanding of the rate of environmental change, we need to start assessing how cold weather affects our platforms, sensors, weapons systems and people.

Navy Cmdr. Blake McBride standing on sea ice in front of Mt. Dundas during a liaison visit to the U.S. Air Force Base in Thule, Greenland. The area is now off limits due to seasonal melt.

The current fleet is optimized for mid-latitude and tropical operations. For example, we're not sure how sea spray icing will affect our exposed sensors, or how extremely cold air and water temperatures will affect habitability systems on the ship. This will only come from experience, so we will need to start making trips to the Arctic. That in itself is not cheap.

Everything in the Arctic is more expensive because it costs a lot to ship supplies and material up there. For POM 14, we may see some commitment of funds for further studies, strategic tabletop exercises and Arctic training opportunities.

CHIPS: Clearly, the scope calls for a whole government approach to dealing with the changes to global navigation, competition for resources, increased greenhouse gases and rising sea levels. What organizations is the Navy working with?

McBride: The Navy's Arctic Roadmap and Strategic Objectives for the Arctic emphasize the importance of partnerships. We recognize that no one agency can afford to deal with the changing Arctic on its own. Task Force Climate Change, for instance, is highly networked, with membership from over 130 military, federal and civilian organizations. We are working particularly closely with the U.S. Coast Guard. We are also building relationships with Arctic nation militaries and security forces so we can learn from their experience and share responsibility for things like search and rescue, oil spill mitigation, disaster response and maritime domain awareness.

"The shrinking ice cap is playing a triple role in warming the Arctic: diminished ice is reflecting less solar energy; the open water is storing more energy that is released back to the atmosphere. This open water is also supplying greenhouse gas to the atmosphere in the form of water vapor …"

CHIPS: Anything else readers should know?

McBride: There are many competing priorities facing the Department of Defense that must be considered in light of limited resources. The good news is that senior leadership of the Navy is aware of the changes taking place in the Arctic and the challenges that we will face in the future. The Navy will ensure that we are ready for any future mission requirements in the Arctic, but we will approach this in a deliberate and responsible manner. CHIPS

Follow Task Force Climate Change on Facebook: www.facebook.com/NavyTFCC. To access the Arctic Environmental Assessment and Outlook Report, go to http://greenfleet.dodlive.mil/files/2011/08/U.S.-Navy-Arctic-Environmental-Assessment.pdf.

Cyber Strategy Initiatives

By Mary Purdy and Rob Psimas

CYBERCOM's Effect on the Cyber/IT Workforce

In 2010, when United States Cyber Command (CYBERCOM) was established to unify the military's computer network defense and cyberspace operations, it became imperative for the services to integrate several distinct communities into a single warfighting "team." As a result, cross training the workforce was implemented, personnel career paths were revised in concert with and supported by new technical training, and recruitment and retention of personnel with specific technical skills became essential.

With cyber workforce management recognized as a top priority, the "Department of Defense Strategy for Operating in Cyberspace," issued in July 2011, includes five strategies, of which two are workforce related:

- **Strategic Initiative 1:** Treat cyberspace as an operational domain to organize, train and equip so that DoD can take full advantage of cyberspace's potential; and

- **Strategic Initiative 5:** Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation. This cultural shift that recognizes cyberspace as a warfighting domain and the cyber workforce as a key element is already driving change within the community.

In addition to the establishment of the Navy's U.S. Fleet Cyber Command/U.S. 10th Fleet and Marine Forces Cyber Command, and the publication of the DoD's Cyber Strategy, two other initiatives are converging to affect changes in cyber/IT professional workforce development. First, the federal government, collaborating across federal agencies, is working to provide a better picture of the work carried out by the federal cybersecurity workforce, defined by the Department of the Navy as the cyber workforce. This includes information technology, intelligence and law enforcement (Naval Criminal Investigative Service) portions of the workforce.

Second, under current fiscal realities, the DON Chief Information Officer, with a Secretary of the Navy mandate, is reviewing and instituting IT efficiencies to reduce the overall costs of operation and increase effectiveness. This effort includes cyber/IT workforce management.

National Initiative for Cybersecurity Education

For the first initiative, Chris Kelsall, director of the cyber/IT workforce for the DON CIO, is collaborating with the National Initiative for Cybersecurity Education (NICE), the National Institute of Standards and Technology (NIST), the DoD CIO and CYBERCOM, as well as other federal agencies, to develop a standard set of cybersecurity workforce functional roles. This standardized set of federal specialty areas will be mapped to the joint capability areas and the mission essential task list. New

DON policy to address cyber/IT continuous learning and training requirements is under development and will evolve as a comprehensive picture of cyber/cybersecurity/IT work emerges.

DON Cybersecurity/IA Workforce Efficiencies

For the second initiative, the cybersecurity/IA workforce efficiencies working integrated product team (WIPT) reviewed areas that may result in cost savings. Among other cybersecurity/IA workforce efficiencies, the WIPT recommended that the workforce management discipline, instituted for the IA Workforce Improvement Program (IA WIP) under DoD Directive 8570.01, "Information Assurance Training, Certification, and Workforce Management," be expanded to cover the entire cyber/IT workforce. The Department of Defense IA WIP is a noteworthy qualification program that contributes greatly to the knowledge level of the cybersecurity/IA workforce. As the DoD directive is rewritten to include the entire cyber workforce, the DON cyber/IT career development program will provide further guidance on continuous learning, certificate programs, certifications and career progression. At the same time, leveraging IA WIP electronic management and training solutions will reduce workforce management costs.

Snapshot of the Cyber/Cybersecurity/IT Workforce

The NICE initiative organizes the cyber workforce into seven broad categories, each including multiple functional specialty areas. The DON has not formally accepted these groupings. Therefore, readers must keep in mind that this list continues to evolve, but aligns well with the NICE project, as well as the defense planning and program guidance. Figure 1 is a snapshot of the roles performed in the cyber workforce with functional specialty areas defined on the next two pages.

Figure 1. Cyber Workforce Snapshot

Category	Functional Descriptions
Securely Provision	Roles concerned with conceptualizing, designing and building secure IT systems; roles responsible for some aspect of systems development.
Operate and Maintain	Roles responsible for providing the support, administration and maintenance necessary to ensure effective and efficient IT system performance and security.
Protect and Defend	Roles responsible for the identification, analysis and mitigation of threats to internal IT systems or networks.
Investigate	Roles responsible for the investigation of cyber events/crimes of IT systems, networks and digital evidence.
Operate and Collect	Roles responsible for the highly specialized and largely classified collection of cybersecurity information that may be used to develop intelligence.
Analyze	Roles responsible for highly specialized and largely classified review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Support	Roles providing support so that others may effectively conduct their cybersecurity work.

While functional specialty areas of all seven categories are complete, for the purposes of this article, only the specialties of the largest portion of the cyber/IT workforce who securely provision, operate and maintain, and protect and defend, are listed on the next pages and are further defined.

Functional Specialty Areas

Securely Provision

Information Assurance (IA) Compliance – Oversees, evaluates and supports the documentation, validation and accreditation processes necessary to assure that new IT systems meet an organization's IA requirements. Examples of job titles: designated accrediting authority; IA program manager; IA manager; IA officer; accreditor; validator.

Systems Requirements Planning – Consults with customers to evaluate functional requirements and translates these requirements into technical solutions. Examples of job titles: computer systems analyst; capabilities development specialist; solutions architect; systems engineer; contracting officer technical representative.

Systems Development – Works on the development phases of the systems development life cycle. Examples of job titles: systems engineer; IA engineer; information systems security engineer; IA developer; configuration manager.

Enterprise Architecture – Responsible for the capabilities phases of the systems development life cycle. Examples of job titles: systems engineer; information systems security engineer; IA architect; network security analyst; security architect.

Software Engineering – Develops, creates, and writes/modifies codes, computer applications, software or specialized utility programs. Examples of job titles: software developer; software engineer; computer programmer; Web application developer; IA software engineer.

Test and Evaluation – Develops and conducts tests of systems to evaluate integration processes. Examples of job titles: computer network operator; testing and evaluation technician; systems engineer; information systems security engineer; IA engineer; R&D engineer.

Operate & Maintain

Network Operations Management – Plans, organizes and directs the operation, administration, maintenance and provisioning of networked systems to ensure availability and integrity of information. Examples of job titles: senior watch officer; information systems manager; data center manager; computer services director; combat information systems officer.

System Administration – Installs, configures, troubleshoots and maintains server hardware and software to ensure confidentiality, integrity and availability. Also manages accounts, firewalls and patches. Responsible for access control/passwords/account creation administration. Examples of job titles: website administrator; systems administrator; server administrator.

Network Services – Installs, configures, tests and maintains networks including hardware (hubs, bridges, switches, multiplexers and routers) and software that permit sharing and transmission of information. Examples of job titles: network designer; network administrator; network engineer; network systems and data communications analyst; spectrum warfare officer; telecommunications engineer.

Data Administration – Develops and administers databases and/or data management systems that allow for the storage, query and utilization of data. Examples of job titles: data warehouse specialist; database developer; database administrator; data architect; information dissemination manager; content staging specialist.

Protect & Defend

CND Management – Oversees Computer Network Defense Service Provider (CND-SP) operations within organizations. Examples of job titles: mission manager; senior watch officer.

CND Infrastructure Support – Tests, implements, deploys, maintains, and administers the infrastructure hardware and software that are required to effectively manage the CND-SP network and resources. Examples of job titles: CND network security engineer; intrusion detection system (IDS) engineer; IDS technician; IDS administrator; security specialist.

CND Incident Response – Investigates and analyzes all response activities related to cyber incidents within the network environment or enclave. Examples of job titles: incident responder; incident handler; computer crime investigator.

CND Analysis – Uses data collected from a variety of CND tools (including intrusion detection system alerts, firewall and network traffic logs, and host system logs) to analyze events that occur within their environment for the purpose of mitigating threats. Examples of job titles: incident analyst; sensor analyst; network defense technician.

Vulnerability Assessment and Management – Conducts assessments on threats and vulnerabilities, determines the level of risk, deviations from acceptable configurations, enterprise or local policy, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations. Examples of job titles: CND auditor, close access technician; red team technician; blue team technician.

Customer Service and Technical Support – Provides technical support and training to customers who need assistance with using client level hardware and software. Examples of job titles: computer support specialist; technical support specialist; help desk representative; systems administrator.

Information Systems Security Management – Oversees the IA program of an information system in or outside the network environment; may include procurement duties. Examples of job titles: information systems security officer (ISSO); IA manager; IA officer, IA program manager.

Knowledge Management – Manages and administers processes and tools that enable the organization to identify, document and access intellectual capital and content. Examples of job titles: business information manager; document steward; content administrator; information resources manager; cyber battlespace operations officer.

Systems Security Analysis – Conducts the integration/testing, operations and maintenance of systems security. Examples of job titles: IA officer; information systems security engineer; IA operational engineer; spectrum warfare officer.

Ongoing and Future Cybersecurity Workforce Development

An inventory of knowledge, skills, abilities and competencies will be mapped to the cybersecurity specialty areas defined on the previous pages. This effort is ongoing within the federal agencies, the services' functional offices of primary responsibility (OPRs), and in conjunction with manpower and personnel readiness staffs. Concurrently, functional OPRs are teaming with the services' training commands' staffs to update and modernize officer and enlisted courses and roadmaps to ensure the correct training is provided to the appropriate specialties.

Civilian competencies are under review to be translated into common assessment, hiring, qualification, training and performance standards. Once the workforce categories, specialty areas and roles are finished, final validation of the new training will proceed.

Working together our community can build well-defined military and civilian professional career progressions, strong qualification programs through continuous learning, and improved technical training for the cyber/IT team.

Emerging risks, threats and vulnerabilities require workforce and training managers to be vigilant in updating career development and training requirements. It is incumbent on the OPRs and workforce managers to review and monitor community proficiency levels, and then create change to improve the community's operational capabilities.

Workforce management processes are critical to the development of an engaged workforce, and ultimately, to mission success. CHIPS

The Department of Defense Cyber Strategy is available at: www.defense.gov/news/d20110714cyber.pdf.

Mary Purdy holds a Global Information Assurance Certification (GIAC) Security Leadership Certification (GSLC) and is the cybersecurity/IA workforce management, oversight and compliance manager for the DON CIO cyber/IT workforce team.

Rob Psimas led the DON cyber/IT workforce identification tiger team. He worked with USCYBERCOM, NIST, NICE and DoD CIO, Army, Air Force, Marine Corps and Navy representatives to develop a standardized set of cyber specialties/roles mapped to joint capability areas and mission essential tasks.

The SRW Telemetry Operations waveform enhancement demonstrates the ability to rapidly and affordably add capability to JTRS networking capabilities through software-only upgrades

JPEO JTRS Delivers SRW Telemetry Operations Waveform

By JPEO JTRS Corporate Communications and Public Affairs Directorate

The Joint Program Executive Office for the Joint Tactical Radio System (JPEO JTRS) Network Enterprise Domain (NED) successfully completed the SRW1.1 waveform development environment design verification test. This is an important milestone because the enhancement introduces the telemetry operations domain and mode to the current version of SRW 1.01.1, as well as adding significant improvements to the performance and functionality of the core waveform.

The SRW1.1 enhancement was developed in response to the Army's need for a simultaneous control and video feed from small unmanned ground vehicles (SUGV). The SRW1.1 was modified to support the bandwidth requirements needed to display video. The enhancements allow for SRW to control the vehicle and to download imagery from the SUGV. This is significant because it is being done with software and not affecting the hardware.

"Delivery of the SRW Telemetry Operations waveform enhancement demonstrates our ability to rapidly and affordably add capability to JTRS networking capabilities through software-only upgrades," said Navy Capt. Jeff Hoyle, the JTRS Network Enterprise Domain (NED) program manager.

This waveform will be incorporated into the SFF-D radio by the JTRS Handheld, Manpack and Small Form Fit (HMS) program office for eventual fielding on the Army's SUGV platform.

The verification tests validated all telemetry operations functionality and performance and confirmed reverse interoperability between the SRW 1.1 and SRW 1.01.1 waveform variants. It also provided an opportunity to address discrepancies found in the existing SRW 1.01.1 functionality and performance.

"The ability to rapidly improve, upgrade and deploy secure, interoperable waveforms, coupled with a JTRS enterprise business model that maximizes waveform software reuse, affordability, and competition among defense communication providers, enable us to continuously improve fielded JTRS networks throughout their life cycle in response to joint warfighter needs and priorities," Hoyle said. CHIPS

For more information about JPEO JTRS contact the corporate communications and public affairs deputy director James J. "Jeff" Mercer at (619) 524-4600 james.j.mercer@navy.mil.

Powering America's Army

Army's top network and cyber leaders talk about the Network of 2020

By Sharon Anderson

The Army has developed a holistic network strategy that fundamentally changes how it acquires, tests and deploys its network. In the past, the Army fielded network systems independently and on the acquisition timelines of posts, camps and stations, but the Army's new approach will deploy one network as an enterprise linking capabilities to a Soldier and the small unit, as well as to joint, coalition, interagency and mission partners.

The Army's top cyber and network leaders, Chief Information Officer/G-6 Lt. Gen. Susan S. Lawrence, Commander Army Cyber Command Lt. Gen. Rhett A. Hernandez, Commanding General NETCOM/9th Signal Command Maj. Gen. Jennifer L. Napper, and Chief of Signal Maj. Gen. Alan R. Lynn each talked about their roles in building the Network of 2020 at the LandWarNet conference in Tampa, Fla.

The generals also met with the media Aug. 24 to drill home the message that the Army is migrating to a uniform architecture and a common operating environment (COE) that will enable quicker, and potentially cheaper, development and fielding of secure interoperable applications and systems that satisfy operational requirements.

Army CIO/G-6 and NETCOM/9th Signal Command

As the United States winds down Operations New Dawn and Enduring Freedom, the Army will reduce the number of Soldiers on active duty. At the same time, the Defense Department budget will shrink. In these circumstances, the Army's mandate will be to produce a force that is smaller yet better trained and more capable. To address these changes, Lt. Gen. Lawrence explained that in her first few months as Army CIO/G-6, she first focused on the vision of the network and aligned its development over the next three program objective memorandum cycles.

"So the vision is the Network of 2020 — Powering America's Army… One of the forcing functions of keeping us connected globally is the Base Realignment and Closures. We are now an 80 percent based CONUS Army, and what that means is we have to have the network and power for that CONUS-based Army so that they can be better trained, train as Soldiers fight with the ability to deploy with little to no notice to any austere environment but be connected to their mission command applications. And that is what we are working for, and so our bumper sticker is: 'Always networked, always on,'" Lawrence said.

The first step to an enterprise approach is single identity, Lawrence explained.

"That is a Soldier that can take his or her CAC and go anywhere in the world, put it in a government computer and have immediate access to their information because at the end of the day that's what it is all about — data. So whether the Soldier is sitting at home, or TDY, or at their post, camp or station, or deployed in Iraq, Afghanistan, Libya, Syria — in any austere environment — they can connect to the information."

In February 2011, the Army began migrating Microsoft Exchange email users to the Defense Information Systems Agency (DISA) Exchange. As of the end of August more than 90,000 users have migrated to the new enterprise email system. Although there were some problems with latency in the beginning, and a temporary halt to migration in July to resolve the challenges, the Army is now moving full speed ahead on the migration, Maj. Gen. Napper said.

"We knew we had challenges on the network in CONUS because of how many people we had running pieces and parts, and the inability to look at the entire network from top to bottom. We also thought we knew what kind of configuration would be required at the desktop and the network to do this enterprise email. We were not correct on the complete configurations because we also changed identity management. So that gave us a little bit of a challenge. We now have a very good, I would call it a 90-percent solution of how the network and those end devices have to be configured in order for us to be able to draw services from the enterprise."

Users are now armed with a pre-deployment checklist to ensure a smooth transition to enterprise email, according to Napper.

"Since we stopped the pause and restarted with migrating, we did two test locations at Fort Lee and Fort Leavenworth, and we have had absolutely no issues with those two locations. It took less than a minute per email account to migrate. Some of them in the beginning took 10 or 15 minutes so that's a sign you have a problem on your network. We knew it was going to be painful in the beginning. We did warn folks. They really didn't want to hear us, but we did warn them. I think now we have a much better process and configuration control going forward," Napper said.

The Army estimates it will save as much as $500 million in IT costs between fiscal years 2012 and 2017.

"It is a combination of the data center consolidations and enterprise email. As we were working our business case analysis, we computed what it cost to have a Soldier email account today. It is very expensive — over $125 just for a basic email account. So by going through a managed service and doing the consolidations that same account is now costing about $34. So that's where the huge savings are," Lawrence said.

Enterprise email will provide users with much greater storage and a Defense Department global address list. It will significantly reduce hardware, storage and personnel costs, and by eliminating the seams between heterogeneous local networks, security will increase.

"Today we have multiple help desks on installations managing their post, camp and station email. In the future we are going to have an enterprise service desk… In some posts, camps and stations that we inventory, we'll find five or six different help desks doing their own thing. So those are the things

Maj. Gen. Jennifer L. Napper, Lt. Gen. Rhett A. Hernandez, Lt. Gen. Susan S. Lawrence and Maj. Gen. Alan R. Lynn, the Army's senior network and cyber commanders, discuss the network strategic vision moving toward 2020 at the LandWarNet 2011 conference in Tampa, Fla., Aug. 24, 2011. Photo by J.D. Leipold.

Enterprise email will significantly reduce hardware, storage and personnel costs, and by eliminating the seams between heterogeneous local networks, security will increase.

Army Cyber Command: www.arcyber.army.mil/.

Army CIO/G-6: http://ciog6.army.mil/.

The Network Enterprise Technology Command/9th Signal Command (Army) www.army.mil/netcom/.

Office Chief of Signal (OCOS): www.signal.army.mil/ocos/.

we are going to go after. We are literally going to go post, camp and station because I need those resources to reinvest in the Network of 2020. We want to get to everything over IP, wireless TOCs, tactical operations centers, Voice over IP. There are so many things that we need to be doing quickly. So we need to get those dollars back in and reinvested as fast as we can," Lawrence said.

The Army will eliminate approximately three-quarters of its data centers between 2011 and the end of 2015. In their stead, the Army will use a unified cloud computing operational model to provide enterprise hosting as a managed service. The Army will move applications into the DoD cloud as much as possible; then leverage commercial infrastructure; and, as a last resort, use Army-owned data centers.

The DISA managed cloud and nine Defense Enterprise Computing Centers will provide email for 1.4 million unclassified network users and more than 200,000 secret network users across the Army, and Transportation, European and Africa commands. The Army is moving along smartly in this direction, according to Lawrence.

"In fact, the Army is one of the more proactive ones in federal service when you look at all the data centers across federal service. We are going to take down about 25 percent [data centers] for all the right reasons. One of the things we learned during Operation Rampart Yankee is that we were operating at a very low inefficient rate across our servers in the Army.

"So this is just a no-kidding, smart thing to do. Twofold, one is not just doing the physical data center consolidation thing; it is spring cleaning. We have old applications we have been maintaining for a long time and so as we reduce our data centers, we are mandating that you cut your applications 30 to 50 percent. That's where you are going to get real savings and also in manpower as we go down from 300 data centers to 75 — it's even going to be below that by the time we are done, and it will be less people needed to maintain it."

Reducing costs is not the only factor in moving to an enterprise network. Lawrence explained the network will be more capable, global, seamless, trusted and reliable and meet the functional needs of the entire Army.

"Someone asked me what is the hardest, biggest impediment to achieving this [building the network], and I said it has to be the culture. The environment of 'if I can't touch it myself, if I don't own it, I don't trust it …' Intuitively we know what we are doing is right. It is just the culture of the trust," Lawrence said.

While Lawrence as the CIO/G-6 provides the vision, governance and policy for the Network of 2020, NETCOM/9th Signal Command is the operational arm of building, operating, defending and maintaining the network for the Army.

"In a short synopsis I'd say that our job is to execute the vision of the CIO in accordance with the orders from Army Cyber Command. It is an exciting time for us. We are in the middle of implementing all of the global networking enterprise initiatives that General Sorensen [former Army CIO/G-6 Lt. Gen. Jeffrey A. Sorensen] and now General Lawrence have been talking about for about three years.

"The second focus that we have this year is transforming the way we deliver the capabilities on every post, camp and station globally. We are getting at this as an enterprise approach. We have built together a process we are calling Army baseline IT services (ABITS) by which we can identify the kind of capabilities they need in the posts, camps and stations and the resources necessary to deliver that and to get down to one enterprise," Napper said. "If we have a bumper sticker it is that: 'We are one team in the Army providing one network.'"

Army Cyber Command

The Army activated Army Cyber Command/2nd U.S. Army Oct. 1, 2010, with its headquarters split based at Fort Belvoir and Fort Meade. The command provides the full spectrum of cyberspace operations.

It is a global command with more than 21,000 Soldiers and civilians serving worldwide. Army Cyber Command is supported by NETCOM/9th Signal Command, Intelligence and Security Command (INSCOM), and 1st Information Operations Command (Land).

"Our mission is to direct and conduct network operations and defense of all Army networks. The Army Cyber Command is the Army's proponent for cyberspace operations to improve all aspects of doctrine, organization, training, materiel, leadership, personnel and facilities related to cyberspace operations.

"As we work to train, man and equip in cyberspace — it is a domain we must ensure we maintain the freedom to operate. And as you all know, each day the threat is growing more sophisticated and evolving. [We] recognize the need to

The Network of 2020 will enable:

- Access to key information anytime, anyplace.
- Sharing of information to facilitate fire and maneuver — and survive in close combat.
- Provide collaboration capability to aid in seizing and controlling key terrain.
- Employ lethal and non-lethal capabilities, coupled with sensors, to effectively engage targets at extended range.
- Distinguish among friend, enemy, neutral and noncombatant.
- Integrate indirect fires.

operate and defend against cyber threats and the importance of enabling mission command, and when directed conduct cyberspace operations in support of full spectrum operations to ensure U.S. allied freedom of action in cyberspace and to deny the same to our enemies. We also serve as the cyberspace proponent for the Army and coordinate information operations with the Army. We are the service component to U.S. Cyber Command," Lt. Gen. Hernandez said.

Network dominance is an integral part of the cyber fight, Hernandez explained.

"Cyber threats demand new approaches to managing information, securing information and ensuring our ability to operate. Cyberspace is on par with the other warfighting domains of land, sea, air and space. It is in cyberspace that we must use our strategic vision to dominate the information environment throughout interdependencies and independent systems." Hernandez said.

The 1st Information Operations Command (Land) is the Army's only full spectrum information operations organization engaged in IO theory development and training and operational application across the full range of military operations. The command has regionally focused information operations and IO-related intelligence planning teams assigned to provide reach-back planning and special studies support. Operations planners are involved prior to, during and after exercises and support contingencies, such as the counter-improvised explosive device effort.

"Our operations center directs our mission, and in many ways, is our center of gravity. Additionally, we are growing a cyber brigade to serve as our operational arm for full spectrum capabilities. During the last year, we have been pretty busy, as you consider, we started from scratch. We have accomplished some major objectives that I'd like to highlight.

"First and foremost, we have established a high level of integration with U.S. Cyber Command and our fellow service cyber components. We have an operation focus with an unprecedented unity of effort in operating and defending all Army networks globally 24/7.

"We are heavily engaged in operational planning with U.S. Cyber Command contributing a growing bench of cyberspace planners that are focusing our efforts on cyberspace operations and to support warfighting commanders. For the first time I believe we have really planned and executed realistic cyber integration into major exercises, and I am excited that we have established the Army cyber proponent and begun the hard force development work.

"Additionally, we have conducted the comprehensive Army Cyberspace Assessment leading to our work on an Army Cyber 2020 Strategic Plan. While our mission is clear so too is our vision for Army Cyber 2020 starting to take shape. I'm building a professional team of elite, trusted, precise, disciplined cyber warriors defending Army networks, who when directed are able to provide dominant full spectrum cyber effects enabling mission command and ensuring a decisive global advantage," Hernandez said.

Army Cyber Command has three major lines of effort to guide its work, according to Hernandez. "First, operationalize cyber. Second, grow Army's cyber capacity and capability, and third, recruit, develop and retain the right cyber warrior force. The final point I would like to make is for a command built around technology, it is important to remember our most valuable asset is our people. They are the centerpiece to our work. Our Soldiers and civilians will determine our success and ensure that we remain second to none."

Chief of Signal

The Office Chief of Signal (OCOS) is the single point of contact for personnel development matters affecting the Signal Regiment within the eight personnel life cycle management functions: structure, acquisition, individual training and education, distribution, deployment, sustainment, professional development and separation.

As the commander for the Fort Gordon home of the Signal Center of Excellence, Maj. Gen. Lynn is the 35th Chief of Signal.

"Essentially what I do is run the university for signal officers, non-commissioned officers, Soldiers and warrant officers. But we also provide the future vision for the Signal Regiment. What I have been working on the last year is a fundamental change to the Signal Corps. Our current design is probably Desert Storm-era doctrine where we provided support just down to the battalion level. As you know, battalion level is just not low enough in the formation right now.

"The Combined Arms Center at Fort Leavenworth took a look at what our requirements would be, and they came across the mission essential capabilities list that we need to provide and that includes communications down to the company level and below. There is one caveat though, they did not want us to grow the number of Signal Soldiers that we have so we had to go from battalion level to company level and below without any growth in personnel," Lynn said.

To meet the challenge, the Army studied signal structure, doctrine, training, equipment and the employment of signal forces to design a new construct.

"So what we came up with is that we need smaller, more capable teams, much like the Special Operations Forces use, like the JCSE (Joint Communications Support Element) is running with, and smaller, more capable systems as well.

"[We looked at] commercial standards, a lot of commercial off-the-shelf equipment. We even looked at some small handhelds, including iPhones and Droids, this will allow us to cover more area because they are smaller teams. Same number of people but smaller teams, more capable equipment that can go further down in the force to provide support," Lynn said.

Training is also changing, according to Lynn.

"Instead of training on one box, which we do today, for example, we will train a satellite operator. Tomorrow, we are going to teach them the theory of satellite line-of-sight and triple spherical scatter. If they understand the theory, as the boxes change according to Moore's Law, and they will change rapidly, they will understand the theory, and we just have to teach them how to operate the buttons. The buttons piece they will be getting from their apps, the applications we develop.

"We are developing our own apps at the Signal Center of Excellence. These apps are how the Soldiers like to train today. If you show them a projector and a PowerPoint slide, they will look at you like, *Are you kidding me*? They want to have that touch and feel on that system, they want to see it on a screen … By the time they actually get to the equipment, they are very familiar with it; they know how to operate it. It is the way they like to learn."

Training includes a range of opportunities: live, virtual, constructive and gaming.

"Soldiers today are interested in gaming. So we are already developing gaming in a number of the centers of excellence. Soldiers really care about their avatar. If they shoot OK at the range, their score is put into the system. So if they only score marksman in the virtual gaming environment, and they don't do as well as their buddies, their buddies are shouting at their avatar… And for the PT test, if they don't run as fast, we put that into the game… If that avatar is not performing well in the gaming their buddies are beating them up about it," Lynn said. "It is a new paradigm; a new way of thinking, a new way of training and it is pretty exciting."

Avatars are undergoing testing in the Maneuver Center of Excellence and Aviation and Mission Command Center of Excellence and could be deployed across the Army in a matter of months, according to Lynn.

"They have already laid out some of the digital maps for the actual areas that we used in Afghanistan, for example. It's new. It's just now taking off, but the quality is really pretty good… When they assess [recruits] when they come in, just like you get an ID card, you get an avatar, and it is going to look like you," Lynn said.

The Network — Robust, Effective and Secure

The Army is changing the way it supplies network systems and capabilities to operational units by incrementally aligning the delivery of new technology within its defined COE and "Everything over Internet Protocol (EoIP)" strategy. To address the demand for mobile devices at the small unit level, the Army is working with industry to securely bring mobile devices onto the network, according to Lawrence.

"There is no doubt we are going to have millions to billions of sensors in the near future on this network. We are going to have mobile devices on the network and so the key is how we bring them onto it… I'm working with big companies, partners, Apple, Google, different companies, to say that this is what our requirement is going to be. We are testing one device right now that you can embed. It is an iPad-like device that you embed your CAC in and now we have the ability to log on to the network and sign in

"Those are the devices we are going to seek out. We are working with a lot of partners, and I hope we have a decision within this week that the device does work and sign and encrypt. And if that is the case then we are going to put it on the shelves very quickly for our units to be able to procure." (See text box about the 30-Day Tablet Test.)

Because the COE and EoIP are aligned with commercial standards, they can also enable the Army to "commoditize" many portions of the network and possibly lower costs. In this way, the Army will get out of the information technology research and development business, and rely instead on commercial off-the-shelf solutions as much as possible. The easier it is to acquire IT, the faster — and more frequently — the Army can deploy new capabilities in the field.

"A lot of discussion here is on enterprise initiatives and enterprise services, and I applaud them all. And I keep saying the faster we can get to them the better we are," Hernandez said.

"I am comfortable with all the efficiencies that we will gain… I am really more excited about the effectiveness that this will bring to our ability to defend our networks, and the ability to see ourselves, to see the threat, to see the cyber surfing, and now really start getting into a more active defense, the types of defense strategies that the Department of Defense has asked us to look at in its Cyber Security Strategy." CHIPS

30-Day Tablet Test

The Army is conducting a limited 30-day test of Fujitsu Q550 tablets to ensure the tablet meets Army user requirements for a mobile device.

The tablet is running an Army gold master version of Windows 7. If the pilot is successful, the tablet will be available for Army purchase though the Army acquisition vehicle: Computer Hardware, Enterprise Software and Solutions. Any vendor meeting Army requirements can make a device available for Army purchase though CHESS.

Currently, mobile devices are required to: have an Army approved operating system; be able to authenticate to the network; be Common Access Card (CAC)/PKI-enabled to sign and encrypt email; have a FIPS 140-2 certified encryption for data at rest; and have an enterprise management capability to turn off Wi-Fi and enable and disable cameras.

The test is expected to conclude Sept. 30.

DON Enterprise Architecture Supports the DON IM/IT/Cyberspace Campaign Plan

By Victor Ecarma

In May 2011, the Department of the Navy Chief Information Officer released the DON Information Management/Information Technology/Cyberspace Campaign Plan for Fiscal Years 2011-2013. As stated in the campaign plan, "Fiscal realities in the Defense community today and in the anticipated future will not support our continued development and delivery of Information Management (IM), Information Technology (IT) and Information Resources Management (IRM) capabilities as we have in the past." As a result, there are many DON IM/IT/cyberspace efficiency initiatives underway, and the DON enterprise architecture (EA) supports these initiatives.

The DON EA is made up of products that are aligned with the department's business goals and objectives. DON EA compliance became mandatory for all DON IT, including national security systems programs, in October 2009. Through the DON EA compliance, waiver request and review process, the department can determine how well DON strategy and policies are executed by individual DON programs. The most recent release of the DON EA, Version 3.0, contains two products that are directly related to the DON IM/IT/cyberspace efficiency initiative. These two products are focused on assisting with implementing the DON's plans for implementing enterprise software licenses/enterprise software agreements (ESL/ESA) and data center consolidation.

The new DON EA enterprise software licenses/enterprise software agreements product requires all DON programs to make use of the growing list of departmentwide enterprise licenses and agreements when procuring commercial off-the-shelf (COTS) software and hardware. This will allow DON programs, and the department as a whole, to get the best prices possible for COTS software and hardware. In addition, the existing DON EA "COTS Software Fielding" product will support identification of the COTS software applications most frequently used across the department and, therefore, would be good candidates for new enterprise software licenses and agreements.

Another new DON EA v3.0 requirement, the data center consolidation product, ensures DON programs use available data storage capacity at established department enterprise and regional data centers before procuring additional data storage capacity. To this end, the DON CIO issued data center consolidation guidance July 20 establishing a moratorium on the purchase of additional data center capacity.

The memo, "Department of the Navy Data Center Consolidation Policy Guidance," halts all DON investment (to include individual program of record resources) in increased data storage capacity without first determining that existing DON data center capacity is insufficient to meet the storage requirements, and determining it is not more cost effective to expand capacity in an existing DON-owned, Space and Naval Warfare Systems Command, Navy Marine Corps Intranet, or Marine Corps enterprise or regional data center.

As an alternative, qualifying Defense Department or commercial facilities can be used upon completion and approval of a valid business case analysis using the DON standard BCA template. As part of the DON EA compliance assertion process, DON program managers will be asked to verify whether their programs are compliant with this requirement.

As DON IM/IT/cyberspace efficiency efforts continue, the DON EA compliance assessment and review process will continue to be a transparent mechanism for ensuring proper program alignment with the strategies, plans and policies associated with achieving greater departmentwide IM/IT/cyberspace efficiencies.

All authoritative DON EA content, policy, procedures and guidance can be accessed at http://go.usa.gov/1bf. DON Data Center Consolidation Policy Guidance is available from the DON CIO website at www.doncio.navy.mil/PolicyView.aspx?ID=2504. CHIPS

Victor Ecarma provides support to the Department of the Navy enterprise architecture team. Fumie Wingo is the DON enterprise architecture lead.

Department of the Navy Architecture Development Guide Updated

The Department of the Navy Chief Information Officer published the DON Architecture Development Guide (ADG) version 2.0. The ADG, formerly known as the Architecture Product Guide, serves as the overarching guidance for developing and maintaining all architecture models within the department. The ADG incorporates DoD Architecture Framework (DoDAF) v2.0 guidance and provides a number of model examples. It also includes a list of development tasks, style and format tips, as well as best practices gathered from Navy and Marine Corps architecture practitioners. Use of the ADG will enable uniform development and analysis of DoDAF models in support of the requirements identification and acquisition processes.

The DON ADG and other authoritative information about DON EA content, policy and procedures may be downloaded from https://www.intelink.gov/wiki/DONEA.

GOING MOBILE

Telework Driving Demand for Remote Access

By Mike Hernon

The Department of the Navy anticipates that personnel will begin teleworking in significant numbers when a new telework policy is released shortly. As a result, there will be explosive growth in the number of users who need to connect to the Navy Marine Corps Intranet and other government networks from remote locations, primarily from a home office, but also from other locations via cellular or Wi-Fi networks. Understanding the advantages and disadvantages of the technology options available for remote access will allow commands to make more informed decisions as they plan and budget for an increasing number of teleworkers.

While a number of remote access options are available, the network capacity to deliver full desktop functionality from remote locations is limited. Exceeding this capacity could compromise the DON's mission by preventing some personnel from accessing the network entirely or limiting the functionality or level of performance they have available once connected. The new policy guidelines assume teleworkers will be working with unclassified information only.

Provision of Equipment

Government furnished equipment (GFE) is strongly recommended for regular, recurring remote access. Use of GFE guarantees segregation of government information from personal devices and ensures the device meets current DON information assurance standards. Use of GFE also ensures that the appropriate device management controls, such as remote disk wiping, and software, such as antivirus, are present and up-to-date.

GFE includes laptops; BlackBerrys or other smart phones; tablets; and a virtual desktop solution, such as "NMCI on a Stick." An external smart card reader may also be required to support Common Access Card (CAC) login and authentication. However, flash and thumb drives are not authorized for use on GFE.

The use of privately owned equipment, such as a personal computer, is permissible for occasional telework. For regularly recurring telework, privately owned equipment should only be used as a last resort because its use for official business introduces a number of issues that could negatively affect both the government and the employee. Unlike GFE, personal devices cannot be integrated into the network's device management tools. Also, the government cannot ensure that the optimal antivirus software and other security controls are installed on personal devices.

More important, if there is a spillage of classified material on a personal device the government may have the right to confiscate the device and dispose of it (destroying the hard drive) in accordance with guidance regarding the handling of a classified material incident.

Connection Options

Various options exist for connecting remote devices to DON networks. Many devices may be capable of network connectivity through two or more options. Users should be provided with a hierarchy of connection options so that if the preferred method is unavailable, they can try to connect with the next alternative. Thus, when providing a device to a teleworker, commands should also consider the ways in which it will connect to the network and ensure the device is provisioned accordingly.

Web Access. Web access involves using an Internet site, or portal, to connect to a government network through wired or wireless means. Teleworkers can access most unclassified Defense Department and DON CAC-enabled websites through the Internet, but some government sites may only be accessed through a wired connection.

Outlook Web Access. One of the primary telework products for Web access is Microsoft OWA, which provides a version of desktop email, contacts and a calendar application. Some functionality is lost because access to network drives and other peripherals is not available. At the same time, access to OWA is practically unlimited. Another advantage is that OWA may be used on personally owned equipment with the addition of an inexpensive ($12.99) smart card reader.

OWA, used in conjunction with Web portals, is the preferred telework solution for personnel whose remote work can be accomplished without access to network-based services, such as a network drive.

Virtual Private Network (VPN). A VPN provides a secure, encrypted connection to a network from an outside location, normally through the use of a laptop, but also through other devices. A VPN-connected laptop can provide the full range of network functionality that users would experience from their desktop in the office. VPN access can be accomplished through a wired connection, a cellular air card or an approved Wi-Fi connection. However, the number of VPN ports on the network is limited.

Wi-Fi. Most portable devices, such as laptops, smart phones and tablets, come with built-in Wi-Fi wireless capability. However, due to concerns with potential security vulnerabilities, use of Wi-Fi is strictly controlled in the following ways.

Public Hot Spots. A public hot spot is a Wi-Fi offering that is often available at coffee shops, airports and other public places. The only accepted method of connecting to a DON network via a public hot spot is via a GFE laptop with the proper Designated Accrediting Authority approved Wi-Fi hardware and software installed. The use of a device's native Wi-Fi capability is not allowed.

Some of Camp Pendleton's civilian employees will now be able to participate in a new program called Telework. The program extends base civilian workers the opportunity to complete their duties from an alternative location, such as their homes. The base's implementation of Telework was granted through Base Order 12600.1 that was signed by the base's commanding officer, Col. Nicholas F. Marano, March 18, 2011. According to base officials, the program will be especially important during local natural disasters, such as a wildfire, by allowing certain base functions to remain uninterrupted. Photo by Lance Cpl. Mike Atchue.

Home Networks. Use of a home Wi-Fi network to provide the connectivity for telework is allowed. Home networks should be set up in accordance with guidance from the DON Chief Information Officer and/or the National Security Agency.

Cellular/Mobile Networks. BlackBerrys, and other approved GFE smart phones and tablets, generally connect through a commercial cellular network as the primary link to the network. Some BlackBerrys also support tethering, which is connecting a laptop to the device for Internet access instead of using an air card. The monthly fee for tethering is about 75 percent less than the cost of an air card and should be used when available.

U.S. cellular providers are generally considered to provide a secure, encrypted connection that supports remote access. Some foreign cellular networks are considered "unsecure" and should not be used. Consult with your local information assurance manager (IAM) or security officer for up-to-date travel guidance whenever taking a cellular, or any wireless device, outside the continental United States.

Telework IT Strategy

When developing a telework strategy, commands must consider the various IT options available, personnel, job requirements and associated costs. Because new devices are frequently released into the marketplace and tested for network compatibility, commands are strongly urged to consult with their IAM and command information officer when devising or assessing a telework strategy. These individuals will have the most current information on all IT options.

Command IOs will also ensure that all GFE devices are configured to support telework in accordance with all applicable DON and DoD IT policies. Command IOs will also provide training as required to teleworkers on the various connectivity options available to them, including selecting the optimal network operations center when VPN access is used.

Online Resources

The following websites contain recent information on topics of interest to teleworkers. Because new mobile and remote access solutions continue to be tested these sites should be consulted regularly for the latest options. CHIPS

- NMCI Remote Access Options:
  https://www.homeport.navy.mil/home/
- DoD Telework:
  www.cpms.osd.mil/telework/telework_index.aspx
- DON CIO: www.doncio.navy.mil/
- DON Policy Issuances
  http://doni.daps.dla.mil/default.aspx
- DoD Policy Issuances
  www.dtic.mil/whs/directives/

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

Human Presence Detection

The Navy has tri-service responsibility for EOD-related science and technology development

By Ann Dakis

The ability of man-portable robots to effectively address life-threatening hazards like improvised explosive devices (IEDs) on the battlefield has led to widespread user acceptance and fielding in explosive ordnance disposal (EOD) missions. The Navy has tri-service responsibility for EOD-related science and technology development, and the Space and Naval Warfare Systems Center Pacific supports the naval EOD technology division of the Naval Sea Systems Command in the execution of this tasking.

"Today's warfighter considers the robot an asset, since it saves lives, but at the same time, the current operator control unit is perceived as a liability," said Bart Everett, SSC Pacific's technical director for robotics. "From a command and control perspective, the need to teleoperate these systems severely limits their applicability in missions other than EOD."

Teleoperating a robot is extremely fatiguing, and control equipment is too heavy and cumbersome for extended dismounted operations. In addition, the operator becomes fully immersed in directing such a vehicle at the expense of his or her situational awareness, which can be extremely dangerous under battlefield conditions.

Range and line-of-sight restrictions of radio links further complicate the problem, and when communications are lost, the mission is effectively over, and the asset must be manually retrieved.

For these reasons, SSC Pacific's unmanned systems branch is heavily focused on making a robot a more intelligent and effective asset, and the operator control unit less of a liability. According to Everett, "The ultimate goal is to eliminate the need for a robot-specific controller altogether."

Smarter robots and a reduced control burden will expand the use of unmanned systems across a much broader spectrum of military operations than just EOD. The branch has already made significant progress toward these goals in the past few years.

Figure 1. Fused sensor solutions, such as color and thermal imagery, are used to detect and track humans. The image on the left shows a thermal image overlaid directly on a color image. Regions which are likely to correspond to human skin or thermal signature are highlighted in the fused image on the right.

The Autonomous Robotic Mapping System (ARMS), for example, can automatically explore an unknown or hostile environment while building a highly accurate and detailed map. A scanning laser rangefinder measures distance to all surrounding objects within a 360-degree field of view, and stereo cameras assist with three-dimensional rendering. No human guidance is necessary, other than initial high level direction telling the robot where to search.

"Current efforts include optimizing and testing these autonomous exploration and mapping behaviors in urban environments with multiple buildings and varying terrain," said Estrellina Pacis Rius, project manager of the urban environment exploration (UrbEE) project. "It is projected that future conflicts will increasingly occur in urban settings, so we are evaluating realistic use of these robots to support dismounted troops operating in such areas."

For example, urban settings pose challenges for line-of-sight communications and GPS dependent navigation. If radio communication with the warfighter is lost, UrbEE developed behaviors enable a robot to complete its search-and-map mission and return to the starting point to upload the results.

Another UrbEE capability includes adaptive position estimation, which allows the robot to maintain accurate knowledge of its position and location without GPS.

Having a freshly generated floor plan of a previously unknown structure is a huge advantage, but if warfighters then have to enter the space, it is very important for them to know of any hazards. The robot must detect objects of tactical significance and annotate such on the map.

"When you ask warfighters for a prioritized list of what they want to know about… the No. 1 answer is always human presence," Everett said. "From a detection standpoint, humans have two obvious characteristics that can be exploited, in that we move around and we give off heat."

Inexpensive passive-infrared (PIR) motion sensors, or pyroelectric sensors, like those commonly used for home lighting control, exploit both these features. In home systems, to make a sensor that can detect a human being, it must be sensitive to the temperature of a human body. Humans have a skin temperature of about 93 degrees Fahrenheit, and radiate infrared energy with a wavelength between 9 and 10 micrometers. Therefore, the sensors are typically sensitive in the range of 8 to 12 micrometers.

Fused sensor solutions, such as color and thermal imagery, are used to detect and track humans. In Figure 1, the image on the left shows a thermal image overlaid directly on a color image. Regions

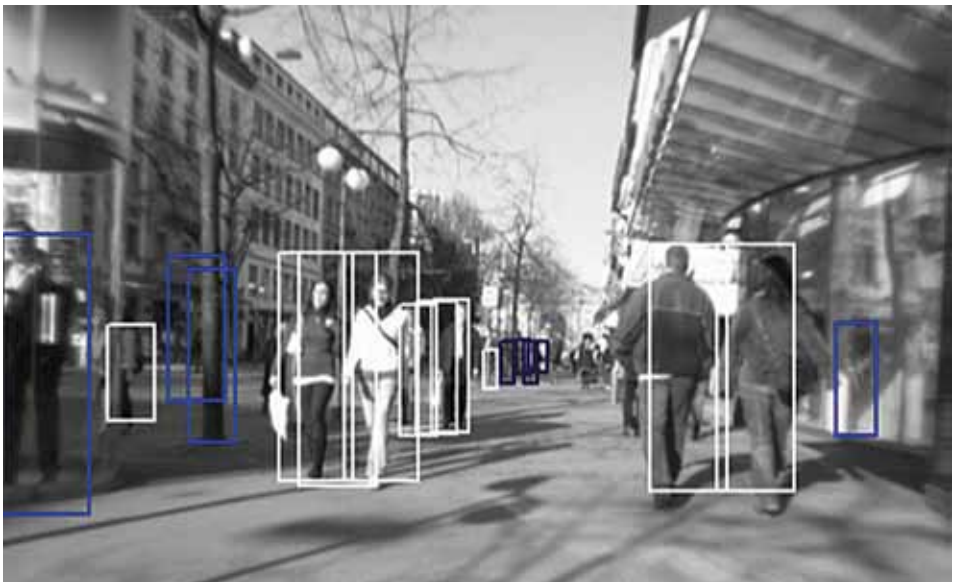


Figure 2. An example of urban test data illustrating rejected false positives (blue boxes) and accepted positives (white).

which are likely to correspond to human skin or thermal signature are highlighted in the fused image on the right.

The first robot to successfully demonstrate such a static motion detection capability was ROBART I, which was Everett's 1981 thesis project at the Naval Postgraduate School. ROBART I used a combination of infrared, optical, acoustical and vibration sensors. This research prototype laid the framework for subsequent robotic security efforts at SSC Pacific, and motion detection from stationary vehicles is now a common and mature technology.

"The fundamental problem is fairly obvious," Everett said. "If the robot is standing still, anything that moves could potentially be a human. But once the robot itself starts to move, everything its sensors 'see' appears in motion, and so this simplistic algorithm becomes ineffective."

This challenge is further complicated by the fact that the very nature of mobility introduces constantly changing variables that alter the physical relationships between a moving platform and its surroundings.

"To address these issues, we employ two-stage sensor fusion," Everett said. "The first stage uses a scanning laser to detect changes in range data, while the second stage processes thermal imagery to verify any potential human presence."

These complementary sensors have non-overlapping strengths and weaknesses that can more reliably detect an intruder from a moving platform, while minimizing the number of false and nuisance alarms. Figure 2 illustrates the power of new algorithms to detect false positives in human presence detection.

After the robot builds a map of the area of interest, it can then detect anomalies in the environment and mark the locations on a map with an icon indicating a potential human presence. An operator can then click on the icon to view more detailed information to confirm whether it is a human presence or not. An example is shown in Figure 3.

On the battlefield, however, a robot must also be able to detect people that are not moving, and may in fact be hiding or otherwise occluded. Rius, who also oversees the human presence detection project, has been leading a team in developing such a capability since 2008 for tactical purposes and for safe operation near pedestrians.

Collaborative work with Sarnoff Corp. (now SRI International) has been ongoing for the past three years to develop a compact, fused visual and thermal stereo camera payload optimized for detecting occluded individuals. The same payload can be used to follow a person's movements.

SSC Pacific scientists and engineers continue to advance robotic technology and artificial intelligence.

According to lead project engineer Greg Kogut, "There is increasing demand from dismounted Navy and Marine Corps warfighters for a leader-follower behavior for small-to-medium sized robotic vehicles. This scenario involves a robot following a particular human like a well-trained dog would do, while avoiding other people who might get in the way. Our human presence detection projects allow us to demonstrate meaningful progress towards such a capability." CHIPS

Follow SPAWAR on Facebook:
www.facebook.com/
spaceandnavalwarfaresystemscommand.

Ann Dakis is a staff writer in the public affairs office of SSC Pacific.

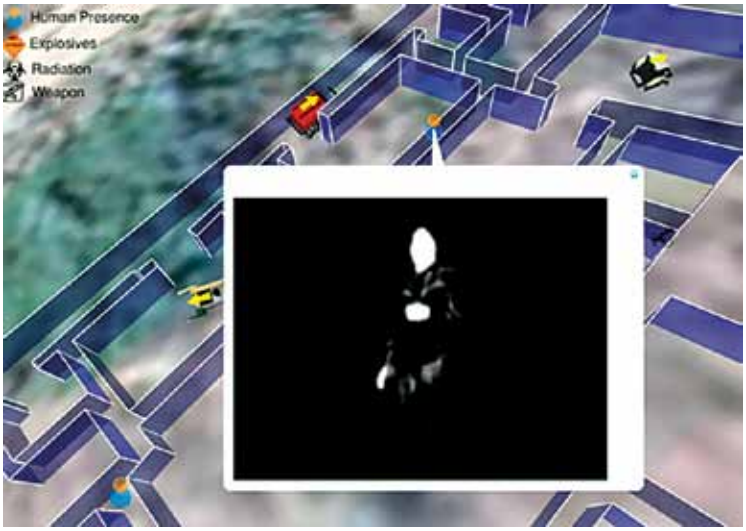


Figure 3. After a robot builds a map of the area of interest, it can then detect anomalies in the environment and mark the locations on a map with an icon indicating a potential human presence. An operator can then click on the icon to view more detailed information to confirm whether a human is present.

Ensuring Your Solicitation is Section 508 Compliant

By Sherrian Finneran

Since 1998, when Congress amended the Rehabilitation Act, all federal agencies, including the Department of Defense, are required to make electronic and information technology (E&IT) accessible to individuals with disabilities. The law applies to all federal agencies when they develop, procure, maintain, or use electronic and information technology.

Accessible E&IT includes technologies that allow those who are blind or visually impaired to easily obtain information on websites and participate in online training. Exceptions to compliance are identified by the Federal Acquisition Regulation (FAR), part 1194, as detailed below.

In June 2011, the Department of Defense Chief Information Officer published DoD Manual, 8400.01-M, "Procedures for Ensuring the Accessibility of Electronic and Information Technology (E&IT) Procured by DoD Organizations." The manual, available at www.dtic.mil/whs/directives/corres/pdf/840001m.pdf, assigns responsibilities and provides procedures for implementing Section 508 requirements.

The manual provides guidance to requiring officials, purchasers and requesters to ensure that their acquisition meets U.S. Access Board accessibility standards unless a FAR exception applies. Requiring officials must conduct market research to find products or services that meet the standards. Market research results must be attached to the purchase request or, in the case of a contract for services, the statement of work (SOW). Requiring officials must also include draft technical specifications, minimum requirements and a statement of applicable U.S. Access Board standards. If it applies, officials must include a statement documenting non-availability of

accessible products or services, or include a statement that meeting accessibility requirements causes an undue burden for the agency.

Contracting officers or procurement officials are instructed to review SOWs and purchase requests to ensure that Section 508 requirements are properly addressed and that applicable documents are provided by the requiring office.

Accessible E&IT includes technologies that allow those who are blind or visually impaired to easily obtain information on websites and participate in online training.

In July 2010, the Office of Management and Budget issued a memo, "Improving the Accessibility of Government Information," directing agencies to take stronger steps toward improving the acquisition and implementation of accessible technology. The memo, available from www.whitehouse.gov/sites/default/files/omb/assets/procurement_memo/improving_accessibility_gov_info_07192010.pdf, directed the General Services Administration (GSA) Office of Governmentwide Policy to review solicitations posted on the federal business opportunities website, FedBizOpps.gov, for compliance with Section 508 and to report the results of the reviews quarterly to OMB beginning fiscal year 2011.

GSA is also directed to provide review results to applicable agencies. Since that time, GSA sends emails to agencies either congratulating them for a job well done or providing them with opportunities to improve their solicitations for compliance with Section 508.

There are a number of resources to assist agencies in their compliance with Section 508. As part of its statutory requirement, GSA provides technical assistance to agencies on Section 508 implementation. GSA created a number of tools, available at www.Section508.gov, to help agencies develop accessible requirements, test the acceptance process, and share lessons learned and best practices.

Users may also access training by clicking the 508 Universe Training link, www.section508.gov/index.cfm?FuseAction=RegisterUniverse, which provides multiple courses on how to develop accessible Web pages, as well as compliant solicitations. In addition, the website includes answers to frequently asked questions about acquisition.

The Buy Accessible Wizard tool (www.buyaccessible.gov) assists government personnel in completing the market research necessary to ensure they are buying the most accessible IT products and services available. Users are able to search the site, using Quick Links, by specific product or service type and see all the vendors who have provided links to their Section 508 compliant products. These same links may be used to access government product/service accessibility templates.

The tool also produces suggested solicitation language tailored to specific E&IT deliverables that may be used in procurement documentation. Training for the Buy Accessible Wizard is available in the Section 508 Universe Training section of the Section508.gov website. The Quick Links site, located at https://app.buyaccessible.gov/baw/Quick-Links/index.jsp, provides quick and easy pre-packaged Section 508 documentation.

Finally, the U.S. Access Board website, www.access-board.gov, provides additional resources to assist agencies in ensuring compliance with Section 508 accessibility requirements. CHIPS

Sherrian Finneran is the DON Section 508 coordinator.

Federal Acquisition Regulation Exceptions:

Unless an exception of FAR 39.204 applies, acquisitions of E&IT supplies and services must meet the applicable accessibility standards of 36 CFR part 1194. The exceptions in 39.204 include:

- Micro purchases, prior to Jan. 1, 2003. However, for micro purchases, contracting officers and other individuals designated in accordance with 1.603 3 are strongly encouraged to comply with the applicable accessibility standards to the maximum extent practicable;
- E&IT for a national security system;
- E&IT acquired by a contractor incidental to a contract;
- E&IT located in spaces frequented only by service personnel for maintenance, repair or occasional monitoring of equipment; and
- E&IT that would impose an undue burden on the agency.

For additional information regarding exceptions visit www.section508.gov.

Responding at the Speed of Change — NCTS Sicily Supports Operation Odyssey Dawn and Operation Unified Protector

By Cmdr. Bruce Black and Cmdr. M. Barry Tanner

International military operations in Libya began March 19, 2011, after the United Nations authorized action to protect Libyan civilians from attacks by government forces. NATO took over the mission March 31, but the United States continues to provide aircraft and warships off the coast.

In any operation, the rapid and accurate flow of information is critical to success. As soon as Naval Air Station Sigonella began preparing to support what would become Operation Odyssey Dawn, the U.S. part in the intervention, the staff of Naval Computer and Telecommunications Station (NCTS) Sicily immediately began planning to support the increased demands that would soon be placed on the information technology resources of the base. It quickly became clear that requirements for support would change rapidly, and that flexibility and adaptability were the key elements critical for success.

As first Operation Odyssey Dawn, and then, under NATO command, Operation Unified Protector, evolved, this flexibility would be needed time and again to ensure mission critical information was available to U.S. operational and support personnel, as well as coalition partners.

In the words of Capt. Scott Butler, commanding officer of NAS Sigonella, NCTS Sicily personnel demonstrated "complete and utter commitment to the mission" as they executed their support to U.S. and coalition partners alike.

One of the unique aspects to the operation as it unfolded was the rapid pace at which the overall situation changed. Very little about either operations Odyssey Dawn or Unified Protector was done using traditional planning vehicles such as operational orders or fragmentary orders. The primary method for receiving new requirements and changes to the existing plan was via email and text message. Knowing this, the staff at NCTS Sicily "leaned forward" and ensured that the infrastructure and resources needed to get the voice, video and data messages to the right people were ready at all times. According to Butler, without the support of the information professionals at NCTS Sicily, operations would simply have failed to meet the needs of the operational elements based at NAS Sigonella.

Because NCTS has several officer and enlisted information professionals that were veterans of multiple deployments, at sea and ashore, they were able to leverage lessons learned and apply them to what they guessed the "problem would be tomorrow."

Working with joint and coalition partners proved to be the same in Sigonella as it was in the Northern Arabian Sea or in Afghanistan. It was an environment that had the same information sharing challenges that could be overcome by coordinating, cooperating and communicating.

Keeping flexibility in mind, the team ensured that network infrastructure could be rapidly reconfigured as requirements changed. Additionally, with coalition partners occupying spaces, the team ensured that both U.S. and coalition networks were available for connection to the building and could be moved quickly as the spaces were reorganized. This infrastructure included the installation of new fiber throughout the building together with rapidly configurable switches that are capable of connecting to multiple coalition networks, such as the Combined Enterprise Regional Information Exchange System (CENTRIXS), Battlefield Information, Collection and Exploitation System (BICES), NATO Secret Wide Area Network (NSWAN), Crisis Response Operations in NATO Open Systems (CRONOS) and more.

Additionally, the team configured the building network to connect to commercially provided Asymmetric Digital Subscriber Lines (ADSL) to accommodate those coalition partners that could not have access to NATO networks. Finally, the team ensured that the network switches and routers were capable of being rapidly swapped out ensuring that the right services could be provided when tenant spaces were reconfigured or new tenants arrived.

This forward thinking approach proved pivotal as building 407 became the home for no fewer than six separate coalition partners from both NATO and non-NATO nations, including Denmark, Sweden, Turkey, Canada, France and the United Arab Emirates. Because the infrastructure had been designed for flexibility, NCTS was able to provide the full spectrum of information services including voice, data and video on NATO and non-NATO networks to all the tenants on demand, ensuring no gaps in mission capability.

Although operations Odyssey Dawn and Unified Protector presented a number of unanticipated challenges, for one command at NAS Sigonella that is supported by NCTS Sicily, operations proceeded exactly as expected. Commander, Task Force 67 coordinates and manages maritime patrol aircraft in support of Commander Naval Forces Europe and Africa.

Additionally, CTF-67 is the U.S. component for the overall maritime patrol aircraft mission for NATO. In this role, CTF-67 conducts annual exercises with NATO partners to ensure they practice all elements of potential coalition operations. One key element of the exercises is command and control, directly supported by the tactical support communications (TSCOMM) element of NCTS Sicily, embedded with CTF-67. As a result of the lessons learned from these exercises, TSCOMM personnel were

NCTS Sicily technician responded rapidly to ensure Naval Air Station Sigonella infrastructure remains ready to support mission requirements.

prepared to support the rapid stand up of operational support to multiple NATO partners and did so without any interruption in services.

In the words of Cmdr. Jeff Mullen, chief staff officer for CTF-67, "We had zero issues with command, control or communications support as we ramped up for these operations. Everything worked exactly as we practiced, and that's a testament to the professional approach that these Sailors bring to their mission every day, not just when operational tempo increases."

Practicing for rapidly changing operational missions with multiple coalition partners was critical in ensuring seamless support when the real operation began.

Another example of how planning for change resulted in mission success was the support NCTS provided to one of the largest information consumers of the operation, the EC-130-J Commando Solo aircraft from the 193rd Special Operations Wing of the Pennsylvania Air National Guard supporting electronic warfare missions over Libya.

The EC-130-J is a specially-modified four-engine Hercules transport, conducting information operations, psychological operations and civil affairs broadcasts in AM, FM, high frequency, television and military communications bands.

The nature of the EC-130-J mission presents unique connectivity requirements for planners and support personnel, but NCTS Sailors were ready from the moment the unit arrived, providing connectivity to mission critical systems and ensuring that the unit had all the necessary resources to effectively execute its tasking, including access to U.S. SIPRNET, NIPRNET, BICES and NATO secret networks. Even as plans changed and the unit's support crews were moved from one building to another, the flexible approach NCTS used ensured that there was no loss of service or impact to mission operations. Technicians were on the ground connecting equipment and configuring workspaces so that the EC-130-J team could focus on its mission and not worry about connectivity. In the words of Lt. Col. Bill Harris, local commander for the EC-130-J detachment, "It all just worked; we didn't have to worry about a thing."

Perhaps the most unique solution created by the NCTS team dealt with providing services to non-NATO coalition partners. Since these units are not permitted access to coalition networks for security reasons, the team had to find a way to provide them with connectivity that was not dependent on U.S. or NATO networks. To solve this problem, the team created a connectivity suite using open source Linux operating systems coupled with ADSL connections from a local provider. This package provided units from the United Arab Emirates, and other non-NATO partners, with the connectivity they needed to stay in touch with their higher headquarters, as well as receive direct information from the coalition through approved channels. Without this "out-of-the-box" solution, non-NATO partners would have been isolated from their chain of command, resulting in long delays in mission planning and execution.

The best way to describe the environment at NAS Sigonella would be one that is volatile, uncertain, complex and ambiguous. Uncertainty and the change it causes are simply the norm, calling to mind the classic phrase "If you don't like how things are going, wait five minutes, it will change." The inclusion of coalition forces within these operations added to the complexity of the information environment, making it more critical than ever to be ready for every possible situation when it came to information management, command and control, and information security. By leaning forward and anticipating this situation, the staff at NCTS Sicily ensured that operational elements had the resources they needed, from crypto, Iridium satellite phones, BlackBerrys, computers and printers — to U.S. and coalition network access.

In 2008, the Chairman of the Joint Chiefs of Staff Adm. Mike Mullen said that he needed his Joint Staff to "respond at the speed my job requires, not at the speed a particular process allows."

During Operation Odyssey Dawn and continuing through Operation Unified Protector, the staff of NCTS Sicily continues to demonstrate this principle by "responding at the speed of change" and establishing a best practice for how to effectively execute information management, information security, and information technology service support for future coalition operations. CHIPS

OAK HARBOR, Wash. (July 9, 2011) EA-18G Growlers assigned to the Scorpions of Electronic Attack Squadron (VAQ) 132 perform a fly-by during a homecoming ceremony at Naval Air Station Whidbey Island following an eight-month expeditionary deployment supporting Operation New Dawn and Operations Odyssey Dawn and Unified Protector. VAQ-132 protected numerous U.S. and Coalition military assets and personnel in the U.S. Central Command and U.S. European Command areas of responsibility. U.S. Navy photo by Mass Communication Specialist 2nd Class Nardel Gervacio.

Cmdr. Bruce Black is an information professional officer and the commanding officer of NCTS Sicily.

Cmdr. M. Barry Tanner is a Navy Reserve information professional officer assigned to the Navy Reserve Navy Cyber Forces headquarters unit, currently supporting NCTS Sicily and multiple European regional naval communications units.

Trident Warrior 2011

Demonstrating cooperative autonomy in Navy unmanned systems

By Emily Doll

In its ninth year of execution, Trident Warrior 2011 (TW11) lived up to its reputation for robust experimentation using complex real-world scenarios. TW experiments are designed to fast-track the introduction of new capabilities, innovative technologies, and tactics, techniques and procedures (TTPs) to aid maritime forces in the full range of warfare — air, land, sea and cyber.

Directed by U.S. Fleet Forces Command (USFF), TW11 featured at-sea experimentation of more than 50 critical maritime initiatives. Joining in TW11 were participants from USFF, U.S. 2nd Fleet and 5th Fleet, program executive offices, Navy systems commands, the Naval Postgraduate School, academic and industry partners, and multiple ships and aircraft from the U.S. Navy and Air Force. Multinational participants included Australia, Canada, New Zealand, the United Kingdom and France.

TW temporarily deployed advanced capabilities on ships to collect real-world performance data and feedback from fleet users during the underway experimentation period. Data collected throughout the experiment is provided to Navy decision makers as recommendations regarding future capability investments for the fleet. The main U.S. event began July 18 and concluded August 1.

On July 20, 2011, CHIPS staff took part in a demonstration of unmanned surface vehicles (USV) performing interdiction operations. The demo, led by Capt. Carl "Carlos" Conti, USFF director of fleet experimentation, was conducted in a 3,600-meter area off the shores of Fort Monroe, Va.

FORT MONROE, Va. (July 20, 2011) Autonomous Maritime Navigation 1 (AMN1) and Autonomous Maritime Navigation 2 (AMN2) patrol for intruders during Trident Warrior 2011. The experimental boat can operate autonomously or by remote. The Trident Warrior experiment, directed by U.S. Fleet Forces Command, temporarily deploys advanced capabilities on ships to collect real-world data and feedback during an underway experimentation period. U.S. Navy photo by Mass Communication Specialist Seaman Scott Youngblood.

Any Vessel Can Be a USV

Full autonomous capabilities for a USV are portable to any maritime vehicle and are enabled by a multipurpose sensor system. Autonomous Maritime Navigation (AMN), sponsored by Naval Surface Warfare Center, Carderock Division (NSWCCD), has been in development since 2006. During Trident Warrior, four boats, performing as USVs, were used in a force protection mission experiment, utilizing the AMN "brain" to perform cooperative autonomous behaviors within oil platform force protection scenarios. The AMN brain is an adaption of the NASA Jet Propulsion Laboratory's Mars Rover autonomy software, used in its "Opportunity" and "Spirit" robots.

The USVs were programmed to protect a specific area by creating a diversion between the position they defend and a perceived threat.

The USVs were equipped with multiple sensors and could share their individual surface picture to intercept intruders based on their combined situational picture. AMN has the ability to employ "sliding" autonomy, where it can operate in either fully autonomous mode (independent of humans) or in remote control (human in the loop). The capability allows a command center to monitor multiple USVs simultaneously while letting them perform as intelligence, surveillance and reconnaissance (ISR) collectors and intruder interceptors with no human intervention.

Two of the boats that were used are government owned from NSWCCD, one USV is a Northrop Grumman 11-meter-long rigid hull inflatable boat, and the fourth boat is a commercial vessel from Textron/AAI Corp., called Common USV. The Office of Naval Research, Defense Advanced Research Projects Agency and Office of the Secretary of Defense are sponsors in USV development.

Another component of the experiment aimed to determine if the USVs can operate with unmanned underwater and air vehicles. Collision avoidance and maritime regulations are the next

VIRGINIA BEACH, Va. (July 20, 2011) Information Systems Technician 2nd Class Michael Smith, left, assigned to Riverine Squadron (RIVRON) 3, Operations Specialist 2nd Class Denise Sanders, assigned to Expeditionary Training Group, and Operations Specialist 1st Class Robert McGill, assigned to Navy Expeditionary Combat Command, test communications equipment during Trident Warrior 2011 at Joint Expeditionary Base Little Creek-Fort Story. Trident Warrior is an annual fleet experiment focusing on new technology. U.S. Navy photo by Mass Communication Specialist 2nd Class Steven Hoskins.

frontier the USVs are tackling; they are programmed to automatically sense and avoid obstacles.

Capt. Conti explained that the most surprising aspect of the advancing technology is the "cooperation" displayed between the USVs. In a similar experiment conducted last year in San Diego, two boats had faulty equipment, but the sensors on board allowed the boats to self-identify the failures, he said.

"One of the boat's radar was broken, and all of the other boats 'knew' that because the boat that had the broken element said, 'I'm broken.' In response, the other boats provided radar information to the crippled vessel. Likewise, another boat self-identified that one of its engines was disabled, and the other boats came to its rescue," Conti said. "They (USVs) did it all by themselves. To me that's very exciting when you have that kind of brain power on board these computers. It's revolutionary."

Non-lethal Weapons

During the USV demonstration, NSWCCD's Guardian Fast Patrol Craft challenged the unmanned boats by entering a protected area. Using a long-range acoustic device (LRAD), one unmanned boat transmitted an oral warning through a loudspeaker cautioning the patrol craft that its intentions were unclear and it should not proceed.

Loudspeaker warnings, or acoustic hailing devices, optical distracters and other non-lethal systems are incredibly effective in extending the battlespace by increasing the distance between a Navy ship and suspect vessel. The warning buys the commanding officer precious distance and time to assess the intent of an approaching vessel.

Non-lethal capabilities enable operational forces to effectively deter potentially dangerous individuals at increased distances, stop suspicious vehicles or vessels, and render enemy assets inoperable with few or no unintended casualties.

"In another spiral we are going to look at other non-lethal weapons for the vehicles besides LRADs that include: dazzlers, louder noises, [and] flashbang grenades, like those the Special Forces guys use. You shoot a couple of those out there and then you really make your intentions clear," Conti said.

LRADs and other acoustic hailing devices, produce focused, directional sound beams that project attention-getting, highly irritating tones intended to deter or modify an individual's behavior. This capability assists warfighters in determining intent at a safe distance and can potentially deter an individual prior to escalating to lethal force.

Flashbang grenades temporally neutralize the combat effectiveness of enemies by disorienting their senses. The flash of light momentarily activates all light sensitive cells in the eye, making vision impossible for approximately five seconds until the eye restores itself to its normal, unstimulated state. The incredibly loud blast produced by the grenade adds to its incapacitating properties by disturbing the fluid in the ear.

Within irregular warfare environments, non-lethal capabilities can be valuable in enabling warfighters to tailor their responses to complex, threatening situations more precisely and appropriately when reduction of civilian casualties is essential to mission accomplishment. In addition, use of non-lethal weapons may help avoid destruction of culturally significant structures, or critical infrastructure, such as oil platforms.

USV Development

Research programs are focused on developing mission-level autonomy, perception-guided maneuvers and unmanned surface behaviors in more complex environments. This effort involves developing high-reliability sense-and-avoid algorithms to conduct coordinated and cooperative operations between multiple USVs and to further the development of autonomous systems for real-world operational employment.

The command and control of the USVs varies from fully autonomous to remote control. If a threat persists beyond the initial warning to retreat, an operator in the control room has the power to gain control of the USV at any time and then release it back to its own control/mission when appropriate.

The obvious scenario that would require the control room to gain access of the USV through a man in the loop intervention would involve the deployment of non-lethal and lethal weapon assaults. The ability to use force against an enemy without concern for loss of human life is an incredible advantage of the USVs, said an enthusiastic Conti.

"You have an unmanned boat that may get damaged or even sink, but that's OK, we protected our guys from getting hurt — and that's a big part of this.

"Our mission is to make this unnerving, and if we can make an enemy think twice about coming anywhere near us because of technology like this then we are doing our job." CHIPS

Visit Trident Warrior on Facebook at www.facebook.com/tridentwarrior.

Emily Doll is a computer scientist student who completed a summer internship at SPAWARSYSCEN Atlantic.

CHIPS senior editor Sharon Anderson contributed to this article.

Enterprise Software Agreements

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

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

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

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

Software Categories for ESI:

Asset Discovery Tools

Belarc

BelManage Asset Management – Provides software, maintenance and services.

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

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

Ordering Expires: 28 Mar 12

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: 17 Sep 12

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

Database Management Tools

Microsoft Products

Microsoft Database Products – See information under Office Systems on page 61.

Oracle (DEAL-O)

Oracle Products – Provides Oracle database and application software licenses, support, training and consulting services. The Navy Enterprise License Agreement is for database licenses for Navy customers. Contact the Navy project manager on page 62.

Contractors:

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

DLT Solutions (W91QUZ-06-A-0002); (703) 708-8979

immixTechnology, Inc. (W91QUZ-08-A-0001); Small Business; (703) 752-0628

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

Affigent, LLC (W91QUZ-09-A-0001); Small Business; (571) 323-5584

Ordering Expires:

Oracle: 28 Mar 12
DLT: 01 Apr 13
immixTechnology: 02 Mar 16
Mythics: 18 Dec 11 (Please call for extension information.)
TKCIS: 9 Nov 11 (Please call for extension information.)

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 66 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

Ordering Expires: 24 Sep 12

Web Links:

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

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; (703) 752-0641 or (703) 752-0646

Ordering Expires: 02 Mar 16

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

VMware

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

Contractor: *Carahsoft Inc.* (W91QUZ-09-A-0003)

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

Ordering Expires: 27 Mar 14

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

Enterprise Management

CA Enterprise Management Software (C-EMS2)

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

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

Ordering Expires: 22 Sep 12

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

Microsoft Premier Support Services (MPS-2)

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

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

Ordering Expires: 31 Mar 12

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

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) 820-4889

DLT Solutions (W91QUZ-06-A-0004); (703) 708-9127
Ordering Expires:
Quest: 29 Dec 15
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 58.*

RWD Technologies

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

SAP

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

Information Assurance Tools

Data at Rest (DAR) BPAs offered through ESI/SmartBUY

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

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

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

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

The Department of the Army issued an enterprise solution for Army users purchasing DAR software. See the information provided on the Army CHESS website at https://chess.army.mil/ascp/commerce/index.jsp. As of this printing, the Air Force has not yet provided a DAR solution.

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

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: 08 Sep 12
Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

Xacta

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

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

Lean Six Sigma Tools

iGrafx Business Process Analysis Tools

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

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

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

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

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

Ordering Expires: 31 Jan 14

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

Minitab

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

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

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

Ordering Expires: 07 May 13

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

PowerSteering

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

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

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

Ordering Expires: 14 Aug 13

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

Office Systems

Adobe Desktop Products

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

Contractors:

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

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

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

Insight Public Sector, Inc. (N00104-08-A-ZF36); (443) 534-6457

Ordering Expires: 30 Jun 12

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

Adobe Server Products

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

Contractor:

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

Ordering Expires: 14 Jan 14

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

Microsoft Products

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

Contractors:

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

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

GovConnection (N00104-10-A-ZF30); (301) 340-3412

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

Hewlett-Packard (N00104-02-A-ZE80); (845) 337-6260

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

SHI (N00104-02-A-ZE86); (800) 527-6389 or (732) 564-8333

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

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

Ordering Expires: 31 Mar 13

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

Red Hat/Netscape/Firefox

Through negotiations with August Schell Enterprises, DISA has established a DoD-wide enterprise site license whereby DISA can provide ongoing support and maintenance for the Red Hat Security Solution server products that are at the core of the Department of Defense's Public Key Infrastructure (PKI). The Red Hat Security Solution includes the following products: Red Hat Certificate System and dependencies; Red Hat Directory Server; Enterprise Web Server (previously Netscape Enterprise Server); and Red Hat Fortitude Server (replacing Enterprise Server). August Schell also provides a download site that, in addition to the Red Hat products, also allows for downloading DISA-approved versions of the following browser products: Firefox Browser; Netscape Browser; Netscape Communicator; and Personal Security Manager. The Red Hat products and services provided through the download site are for exclusive use in the following licensed community: (1) All components of the U.S. Department of Defense and supported

organizations that utilize the Joint Worldwide Intelligence Communications System, and (2) All non-DoD employees (e.g., contractors, volunteers, allies) on-site at the U.S. Department of Defense and those not on-site but using equipment furnished by the U.S. Department of Defense (GFE) in support of initiatives which are funded by the U.S. Department of Defense.

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

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

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

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

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

Download Site: http://redhat.augustschell.com
Ordering Expires: Please call (703) 882-1636 for information about follow-on contract.
All downloads provided at no cost.

Web Link: www.disa.mil

Red Hat Linux

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

Contractors:
Carahsoft Technology Corporation (HC1028-09-A-2004)
DLT Solutions, Inc. (HC1028-09-A-2003)
Ordering Expires:
Carahsoft: 09 Feb 14
DLT Solutions, Inc.: 17 Feb 14
Web Link: www.esi.mil

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: 30 June 11 (Please call for information about follow-on contract.)
Project Management:
Jonnice Medley (301) 225-8081 (DSN 375) (jonnice.medley@disa.mil)
Web Link: www.disa.mil/contracts/guide/bpa/bpa_sun.html

Research and Advisory BPA

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

Gartner Group (N00104-07-A-ZF30); (703) 378-5697; Awarded Dec. 1, 2006
Ordering Expires: Effective for term of GSA contract
Authorized Users: All DoD components. For the purpose of this agreement, DoD components include: the Office of the Secretary of Defense; U.S. Military Departments; the Chairman of the Joint Chiefs of Staff; Combatant Commands; the Department of Defense Office of Inspector General; Defense Agencies; DoD Field Activities; the U.S. Coast Guard; NATO; the Intelligence Community and Foreign Military Sales with a letter of authorization. This BPA is also open to DoD contractors authorized in accordance with the FAR Part 51.
Web Link: www.esi.mil/contentview.aspx?id=171&type=2

Department of the Navy Agreement

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

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

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

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

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

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

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

CONTACT THE SOFTWARE PRODUCT MANAGERS BELOW FOR ASSISTANCE

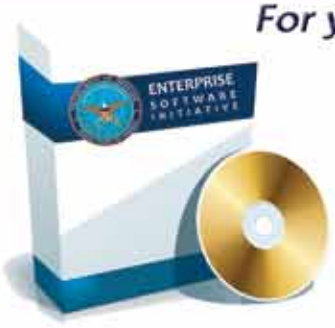
Program Manager
Susan Ellison

Oracle (DEAL-O) Navy Project Management
Jeffrey Ho

Microsoft Products
LaToya Lowery

iGrafx, Research and Advisory BPA, SAP
Nina Diep

Adobe Desktop Products, Adobe Server Products, Enterprise Application Integration, Sun Software Minitab, PowerSteering, RWD Technologies
Thao Vu



For your convenience all enterprise contract information is consolidated under

www.esi.mil

www.doncio.navy.mil/chips

www.doncio.navy.mil

ENTERPRISE COST $AVINGS ARE JUST A CLICK AWAY

JOIN US AT THE DEPARTMENT OF THE NAVY

IT CONFERENCE

JAN. 23-26, 2012

AT THE SAN DIEGO CONVENTION CENTER

NOTE:

JAN. 23 CONFERENCE SESSIONS ARE LIMITED IN SCOPE TO KNOWLEDGE MANAGEMENT ONLY.

REGISTER NOW AT:

HTTP://WWW.DONCIO.NAVY.MIL/EVENTS.ASPX