
Fall 2003
CHIPS
magazine
Dedicated to Sharing Information - Technology - Experience

Department of the Navy Chief Information Officer
Mr. Dave Wennergren

Space & Naval Warfare Systems Command
Rear Admiral Kenneth D. Slaght

Space & Naval Warfare Systems Center Charleston
Commanding Officer
Captain John W. R. Pope III

Senior Editor
Sharon Anderson

Assistant Editor
Nancy Reasor

Web support by Tony Virata and Bill Bunton, DON IT Umbrella Program.

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

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

Submit article ideas to CHIPS editors at chips@spawar.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 Charleston, 9456 Fourth Ave., Norfolk, VA 23511-2130, or call (757) 444-8704; DSN 564. E-mail address: chips@spawar.navy.mil; FAX (757) 445-2103; DSN 565. Web address: www.chips.navy.mil.

Features

Page 6

"Each of us must be change leaders. Each of us must be willing to do our part to leverage technology as a part of a larger effort to reinvent and reinvigorate our warfighting processes."

Dave Wennergren
DON CIO

Page 10

Interview with Barbara Johnson, DON IT Umbrella Program Manager and Floyd Groce, DON Representative and Co-Chair of the ESI Working Group

Page 15

"One of the most consistent focuses and approaches in the SPAWAR organization is the constant focus on the customer."

Scott R. Randall
SPAWAR Deputy Commander

Page 19

"The Global War on Terrorism has reinforced our commitment to a force focused on operating along the full spectrum of conflict."

Lt. Gen. Steven W. Boutelle
Army CIO/G-6

CHIPS FALL 2003

Volume XXI Issue IV

Transformation TechNet - May 2003. Vice Adm. Richard W. Mayo, Commander, Naval Network Warfare Command, talking with Lt. Mark Preissler, who was representing the Information Professional (IP) Officer Community and exhibiting CHIPS in the NETWARCOM exhibit, as well as fielding questions on NETWARCOM and other topics.

Editor's Notebook

This issue, I want to share some information with you — about you. There is no better way to find out what people want than by meeting them face-to-face and asking them — so we did. We participated in a sampling of DON and DoD IT conferences across the country and asked you questions about your preferences for CHIPS — online and in hardcopy. What we found is that the CHIPS online reader is goal-oriented, interested in factual information that is easy to retrieve and manipulate. We also found that a great number of readers, who are supervisors or project leaders use CHIPS articles for team training.

Acting on this information, we redesigned the CHIPS Web site with a cleaner look to include both html and PDF versions of articles for flexibility. We only use graphics that are relevant to the topic to reduce loading time and bandwidth. With the help of Tony Virata, DON IT Umbrella Program Webmaster, we added a Search Utility and Author Index. Tony also completely redesigned the online subscriber capability and database system. All we had to do was tell Tony what we needed and he made it happen. Visit the CHIPS Web site www.chips.navy.mil and see what's new.

In the hardcopy edition, readers told us that they like lots of color and graphic illustrations, articles from top DoD and DON leadership regarding new programs and technology, and project management and process improvement topics. So each issue includes articles or interviews with top leadership, program managers and IT innovators — and articles from the DON CIO and the DON IT Umbrella Program — our key stakeholders.

At the TechNet Washington, D.C., conference, CHIPS had double exposure. We found the new Information Professional (IP) Officer Community exhibiting CHIPS in partnership with the DON CIO. At Transformation TechNet in Virginia Beach, Va., we partnered with the Naval Network Warfare Command (NETWARCOM) to exhibit and distribute CHIPS.

In a five-month period (March - July 2003) the CHIPS Web site had over 352,470 readers. Online readership from mil, gov and edu domains was 120,936. The remaining readers are from dot-coms, net, biz, info and org domains, and include many of our industry partners. On average we print and mail between 35,000 to 40,000 hardcopies for each edition.

Thank you to the DON CIO, NETWARCOM and the IP Officer Community for exhibiting CHIPS — and to you our readers for sharing your comments and suggestions. We always enjoy hearing from you so please send comments and suggestions to chips@spawar.navy.mil.

Sharon Anderson

DON CIO

Putting information to work for our people

As the community of Navy-Marine Corps information technology professionals — both military and civilian — we are change leaders for the Department of the Navy. The Department's journey of transformation will only truly be successful if each of us is a positive force for change. Opportunities for transformation and innovation surround us; these opportunities must be exploited. We must never forget that our "shipmates" on the Navy-Marine Corps team look to each of us as examples. Our commitment to change, our acceptance of new ideas and initiatives, and our positive reinforcement and support is observed and assessed by our teammates — they take their cue from us. We must be positive forces for change, supporting and improving our strategic initiatives like FORCEnet, PKI, NMCI, etc., and thereby ensuring their maturation and success.

Recently, I had the honor and privilege of spending time with a large group of positive change leaders — the Navy's Information Professional (IP) Officer Community. The IP Summit 2003 focused on a theme of "Sea Power 21 — Realizing the Information Power Advantage." Under the gifted leadership of Vice Admiral Dick Mayo, the IP Community has grown to 410 officers, and in only two short years has truly forged a "team" of extremely innovative and dedicated advocates for the digital transformation of the Department. In addition to aligning community goals and competencies, the forum served as both a knowledge-sharing forum and an important opportunity to prioritize community efforts to ensure the continued success of the naval warfighting mission in the digital age. Every attendee of the conference, which included 70 stakeholders external to the community, came away from the event both energized by the enthusiasm and commitment of our officer community, and impressed by the willingness of all of the participants to work on 14 pilot projects over the coming year that will provide real value to the Navy.

The summit was also an outstanding example of the power of appreciative inquiry and positive organizational change techniques. The success of this approach can be traced to the outstanding efforts of Dr. Ron Fry of Case Western Reserve University, and Dr. Frank Barrett of the Naval Postgraduate School. If you would like to know more about the importance of appreciative inquiry and positive change as leadership skills, you can check out Dr. Barrett's Web site at www.nps.navy.mil/cpc.

It is only through positive change leadership that we can ensure that bold new IT initiatives are embraced and sustained, rather than stifled before they have a chance to succeed. I am excited and energized by the success of our Navy IP Officer Community as exemplars of the power of positive change leadership. I encourage each of you to join them in positively shaping the "IT future" of this great Navy-Marine Corps team.

Dave Wennergren

Department of the Navy Chief Information Officer Dave Wennergren

Mr. David M. Wennergren serves as the Department of the Navy Chief Information Officer (DON CIO). Reporting directly to the Secretary of the Navy, he provides top-level advocacy in the development and use of information management/information technology (IM/IT) and creation of a unified IM/IT vision for the Navy-Marine Corps team. He develops strategies, policies, plans, architectures, standards, guidance and process reinvention support for the entire Department of the Navy. Additionally, he ensures the development and acquisition of IT systems are interoperable and consistent with the Department's vision.

CHIPS: As the driving force for successfully implementing information technology (IT) and information management (IM) initiatives across the DON, what agencies do you work with?

Mr. Wennergren: One of the most critical jobs for a CIO is this idea of "integrating." Most of the initiatives that we work on are complex, with relationships and impacts across many organizations, so it's really important that you have both a good internal team and a lot of external partners. Internally, my two closest friends, if you will, are my new Deputy CIOs — Deputy CIO (Navy), Rear Adm. Tom Zelibor and Deputy CIO (Marine Corps), Brig. Gen. John Thomas. Their teams represent the alignment of C4 and CIO initiatives, and our staffs work very closely together to craft and execute the IT agenda for the Department. There are obviously other key players who are working big initiatives that are very important to us in the DON, including, Rear Adm. Chuck Munns, Director of the Navy Marine Corps Intranet (NMCI) project and Monica Shephard, Commander, Task Force Web. So there is quite an elaborate network of organizations that we work with inside the Navy-Marine Corps team.

As you can imagine, we are more and more focused on "joint" solutions and interoperability with our allies and coalition partners, and we also collaborate across the federal government; so there is a lot of work that I have to do with our external partners too. I have very close working relationships with the CIOs for the Army, Air Force and Department of Defense, in addition to working with other Federal CIOs through the Federal CIO Council. We work together to make sure that we align IT initiatives that really deliver the best service to the taxpayers and enhance our warfighting capability.

Industry is probably the last piece of the relationship triad — internal government within the Navy-Marine Corps team, external government and then industry. The only way to be successful in implementing a robust transformational information management agenda in the 21st century is to align with industry best practices. So I spend a lot of time talking with peers and counterparts in industry and academia to make sure we move toward standard solutions that reflect industry best practices, and I think you can see that in some of the big initiatives we are working on in the Navy-Marine Corps. We have moved away from government-only solutions to solutions that really do leverage the best that industry has to offer, so that industry as a whole can help bear the cost of bringing things to market with us.

CHIPS: Can you talk about the DON CIO reorganization in terms of how the DON CIO is structured to perform its mission?

Mr. Wennergren: Absolutely. I think the restructuring initiative for information management/information technology (IM/IT) for the Department that we have been undergoing for the last six to nine months has really done some powerful things to help better align the way we manage IT across the Navy-Marine Corps team. One of the key components of that, as I mentioned before, is the establishment of a formal working relationship with the Navy-Marine Corps chains of command rather than the ad hoc relationship that we previously had. So by designating the Navy and Marine Corps C4 directors to be dual-hatted as Deputy CIOs for the Navy and Marine Corps, we have been able to align command, control, communications and computers with CIO responsibilities to make sure that we have an integrated vision and strategy, and then aligned execution. Rear Adm. Zelibor, Brig. Gen. Thomas and their teams have done a great job of aligning vision with the DON CIO. Rob Carey serves as our Deputy CIO for Policy and Integration, and as a leadership team, we have all the pieces in place to allow us to move from good ideas to execution.

Another part of the restructuring was the further alignment down through the chains of command. So if you are an Echelon II or major claimant on the Navy side, or major subordinate command on the Marine Corps side, you now must have a formal working relationship with either the Navy or Marine Corps Deputy CIO. In this new view of the world, we look similar to the way things work at some large companies, like GE, Northrop Grumman, etc. As a Command Information Officer at a place like the Naval Air Systems Command, you need to make sure two things are happening. You need to make sure that the head of your business unit, the commander of NAVAIR, is happy with the IM/IT agenda for the command, but you also need to make sure that you are working with the Deputy CIO to be in sync with the overall alignment of technology initiatives across the Navy team. So this formal alignment of the Navy and Marine Corps Deputy CIOs to the DON CIO and Echelon II CIOs to the Deputy CIOs is helping us to align and integrate, and also to make sure that best practices and good ideas are being shared.

The third piece of the restructuring plan is what has been called an Enterprise Implementation Plan. It's currently being worked on, and will serve as an investment guide that feeds into the beginning of the programming and budgeting process. This is to make sure that all of our commands understand how they should be investing their IT dollars and know what constitutes a good investment that aligns with our portfolio and vision. As an example, we are moving toward a world of Web-Service solutions that are a part of an Enterprise Portal strategy that leverages Public Key Infrastructure (PKI) for strong authentication. These sorts of things are key to our roadmap of how we are going to complete the digital transformation for the Naval warfighting team, and must also be used as the basis for evaluating future investments.

CHIPS: What are some of the DON CIO's initiatives and products?

Mr. Wennergren: When we say DON CIO, I would like to emphasize that it is really about a very large group of people across the entire Navy-Marine Corps team who work on these initiatives. I'm really excited that most of the policy, products and tools that are developed represent the efforts of IPTs (Integrated Product Teams) and other teaming arrangements that involve key players from across the Navy and Marine Corps. I think the value of this strategy is that we find great minds throughout the organization to help create innovative solutions. I think the CIO team delivers two things, the first one is the most obvious and that is policy — policy and guidance about the vision, strategy and how we move into implementation of our major IT initiatives. Some of our recent policy efforts include the first XML policy in the federal government, and that has been a very successful effort; the policy on how we are going to move to an Enterprise Portal solution — the Navy Marine Corps Portal, smart cards, Critical Infrastructure Protection (CIP), Information Assurance (IA), and the list goes on and on.

But there is a second aspect as well. You need to deliver tools — tools to actually help commands make our vision and policies a reality. So people can actually "learn how to fish" themselves. We have spent a lot of time over the last several years developing tools for Navy and Marine Corps commands to use to turn themselves into knowledge-centric organizations. For example, to actually be able to perform vulnerability assessments under the CIP program, to be able to understand IT issues and know how to be an IT-literate workforce; and if you are an IT professional, how to manage your career, education and competency development, how to develop architectures and how to leverage standards. It is quite a robust set of tools that we have delivered, and they continue to improve as a result of the beneficial feedback that we get from organizations using the tools. One of the measures of success of these tools is that our knowledge management (KM) and IT Workforce tools have been embraced by the Federal CIO Council and implemented as government-wide tools.

CHIPS: Knowledge Management has always been a DON CIO passion. Can you talk about the progress of the KM pilot projects?

Mr. Wennergren: KM continues to be a DON CIO passion. The two core themes of the Navy-Marine Corps IT team are network-centric operations and knowledge dominance for the Naval warfighting team. Knowledge dominance is a critical component — having access to the right information at the right time from authoritative data sources to allow rapid decision-making and collaboration. This is crucial to the success of our warfighting mission and is evident in the recent conflicts in Afghanistan and Iraq. There are a lot of KM initiatives that the Navy and Marine Corps have put into place that have been great successes — Collaboration At Sea, which allows carrier battle groups to do real-time collaboration, the Knowledge Wall, the Knowledge Home Port developed by the Pacific Fleet...

The common thread is that operational forces recognize the power of collaboration and knowledge sharing — and have become champions for knowledge management. There is a lot of great work going on right now. One of the initiatives that I am excited about is at Submarine Group TEN in Kings Bay, Ga., under the leadership of Rear Adm. Gerald Talbot. It involves the Trident submarine "blue" and "gold" crews so that as a crew comes off deployment to shore they can still maintain their proficiencies and share and collaborate during that off-cycle time. At Commander, Naval Reserve Force there is a project to reengineer the entire Naval Reserve Force claimancy using knowledge management as the foundation for that transformational effort.

Vice Adm. Richard W. Mayo, Commander, Naval Network Warfare Command, recognizing the power of KM throughout the Navy-Marine Corps team, is leading a flag officer level knowledge management steering group to make sure we continue to embrace and deploy KM solutions. We are working closely with Vice Adm. Mayo on that initiative. I had the great pleasure of attending the most recent Information Professional (IP) Officer Community Summit where knowledge management was clearly front and center on the agenda of the IP Officer Community.

CHIPS: Can you discuss the NMCI legacy application rationalization and the role of the Functional Area Managers (FAMs)?

Mr. Wennergren: One of the wonderful things about having a Navy Marine Corps Intranet is that moving to a single enterprise network has provided a great "forcing function." Unless you move to a single enterprise network you have no idea how many applications you have in an organization. As long as you have hundreds of disparate, local area networks you can develop applications, run them on a local area network and never comply with security rules and never think about the fact that you may be building the same application that other people already have developed. So you waste a tremendous amount of money; you have an insecure network — it is absolutely chaotic. And you make it very difficult for people to find the transactional databases and applications they need to get their jobs done.

By moving to NMCI we were able to say, "Show us all the applications you have in the Navy and Marine Corps so that we can get them on the network." The awareness we gained was phenomenal because we found close to 100,000 applications, which is a number that you can't possibly deal with. So we had to get really serious about making sure we had the right portfolio of applications for our warfighting mission. We established Functional Area Managers, which is a really novel and important change for the

Navy and Marine Corps. Functional Area Managers are senior leaders for a functional area and they have a new set of responsibilities. The first is to approve which applications within their functional areas will be allowed on the NMCI network. We picked senior leaders in areas like logistics, administration, manpower, personnel — and the list goes on — for all the major functional areas in the Department, to work through these tens of thousands of legacy applications and pick those that really need to be on the network. We made great progress over the last year as we whittled that first list of 100,000 to 63,000 by eliminating duplication. Eventually we worked our way down to 7,000 applications, and now we are at about 5,000 and on our way down to a couple thousand.

This is very important work. We are going to have applications on the network that comply with security rules and we will have single best solutions rather than a lot of duplicative solutions. The Navy and Marine Corps need *the best* online small purchase solution — we don't need many online small purchase solutions. We can't afford to spend money on duplicative efforts. The legacy application rationalization work is a crucially important part of getting to single authoritative databases and best practice solutions.

It has also been a wonderful way to move toward the type of applications we want in the future — Web-enabled, Web-Services solutions over the Navy Marine Corps Portal. As we have gone through this rationalization process, we have weeded out the standalone, legacy mainframe and client-server solutions that don't perform well in this Web-based world — the focus has been to deliver the best solution.

Getting back to the FAMS, we designated 24 Functional Area Managers, and their job is to work through all the applications within their functional areas. The FAMs are the ones who have actually done all that hard work of bringing down 100,000 applications to several thousand. I think it has been a hugely successful effort. I co-chair the Functional Area Manager Council with Vice Adm. Pat Tracey, Director of Navy Staff, and she has done a tremendous job leading the Navy effort to reduce legacy applications. The FAMs have all worked very hard on this, and a couple of our Functional Area Managers, Mark Honecker, who is the Logistics FAM and Scott Slocum, who is the Manpower FAM, deserve special recognition for their exceptional work in transforming logistics and manpower processes as a part of this rationalization process.

CHIPS: Are industry standards driving the importance of having a DON blueprint for a standard architecture? How does XML fit into the modernization plan?

Mr. Wennergren: Our eBusiness Operations Office, smart card and XML work are great examples of this. We have made great progress in the last couple of years in moving away from government-only solutions to industry best practices and standards-based solutions. This is crucially important. If you build it yourself you are responsible for all the research and development, caring and feeding, and maintenance solutions. Then you have to make sure your solution works with every other standard application in the world. If you embrace and leverage industry standards it is a different task, and one that is much easier and more cost effective.

So we have spent a lot of time making sure that we use standards-based solutions. Our XML work is a great example. As I mentioned, we are the first federal agency to have an XML vision, policy and developers' guide. We have made sure that the Navy-Marine Corps team has had strong representation in the national and international XML forums and standards bodies — OASIS, W3C, IETF — to make sure that our voice is heard and that we all work together to develop and operate consistently within standards.

In the smart card world, deploying the Common Access Card — which, when it is fully implemented will have 4 million users — is a huge initiative. And by having that large of an ongoing initiative, we have been able to help align industry standards. It's another example of success being integrally linked to recognizing industry best practices and working with industry to develop standards-based solutions.

CHIPS: Can you talk about the status and security benefits of the NMCI, CAC and PKI/E issuance and implementation across the DON?

Mr. Wennergren: I have a couple of great jobs. In addition to being the CIO for the Navy-Marine Corps team, I also get to chair the Department of Defense Smart Card Senior Coordinating Group, responsible for the rollout of the Common Access Card (CAC) across DoD. We have issued over 3 million CACs to DoD personnel, active duty military, Selected Reservists, civilians and contractors. Within the Navy-Marine Corps team we've issued over 1 million cards. The CAC is the carrier for our Public Key Infrastructure (PKI) digital certificates, which is a fundamental component of our enhanced information security efforts.

Let me share with you my experience with smart cards. I use the CAC to get into the building when I come to work in the morning. When I get to my office, I use the CAC to cryptographically logon to my NMCI workstation. Cryptographic logon is a much more secure way of gaining access to a network than user ID and password. Once I am on the network I use the PKI Digital Certificates on my Common Access Card to sign e-mails to prove beyond a shadow of doubt that it was Dave Wennergren who sent the e-mail. I use my digital certificate to access secure Web sites. Rather than the old practice where you had 30 or 40 Web sites, each requiring a separate user ID and password — which you might have securely kept on a yellow sticky note on your desk — you can now use your digital credentials to gain access to some Web sites. I also use the PKI certificates for digital signatures in systems like the Defense Travel System to file my claim and approve travel orders. The PKI certificates are not only key to the information assurance of the Department, but also to the deployment of eBusiness in the government as we move away from a paper world.

Deployment of the CAC and PKI is absolutely crucial to the Department's security posture. It goes hand-in-hand with the rollout of the Navy Marine Corps Intranet. When you get your NMCI workstation you will also get smart card readers and middleware so you can use your CAC card in the same secure environment that I described to you.

CHIPS: What is the status of the NMCI rollout?

Mr. Wennergren: NMCI rollout is a two-phase process. First, the EDS team goes to a command and assumes responsibility of the existing networks. Then, they bring in their own equipment, software, etc., in the "cutover" phase of the process. To date the NMCI-

EDS team has assumed responsibility for over 200,000 seats and has completed cutover of over 90,000 seats — that's on our way to about 365,000 seats.

CHIPS: What is the DON CIO's role in implementing the Navy Marine Corps Portal and NMCI across the Navy?

Mr. Wennergren: As the CIO I am the advocate for information technology across the Navy-Marine Corps team. For the NMCI, we are truly fortunate to have Rear Adm. Chuck Munns as the Director for NMCI. Rear Adm. Munns, in his former job as a Fleet N6 and from his operational career, has a vast wealth of experience about information technology and its importance to the Department's warfighting mission. He is the absolutely perfect choice to be responsible for the implementation of NMCI. As the senior information technology official for the Department, I work very closely with Rear Adm. Munns to make sure he is successful in his efforts to implement the NMCI contract and to make sure all of the necessary policies and oversight strategies are in place.

Hand-in-hand with the rollout of the NMCI, we also want to move to an Enterprise Portal solution. Just as we talked about the large number of legacy applications, we also have a number of portals in the Department. While the scale is not as large, we do have a similar situation. Lots of innovative people trying to do good things have been building portals to gain access to information, share knowledge and perform transactions. That's great. But the problem becomes too many portals, too much duplication of effort, too much redundancy; and people have to make too many choices about what data or knowledge they need rather than having a clear path to reliable knowledge and authoritative data sources.

Just as we had to whittle our way down through how many applications we had, we also have to whittle our way down through how many portals we have. I have been working with the Navy-Marine Corps team to implement the Secretary of the Navy's direction to move to the Navy Marine Corps Portal. This is an Enterprise Portal solution that will be a constituent portal strategy. It will not make every portal go away initially, but will instead, integrate what we need into a single portal structure where you will be able to find the intellectual capital of the Department, whether you are deployed or ashore, at work or at home.

To be successful in this we need our commands to focus on content management. I don't need command X in New England to be the 500th command to build a portal and worry about a customized look and feel, and channel delivery and those sorts of things. What I need them to do is to think about what content their customers need to access, put that content onto an Enterprise Portal structure and let us have one organization worry about customized look and feel. PKI authentication will be on the front end of the portal with common services provided to everyone.

CHIPS: What is on the horizon for Workforce Competency initiatives?

Mr. Wennergren: The success of the Department of the Navy is directly attributable to the outstanding men and women of our military and civilian service. We are truly blessed by an extremely intelligent and innovative workforce, and our IT professionals are up to the challenge of the 21st century digital revolution. But the world is changing rapidly, and the skill sets and knowledge required of our IT workforce is changing rapidly as well. As the IT workforce leader, I am thrilled to have worked with an outstanding group of individuals to put into place some very robust and groundbreaking tools to help our workforce assess their needs and develop competencies. Sandy Smith, as our CIO Workforce team leader, has championed the development of some outstanding career planning tools that have now been adopted by the entire federal government. We will continue to champion issues such as continuous learning, Web-based individual development tools, a virtual community workspace, and innovative scholarship and apprenticeship programs.

Choosing to change means accepting risks; choosing not to change, in today's world, risks irrelevancy. I am honored to be a part of an outstanding Navy and Marine Corps team that has chosen to champion change.

CHIPS: Let's talk about the DON eBusiness Operations Office.

Mr. Wennergren: It's one of the efforts that I'm most proud of. We had a vision several years ago to create an innovation center that would partner a small team of government professionals with private industry experts to help Navy and Marine Corps commands make the move from labor-intensive paper processes to the world of the Web and eGovernment. The Department of the Navy eBusiness Operations Office has been an unqualified success in accomplishing that goal. Under the leadership of Karen Meloy, and the outstanding work of Karen Gadbois, the entire eBusiness team in Mechanicsburg has made that vision a reality.

There are numerous examples where the consulting services and the 53 pilot projects that they have championed have produced tremendous value — with some solutions expanding across the Department of the Navy or even the entire Department of Defense. It is an outstanding example of how innovative Naval personnel, partnered with industry leaders, are reinventing processes, improving operations and reducing costs. It is also an excellent example of the need to move with speed, and develop solutions in months rather than years. The team has been recognized with numerous awards, and has recently been tasked to provide similar support to the Office of the Secretary of Defense in managing their new incentive pilot fund. The eBusiness team is a classic example of the importance of change management.

In the end, much of what we spend our time doing is leading change across this great organization. That's a responsibility of each of our IT professionals — military and civilian. It is a time of great change — which is viewed with consternation by some, but fortunately is embraced by many more as a time of great opportunity. Each of us must be change leaders. Each of us must be willing to do our part to leverage technology as a part of a larger effort to reinvent and reinvigorate our warfighting processes. At the recent IP Summit, the Chief of Naval Operations asked that group of IT professionals "to deliver tomorrow, today."

The combination of a need to understand and embrace the future, but to deliver results now, is right on target. Choosing to change means accepting risks; choosing not to change, in today's world, risks irrelevancy. I am honored to be a part of an outstanding Navy and Marine Corps team that has chosen to champion change. ☐

Celebrating the DON IT Umbrella Program's 15th Birthday with Barbara Johnson, Umbrella Program Manager and Floyd Groce, Department of the Navy Representative and Co-Chair of the ESI Working Group

CHIPS: Technology has changed so dramatically since the inception of the Umbrella Program. Has this affected the Program vision?

Ms. Johnson: I don't think it has changed the vision. Our charter, drawn up in 1988, was based on assisting the Department of the Navy make more efficient use of IT and IT dollars spent. Since that time, we have migrated efforts to the DoD level. Our mission is the same, but we are working hard to do it better, to buy smarter, ensure a positive return on investment, reduce procurement times and cost, promote standardization and interoperability, and mitigate the risks associated with acquisition for the government. We are now engaged in making that happen for the federal government in our role in SmartBUY. [See Mr. Groce's SmartBUY article on page 14.]

Mr. Groce: I agree that the vision has not changed. However, there have been recent initiatives that are changing the way Navy and Marine Corps customers procure their information technology. These include the DoD Enterprise Software Initiative (ESI) and the SmartBUY program. The ESI is a joint initiative, established in June 1998, to streamline the acquisition process and provide best-priced, standards-compliant software products to DoD customers and authorized DoD contractors. In September 2001, the ESI was approved as a "quick hit" initiative under the DoD Business Initiatives Council (BIC). SmartBUY is an initiative of the Office of Management and Budget (OMB) announced on June 2, 2003, and it is being worked through the Federal CIO Council. The General Services Administration (GSA) is the SmartBUY Executive Agent.

Both initiatives seek to consolidate the purchasing power of the federal government by focusing volume requirements to obtain optimal pricing and preferred terms and conditions for widely used commercial software. As Barbara mentioned, the IT Umbrella Program is supporting both initiatives. The IT Umbrella Program will continue to perform Software Product Manager (SPM) duties for assigned product categories under ESI. And the IT Umbrella Program will assume a similar role in support of ESI under SmartBUY.

CHIPS: What is the average procurement time from when a customer places an order until he receives his purchase?

Ms. Johnson: It really varies on the vendor chosen. Some vendors have items in stock, others build per order. We have had desktops come in anywhere from two to seven days, servers can take up to 30 days. Most of our vehicles have a 30-day delivery schedule, but typically a lot of them are much shorter than that.

Mr. Groce: The primary contract vehicles we use for the ESI are based on GSA Schedules. We rely on the IT Umbrella Program

The Department of the Navy Information Technology (DON IT) Umbrella Program was chartered in 1988 by the Assistant Secretary of the Navy for Financial Management. In his chartering letter, he delineated the benefits of using a Department-wide acquisition strategy with "umbrella contracts" to reduce procurement time and costs, achieve substantial discounts and promote cost-effective standardization.

But the Umbrella Program origins can be traced to September 1983 for this historic Joint Service program, according to Bob Green, Special Assistant for Applications and Data Management, Department of the Navy Chief Information Officer (DON CIO). Bob said, "It was during September 1983 that the first in a series of Joint Navy-Air Force contracts was awarded. This contract was an Indefinite Delivery Indefinite Quantity (IDIQ) requirements contract for 8,500 Zenith Z-100 desktop microcomputer systems running an early version of MS-DOS. This contract was so popular that before the contract ended, over 36,000 desktop computer systems were purchased. The Small Computer Requirements Contracts (SCRC) grew out of the success of the Z-100 contract, and follow-on contracts were awarded for Tempest desktop systems (Z-150), Portables (Federal Data Corporation's "Chameleon"), the Desktop Follow-On Contract for the Z-248, IT Services (still exists as the ITSS BPA), the PC-LAN Contract and the billion dollar Super Minicomputer Contract."

These contracts successfully brought desktop computing to Navy users. The Department of the Navy purchased over 140,000 units from the Z-248 contract. Since that time the number of Navy IT acquisitions has grown exponentially as the DON systematically automated business and operational processes, and built a standardized, flexible architecture for an increasingly sophisticated technology for its tactical and non-tactical operations.

Currently the Umbrella contracts offer a full range of IT services and solutions to meet any requirement including software, hardware, network products, information assurance, project management, security engineering, data warehousing, training, consulting and research for tactical and business operations.

Please go to page 48 for a list of Umbrella Contracts.

www.it-umbrella.navy.mil

and the other SPMs to monitor performance under the Enterprise Software Agreements (ESA).

CHIPS: In talking with Jim Clausen (OASD (NII)/DoD CIO and ESI Working Group Co-Chair), he said that when deciding on which IT products to pursue for contract negotiations, the DoD strategy is to "follow the money" and monitor what DoD IT consumers are purchasing. Does the Umbrella Program follow this strategy?

Ms. Johnson: We work very closely with Mr. Clausen's office and that is our strategy as well — how we put a vehicle in place.

Mr. Groce: Correct. The ESI Working Group does not determine requirements. This is the responsibility of the end-user who selects the product based on architecture, interoperability and other requirements. However, we track demand and would ask customers for a forecast of their deployment requirements when available. These requirements could be used to establish an Enterprise Agreement. The team targets common-use commercial software products. Before engaging one or more software resellers in discussions, the team first works with the software publisher to understand their pricing and licensing model, including terms, conditions and product use rights. We also consider the DoD installed base of their software. This helps validate demand and can provide additional leverage so that the installed base of software can be "grandfathered" into the Enterprise Agreement.

CHIPS: How does the Umbrella Program fit into the DoD and DON acquisition strategy?

Ms. Johnson: The Umbrella team, which is made up of several organizations: SSC San Diego, SSC Charleston Technical Specifications and Acquisition Branch (Code J645), Naval Inventory Control Point (NAVICP) Mechanicsburg, Naval Air Systems Command (NAVAIR) Patuxent River and Naval Undersea Warfare Center (NUWC) Newport, works very closely with the DoD and DON in the Enterprise Software Initiative and MID-905 [Management Initiative Decision (MID) 905 Commercial Off the Shelf (COTS) Information Technology/National Security Systems (IT/NSS) Software Action Plan]. We try to determine the requirements and, how we can best service the majority of customers by establishing acquisition vehicles that meet those requirements. We also participate in the IT Corridor Working Group where the ITEC Direct Information System (www.itec-direct.navy.mil) is the Navy's implementation of e-commerce.

Mr. Groce: As I previously mentioned, the IT Umbrella Program serves a critical role as SPM for assigned ESI product categories. This includes Enterprise Resource Planning (ERP) and office systems, which include the entire Microsoft product line, Section 508 tools and CAC middleware. SPM duties are established in a Defense Guidance and Policy memorandum that we have posted to the ESI Web site (www.don-imit.navy.mil/esi). These duties include collecting and validating requirements, implementing or facilitating Component asset management procedures to track and manage acquired software rights and managing the resulting Enterprise Agreements. The IT Umbrella Program also provides a "storefront" for the Defense customer through the Information Technology Electronic Commerce Direct (ITEC-Direct) online catalog.

CHIPS: Is there a group of contracting officers at the NAVICP, for example, who just focus on the Umbrella contracts?

Ms. Johnson: There isn't really a specific group of contracting officers at the NAVICP "dedicated" to the Umbrella Contracts, they do have other assignments. But the NAVICP office has awarded all the recent ESI agreements because of their close proximity to Floyd's office and the DON CIO and their historical expertise in these types of awards.

Mr. Groce: While the contracting professionals do provide IT contracting for other customers, the ESI incorporates a best practice to improve the software acquisition system by use of contracting professionals with expertise in licensing of commercial software. For this reason, responsibility for negotiating Enterprise Agreements is assigned to offices with demonstrated specialized knowledge and expertise. This also permits the collection of lessons learned from each Enterprise Agreement negotiation to be captured for future reference.

CHIPS: Can you discuss some of the successes of the Umbrella Program, I know early successes were the Desktop I and II contracts.

Ms. Johnson: Right, those came in at the very beginning, my history with the Program began in 1994. We consider our work with the DoD ESI a huge success, because there has been substantial savings to our customers in teaming with the ESI. By working within the ESI we have leveraged our advantage in working very closely with the other DON and DoD organizations within the ESI: the Air Force, Army, DISA, DLA, DIA ... all the major DoD Components. We each have areas of expertise where we take the lead in certain types of procurements, for example, the Navy is the designated lead for Office Automation and Enterprise Resource Planning; the Air Force has the lead for Information Assurance (IA) Tools, Enterprise Management and Records Management; the Army has the lead for Business & Modeling Tools, Collaboration Tools, Database Management and Enterprise Architecture Tools; and DISA has the lead for Operating Systems. By working closely we are able to aggregate requirements and achieve greater discounts in partnering with industry. We also can avoid duplication of effort and concentrate on our area of expertise. We are able to assist organizations in smarter procurements — and we now treat software as an asset, similar to hardware management.

CHIPS and the Connecting Technology Symposiums are very important successes. These two projects bring information to the warfighter. CHIPS with an online and hardcopy circulation of over 500,000 and CT hosting 1,500 visitors per show, certainly are impressive accomplishments within the Umbrella Program. Some of the awards the Program has received are:

2000 - DON Competition and Procurement Excellence Award for Outstanding Contribution to the Promotion of Competition and Innovative Procurement - DON Enterprise Licensing Team

1999 - DON Competition and Procurement Excellence Award for Outstanding Contribution to the Promotion of Competition and Innovative Procurement - Voice, Video and Data (ViViD Contracts)

1997 - Senate Productivity and Quality Award, Medallion of Excellence - SuperMini Contract (Now expired)

1997 - Hammer Award for Reinventing Government and Cutting Red Tape - TAC BPAs

Also the ESI Model and strategies that we help put in place for establishing DoD vehicles have now become the model for the

"Standards-based ordering vehicles, technical support for products throughout the life of the contract, integrated logistics support (ILS), e.g., extended warranty periods, customer support help desks, spare parts, and OCONUS support are all truly some of the "best value" features for Umbrella Contract customers."

- Barbara Johnson, DON IT Umbrella Program Manager

SmartBUY initiative that you will be hearing more about from Floyd.

Mr. Groce: The desktop procurements starting in the early 1980s demonstrated the benefits of aggregating IT buying across the DoD. The ESI is leveraging the expertise of the Program Offices that manage DoD-wide IT contract vehicles, such as the DON IT Umbrella Program, the Army Small Computer Program, the Air Force Standard Systems Group and DISA. This cross-Component collaboration is proving very successful. I would also like to add the following ESI awards to Barbara's list:

1999 - GSA Information Resources Management Conference (IRMCO) Award

2000 - Defense Acquisition Executive (DAE) Certificate of Achievement Award

2003 - FOSE/Federal Leadership Council Showcase of Excellence Award Finalist

CHIPS: How do you monitor customer feedback and resolve problems that customers may have with a particular vendor? How do customers contact you?

Ms. Johnson: Customers contact us directly through e-mail from the Umbrella Web site (www.it-umbrella.navy.mil), the ITEC Direct Web site (www.itec-direct.navy.mil) or they can telephone the ITEC Direct Help Desk (619.524.9644) with problems or questions. Our office does Contractor Performance Assessment Reports (CPARS) for IDIQ type contracts, where we go out to a selection of customers who have used these vehicles and ask them to evaluate how the contract and contractor are functioning. When we have our Program Management Reviews (PMRs) we contact customers to obtain their feedback. We also get good customer feedback from vendors.

Vendors can initiate a technical refresh so if there are products that customers want included in the vehicle the vendor can submit a proposal which we review for contract relevancy, and it may or may not be included in the vehicle. For the majority of Umbrella vehicles, technical refresh of products and services is typically on a 4- to 6-week cycle, which is to say that updated products are added and end-of-life products are removed. Customer satisfaction is one of our primary concerns, so we very much welcome feedback.

Mr. Groce: In addition to the methods mentioned by Barbara, the ESI Web site incorporates a communication tool that permits users to communicate with the SPM via e-mail. The tool lets the customer submit either an informal comment or question, or a more formal requirements specification. The tool sends an e-mail notification to the SPM and maintains a record of the original request and actions taken to support collection of product demand and operational metrics. We have recently extended this capability to include SmartBUY reporting. This will enable us to satisfy the requirement to coordinate targeted software acquisitions through the SmartBUY team via ESI.

CHIPS: Can you discuss cost savings and value to customers by using the Umbrella Program contracts?

Ms. Johnson: It is difficult to quantify total savings because our vehicles have decentralized ordering and we do not check industry pricing or the GSA Schedule at the delivery order level — that is done by the contracting office. I do know I'm safe in saying that savings have been significant. Savings vary, but are in a range of 2 (at the minimum) to 60 percent off GSA pricing. Some of the ESI vehicles have discounts above 75 percent. So if you are talking about database software or Microsoft products, etc., the discounts are in the high range. Those are significant numbers. When we put a vehicle in place, we really try to think of the small agency, which may have only 10 to 20 employees so that the small agency will receive the same (at least minimum) discount as an agency placing a large order. Of course, if you are talking about large purchases — $100,000 and up, these customers will get a substantially bigger discount, but small agencies (small orders) will at least get the minimum discount.

Standards-based ordering vehicles, technical support for products throughout the life of the contract, integrated logistics support (ILS), e.g., extended warranty periods, customer support help desks, spare parts and OCONUS support are all truly some of the "best value" features for Umbrella Contract customers.

Mr. Groce: We use cost avoidance as a metric to track ESI performance. This is reported to both the BIC and the DoD CIO Executive Board. We use, as a benchmark, the associated price on the GSA schedule, other Government-wide Acquisition Contracts (GWAC) or the vendor's published catalog price. We compare this price to the price we've negotiated under the Enterprise Agreement to determine the cost avoidance.

The ESI has achieved over $1 billion in cost avoidance over the five-year life of the program. Since all Enterprise Agreements are open for use by authorized contractors, customers in addition to those that purchase directly also share in the savings of reduced cost of software acquisition. The ESI also provides value in other areas besides cost. In addition, Enterprise Agreements include requirements to ensure products are compliant with the DoD Joint Technical Architecture (JTA) standards thereby promoting interoperability. ESI is also spearheading the implementation of Software Asset Management within the Defense Components, which should achieve savings by establishing processes to manage software as an asset throughout its life cycle.

CHIPS: If a customer complains to you that his quote was not below GSA Schedule per the Umbrella Program contract or it was higher than expected can you help negotiate a lower price?

Ms. Johnson: Customers can try to negotiate better terms, but if they don't have time, that is one of the duties of the Software Product Managers — to negotiate for them. The SPM would go out to all our vendors on the contract with the requirements or specific product and ask for their best price.

Mr. Groce: The customer should contact the SPM whenever they have questions concerning an Enterprise Agreement or when they have completed the requirements determination process and have selected a product. The SPM is usually in the best position to advise the customer. Using the ESI Web site communication tool is encouraged, and the SPM is required to respond in three business days. By the way, if our customers find better deals, we have a feedback process built into the regulations and policy. If possible, we want an opportunity to extend these prices to all DoD customers. This is because we take an enterprise view under ESI, and believe that the best discounts can be realized by consolidating our requirements and presenting a single face to industry. Defense customers should be aware of the procedural guidance in the Defense Federal Acquisition Regulation Supplement (DFARS) Subpart 208.74. A copy is available on the ESI Web site at www.don-imit.navy.mil/esi.

CHIPS: So you wouldn't just go to the vendor who didn't meet the contract price, you would canvass all the vendors on the contract?

Ms. Johnson: Right. We would open up the competition among vendors. We don't have very many "sole-source" vehicles.

Mr. Groce: Once a DoD customer determines their requirement, the customer must follow the DFARS guidance. All agreements are constructed for flexibility and the customer has many options when using them. Additional discounts may be obtained through "spot" price reductions and other methods. In many cases, we also try to maintain competition, so the same software products may be available from multiple resellers.

CHIPS: Let's talk about the features of the ITEC-Direct Web site.

Ms. Johnson: ITEC Direct is part of the DON acquisition strategy. The ITEC Direct Information System is the Navy's gateway to the IT Corridor for e-commerce. People can implement their own vision or version of e-commerce in one central marketplace. So we are hoping that all these initiatives lead to one of the main initiatives under MID-905 and the ESI — and that is Software Asset Management — managing software as we have traditionally managed hardware, treating software as an asset because it is an investment.

We find that people are buying licenses for the same product multiple times because licenses are not managed. In vehicles under the ESI we are making SAM a requirement so we can transfer licenses within the DON enterprise. So that if someone purchases a license that he no longer needs, we can find a use for that product within the enterprise. We have been successful so far in doing that with Oracle database licenses. We had people purchase licenses at a better than 64 percent discount and they were not going to use this product any longer. We have been successful in finding another home for those licenses. The agency that needed the Oracle database didn't have to purchase licenses — they could just pick up the maintenance costs. So that is saving a lot of money. We hope this doesn't happen too often, but if it does we have a method to transfer DON assets to where they are needed.

Mr. Groce: ITEC-Direct will continue as an e-commerce tool supporting both the IT Umbrella Program and the ESI. In addition, because the DoD ESI primarily uses Blanket Purchase Agreements (BPAs) under the GSA Schedules for establishing Enterprise Software Agreements, the ESI has reached agreement with GSA for creation of an additional storefront for our Enterprise Software Agreements called the Virtual IT Marketplace, or VITM. This "catalog within a catalog" uses the GSA Advantage infrastructure to provide "point and click" comparison shopping. The VITM will provide access to ESI products and services and will have the same capabilities as GSA Advantage. The VITM is now operational and may be accessed through the GSA Advantage Web site or directly at www.vitm.gov.

Adobe Contract Announcement

The Enterprise Software Initiative (ESI) is pleased to announce the award of a new Enterprise Software Agreement (ESA) for Adobe products. A Blanket Purchasing Agreement (BPA) was awarded to ASAP Software on September, 12, 2003, under BPA N00104-03-A-ZE88. Based on Department of Defense purchases on the previous BPA, the DoD community has qualified for discounts up to 13 percent off Adobe's highest GSA discount level (Level F).

The ASAP point of contact for this vehicle is David Beale. The Software Product Manager is Linda Greenwade. Ordering for this BPA expires September 30, 2005. Additional awards for Adobe vehicles are expected in the near future. Please go to the DON IT Umbrella Web site (www.it-umbrella.navy.mil) or the ITEC Direct Web site (www.itec-direct.navy.mil) for more information.

Thanks, I needed that!

The DON IT Umbrella Program proudly announces the completion of phase 1 of the newly unveiled Umbrella Program Web site — www.it-umbrella.navy.mil. Doris Bohenek, Umbrella Program technical specialist and Tony Virata, Umbrella Program Webmaster, have just completed phase 1 (a major structural and design change) of a multiphase project, which focuses on providing:

- A more intuitive Look-and-Feel Web site that is easy-to-use and navigate
- New Categories — FAQs, News Archives and more...
- News Bulletins
- Up-to-the-minute contract information

In phase 2, they plan to begin stuffing the pull-down menus chock-full of news you can use to make informed and cost-saving IT purchases, adding In-depth Product Reviews from IT technical experts, search capability across mulitiple contracts and a customizable layout tailored to a user's preference.

Visit today and let us know what you think — www.it-umbrella.navy.mil. We think you'll like our new look and features and agree, *"Thanks, I needed that!"*

SmartBUY

By Floyd Groce

What is SmartBUY?

SmartBUY is a government-wide software enterprise-licensing project that leverages the buying power of the federal government. Its purpose is to consolidate the purchasing power of the federal government by focusing volume requirements to obtain optimal pricing and preferred terms and conditions. On June 2, 2003, the Office of Management and Budget (OMB) announced the SmartBUY initiative as part of the President's Management Agenda eGovernment Strategy. The goal is to better manage information technology (IT) resources and save money on commercial software that is generally acquired using license agreements with terms and prices that vary based on volume.

The General Services Administration (GSA) is the SmartBUY Executive Agent and performs SmartBUY contracting responsibilities. Near term efforts have focused on identifying best practices, conducting an agency survey to identify demand for software products, and convening interagency customer feedback sessions with the SmartBUY Team to facilitate sharing of requirements and information on current agency agreements.

The objective is to develop a government-wide process to acquire and manage software as an enterprise asset. The SmartBUY effort leverages the DoD Enterprise Software Initiative (ESI) resources and incorporates many ESI best practices. These practices have enabled the DoD to achieve over $1 billion in cost avoidance for commercial software products in the five-year life of the ESI. The ESI Team has been working closely with the SmartBUY project for several months and coordinated the initial SmartBUY commercial software survey response.

The DoD participation with SmartBUY is through the ESI Team. SmartBUY incorporates the concept of Software Asset Management (SAM). As defined by the DoD ESI, SAM is the process of proactively managing the software technology assets of an organization. It covers management of all processes, procedures, policies, technology, people, and partners/suppliers involved in the acquisition, delivery, deployment, maintenance, administration, management and final disposition of a software asset. The focus is on managing the software life cycle to not only reduce costs, but also to reduce liability exposure, improve software compliance, and better match usage with contract terms.

The ESI has launched a cross-Component Integrated Process Team (IPT) to implement SAM within the DoD and in each of the Defense Components. This includes defining and implementing enterprise processes, and developing Component-level implementation plans. The IPT reports through the DoD ESI Working Group to the DoD Business Initiative Council (BIC), a senior executive forum chartered by the Deputy Secretary of Defense to improve the efficiency of DoD operations and allow identified savings to be reallocated to higher priority efforts.

How does SmartBUY affect me?

SmartBUY does not mandate standard software products. As with the DoD ESI, customers are free to determine their own software requirements to best fit their mission and IT architecture — subject to their agency policy. However, if a customer selects a product or requires software maintenance for which a SmartBUY agreement has been negotiated, SmartBUY will become a mandatory source. SmartBUY policy is posted on the DoD ESI Web site at www.don-imit.navy.mil/esi. This policy provides the framework for migrating existing ESI Enterprise Agreements and other Component and Program specific license agreements to SmartBUY Enterprise Agreements. In the meantime, OMB has established policy to be followed by federal departments and agencies to ensure successful transition to SmartBUY. Specifically, federal agencies are to:

1. Develop a migration strategy and take contractual actions as needed to move to the government-wide license agreements as quickly as practicable, and

2. Integrate agency common desktop and server software licenses under the leadership of the SmartBUY Team. This includes refraining, to the maximum extent feasible, from renewing or entering into new license agreements without prior consultation with, and consideration of the views of, the SmartBUY team.

The GSA-led team is negotiating these enterprise licenses in close coordination and collaboration with federal agencies. The first SmartBUY agreements are planned to be in place by early fiscal year 2004.

How do I comply with SmartBUY policy?

DoD customers will continue to follow procedural guidance contained in Defense Federal Acquisition Regulation Supplement (DFARS) Subpart 208.74. Acquisition personnel must review and be familiar with available SmartBUY and DoD ESI Enterprise Agreements. Software procurement actions that either use existing ESI Enterprise Agreements or are coordinated through the ESI as part of a new agreement being negotiated will be considered as having satisfied the necessary OMB review requirements. Coordination for other targeted software acquisitions can be accomplished through the ESI Web site (www.don-imit.navy.mil/esi). From the "Contact the SPM" frame, select the "Send a requirements specification form" button. From the "Select Company" dropdown list, select "SmartBUY Reporting." Any new commercial software agreements must be flexible to permit migration to SmartBUY consistent with SmartBUY guidance and policy. Coordination with the SmartBUY Team is through the designated DoD SmartBUY points of contact identified in the implementation policy posted on the ESI Web site.

Information Technology in the federal government is big business estimated at over $58 billion in fiscal year 2003 alone. OMB estimates the federal government has more than 4 million desktop, laptop, and network computers using multiple commercial software products and projects savings in excess of $100 million annually using SmartBUY.

Floyd Groce is the Department of the Navy Chief Information Officer (DON CIO) Enterprise Licensing Team Leader and Co-Chair and Navy Representative for the DoD Enterprise Software Initiative (ESI).

Talking with Scott R. Randall SPAWAR Deputy Commander

I want to continue to make SPAWAR a premier workplace, with an opportunity to enjoy the challenges and the achievements that we face everyday serving our country. There is no better job than that.

CHIPS: As the new Deputy Commander for the Space and Naval Warfare Systems Command, would you tell us about your previous professional experience and how it prepared you for the responsibilities as SPAWAR's deputy and senior civilian employee?

Mr. Randall: In my 31 years of government service — all with the Navy — I have served in a variety of positions from junior engineer, to division head, to program manager; and finally, to program director with the three major Systems Commands: Naval Sea Systems, Naval Air Systems and SPAWAR.

In addition to program management, my time as a technical director for a field-activity organization afforded me valuable insight into the staff functions of how organizations operate. This experience with the "back-office" operations of a command is invaluable in my current job. I think this combination of programmatic and organizational leadership, as well as my experience at the headquarters and field level, are complementary in achieving SPAWAR's mission and goals in the future.

Just as important as these factors, is the experience of implementing initiatives that span "the enterprise." We have learned in order to achieve maximum efficiencies in our business practices, as well as maximum effectiveness of our warfighting systems, we must be interoperable across organizational boundaries. That applies not only to the Navy but also to the Army, Air Force, Marine Corps and beyond. My experience with implementing NMCI certainly opened my eyes to the vast challenges of executing programs of that scope, but that is where we must continue to go in implementing new technology and products for our warfighters.

I've got to say that I've enjoyed all of my jobs within the Navy. Each had its own set of challenges, but also each has had a common set of rewards — working with top-notch professionals, working at the leading edge of technology, and most of all, contributing to the nation's defense. If I had to tell someone why they should consider working with, or for the Navy, that is the message I would give.

CHIPS: What are your responsibilities as the Deputy Commander?

Mr. Randall: The responsibility that I'm focusing on is the strategic planning for our claimancy nationwide — with a $4.7 billion annual budget — including five field activities, two Program Executive Offices and the Director NMCI. As you know, information technology moves at the speed of light and we need to at least stay abreast of that pace, if not out in front. We're in the process of transforming that process to not only provide our people some coherent direction, but at the same time, maintain the flexibility to quickly change as the technology and environment continue to evolve. Our warfighters need the latest and the greatest. They need it now, and they need it in numbers to win wars. Providing that to them is job number one in our business, and proper planning and execution are how we succeed.

As demanding of my time, is overseeing the day-to-day operations of the command; and what I consider my most important responsibility — taking care of our people. Most of our 7,700 employees are civilian; and as the senior civilian, people look to me for mentoring and leadership. It is the one role that I have learned is critical in ensuring the organization is productive and effective. This becomes even more challenging in today's environment of constant and accelerating change, and also with the resource pressures of meeting the modernization goals of the Naval Services.

A relatively new role in my position is working across Systems Command boundaries as part of the "Virtual Systems Command." Since the beginning of this year, the Systems Commands have made a concerted effort to operate more closely together. We are aligning common functions and common processes across the commands in order to find efficiencies and increase our effectiveness as an acquisition community. I would characterize this process as a real-time transformation — from initial inception to a fully functioning concept in well under a year. The payoff in this concept is already being reaped in the form of more resources to the warfighter and that will only increase as time goes on.

Finally, an important part of my day is spent with our industry partners. We must maintain a close connection with our business partners, so they know what we require to support our forces; and in turn, they keep us informed of new and exciting technology coming down the pike.

CHIPS: Where does SPAWAR stand today as the premier C4I organization in the Navy?

Mr. Randall: We look at change and transformation as our business and this last year has been one of change and transformation for us. There was significant realignment of our acquisition effort in November 2002 with the establishment of the Program Executive Office for Command, Control, Communications, Computers, Intelligence and Space (PEO-C4I & Space). Recognizing the critical nature of C4I, the PEO's sole responsibility is to acquire, field and support C4I and ground-based space systems for the warfighters.

With the PEO taking on the C4I acquisition role formerly done within our Program Directorates, SPAWAR HQ took on the all-important role of C4I Chief Engineer for the Naval Services. That responsibility includes establishing the architecture and technical standards by which the Program Executive Offices and other Systems Commands, acquire, integrate and field joint interoperable products. If there's one aspect of success that Operation Iraqi Freedom showed us, it's that "jointness" wins wars, and it's the way of the future. FORCEnet will provide the foundation for that joint architecture within the Naval Services.

To achieve these important goals, we have established new and strengthened already existing relationships, not only within the Navy, but also across the uniformed services and other agencies outside the Department of Defense that support warfighting efforts. We've been working hard to build the trust necessary to implement these new ways of doing business and to breakdown the organizational boundaries that have existed in the past. I believe we've made impressive progress in a very short period of time, but this journey is far from over.

It wouldn't be right to talk about the state of our organization without focusing on our workforce. I've been amazed at the capacity of our people to accept change while continuing to execute and innovate throughout the organization. This applies to Headquarters, PEOs and all of our field activities — just amazing people. We keep asking them to accept more responsibility — from the Global War on Terrorism to the efforts in Afghanistan and Iraq — and they keep rising to the occasion. It is an inspiration and pleasure to join these folks every day.

CHIPS: Can you discuss SPAWAR's relationships with the other Systems Commands and the Naval Network Warfare Command (NETWARCOM)?

Mr. Randall: At the same time PEO-C4I & Space assumed programmatic duties (November 2002), SPAWAR was assigned additional duty responsibility to NAVSEA and NAVAIR as the C4I Chief Engineer. While C4I has long been recognized as the link that crossed platform boundaries, there has never been an effective mechanism for exerting end-to-end authority across those organizational and system boundaries. This new alignment makes that mechanism a reality, and the commanders are currently drafting a technical authority delegation letter, which will be staffed through the ASN (RD&A) [Assistant Secretary of the Navy, Research, Development and Acquisition] to formalize this relationship. The agreement has also been recognized by the Marine Corps Systems Command (MARCORSYSCOM), a key participant in this new process.

The other additional duty relationship SPAWAR has is with NETWARCOM. As a Type Commander, NETWARCOM has the overall responsibility for networks and information operations. SPAWAR is effectively operating as the technical arm of NETWARCOM and we have established a close collaborative working relationship with the operational users of our products and services.

CHIPS: You mentioned FORCEnet as a foundation for a joint architecture for the Naval Services. Can you explain this concept further?

What role does SPAWAR play in the development of FORCEnet?

Mr. Randall: The Chief of Naval Operations' vision, Sea Power 21, is the roadmap for Naval warfare today and in the future. FORCEnet is the centerpiece of that roadmap; and once it's implemented, it will give warfighters the knowledge of the battlefield to "know first" and "act first," using the advantage of knowledge superiority over the adversary.

Sea Power 21 is comprised of three pillars: Sea Strike, projecting decisive offensive power; Sea Shield, access to the battlespace to project that power and a sea-based layer of defense; and Sea Basing, projecting battle forces worldwide from the sea. When I look across what those pillars are trying to achieve, many of their goals are tied to specific information and knowledge requirements. Providing that knowledge dominance to support the other pillars is what FORCEnet brings to the table.

As the FORCEnet chief engineer, our role is critical in ensuring the success of this vision. We break this responsibility down into three areas. The first is to be the FORCEnet architect. As the architect, our primary goal is to ensure that Navy-wide everything is built to a common set of architectures and standards to ensure interoperability at both the Navy and joint levels. While this may seem to be a simple task, the complexity of this task is enormous.

The second role is as the FORCEnet assessor. This is a new role for us as a Systems Command, we not only look at the technical implementation of programs for compliance with the architectures, but also the viability of programs to achieve cost and performance goals. In addition, we need to perform the assessment across end-to-end capabilities and not just traditional SPAWAR programs. We are also working with the joint community to ensure that this assessment methodology fits within the program assessment processes being set up at the joint level.

The last role is that of FORCEnet innovator. Not only is developing technology that meets warfighters needs important, but also equally critical is focusing on how quickly that technology gets into their hands. As we find promising technologies or concepts, we are quickly testing them in a series of Limited Objective Experiments (LOEs) and Integrated Product Demonstrations (IPDs) consistent with Sea Trial and the spiral development process to accelerate capability to the fleet.

CHIPS: What does the term "composeable" mean? What will it mean for the joint warfighter and what will it take to bring to fruition?

Mr. Randall: In the past, we built systems to meet specific requirements. What resulted was a variety of different systems that attacked a variety of different capabilities. It was inefficient in the sense that there was the potential for duplication and overlap, not to mention built-in inflexibility in the ways the systems are assembled and used.

In FORCEnet, we are developing the capability to "compose" what warfighters need for a specific mission from a set of services that will be available on the Internet. For example, if an Expeditionary Strike Group is deployed on a humanitarian mission, it would require a certain set of capabilities and information to perform

their mission. If the ESG is called upon to respond to an immediate warfighting scenario, it will have the capability to redefine what services are required and compose that capability in transit to the new situation. Today, it would take a lengthy re-outfitting of the C4I suite on that ESG — an expensive undertaking. Tomorrow, it will be a routine transition to the new mission. This will all be a matter of subscribing to a new set of capabilities that are implemented through flexible and reusable software modules assembled to meet the new requirements.

We feel this capability is very achievable with today's technology by leveraging the state of architecture and standards within the commercial IT and business world. Good examples of making this concept a reality today are the RAPIDS (Rapid Prototype Insertion and Delivery System) initiative being worked on by PEO-C4I and the FORCEview capability being developed at our Systems Center San Diego. Without going into detail, these efforts are demonstrating the ability to rapidly design, compose and field these capabilities in the near future. Some of these capabilities are also being debuted at the Trident Warrior IPD as we speak.

CHIPS: How does the PEO-C4I & Space fit into the SPAWAR claimancy as well as the other organizations it supports?

Mr. Randall: When we reorganized in November 2002, one of the primary goals was to bring SPAWAR into organizational alignment with the other Systems Commands. All of our Programs of Record were in project director offices, none of which had a direct reporting chain back to the ASN (RD&A). With the establishment of the PEO, we established this direct line of authority and provided that focus on execution of the acquisition programs, while at the same time establishing the new SPAWAR roles we've already discussed. It's probably worth mentioning that we've maintained a strong partnership throughout this process, and the organizations remain interdependent with SPAWAR continuing to provide technical talent, contracts, legal and operational support to PEO-C4I. The advantage is that each of the organizations now have a much sharper focus on their individual responsibilities while still complementing the other's mission — it is a strong team.

At this point, let me add that people tend to equate us with a single PEO, which is not the case. The PEO-IT [Program Executive Office - Information Technology] brings in the non-tactical IT or business process piece of the puzzle. While we have rightly focused much of our attention on the warfighter and the capabilities that directly support them, PEO-IT is charged with supporting the rest of the enterprise IT acquisition story. While currently their assigned programs are primarily personnel management related enterprise applications, PEO-IT is increasingly being tasked to work on acquisition for all of the other non-tactical applications and enterprise service issues within the Navy.

PEO-IT and SPAWAR also support the Director of NMCI, Rear Adm. Charles Munns, in executing the NMCI contract across the enterprise. As it is virtually impossible to divide much of the infrastructure and many of the services associated with both tactical and non-tactical information technology efforts, we are working across the organization to ensure that FORCEnet applies to both ends of the equation. We think this is a logical and complementary "marriage" of capabilities and functions represented by these organizations.

CHIPS: How do the SPAWAR field activities fit in with SPAWAR's C4I role?

Mr. Randall: The vast majority of SPAWAR's workforce, and the bulk of our talent, resides at our field activities and neither Headquarters nor the PEOs can function without their dedicated support. I'm going to start with San Diego. The largest part of our technical arm is here at the Systems Center on Point Loma. The vast majority of our laboratories and scientists are here. They provide the bulk of the systems engineering and technical support for our program offices and for our chief engineer organization. This capability allows us to go from concepts (either developed here or around the fleet), to the laboratory, to quick insertion into programs, and then on to rapid fielding and support. We have developed a very good continuum that has improved responsiveness and quality at the same time.

Next, shifting to the East Coast, we have the Systems Center Norfolk, Va., and the Systems Center Charleston, S.C. Their primary focus is the care of all the systems that we currently field and will field in the future. From the in-service engineering support of fixing things when they break, to helping the fleet with a 1-800 number to call if they have problems, to techical manuals and training... the majority of those efforts are done through Norfolk and Charleston, and are done extremely well. Another important aspect of these centers is that they give us a base of operations to directly support the East Coast fleet centers of concentration and they are becoming increasingly important in supporting organizations like NETWARCOM and the Joint Forces Command in the joint arena.

I should note that all of our activities work closely together in providing end-to-end and life-cycle support to the customer. Over the last several years we have developed a very cooperative arrangement for getting the right people onto the right jobs — independent of the location within the SPAWAR community.

The Information Technology Center in New Orleans is the most recent addition to the SPAWAR Corporation. It was added about two years ago. They manage personnel programs like NSIPS and DIMHRS as well as the legacy personnel programs in support of PEO-IT. NSIPS is the Navy Standard Integrated Personnel System. NSIPS replaced four legacy pay and personnel systems and was fielded to the Reserve Component and active duty Navy. DIMHRS is the Defense Integrated Military Human Resource System for Personnel and Pay Joint Program Management. NSIPS and DIMHRS are both newer programs for the military personnel system. They actually replaced vast numbers of personnel systems that existed in the past. They provide a tremendous improvement in efficiency by consolidating those legacy programs under a single program. Now we have a single user interface and single authoritative database across all of the personnel systems.

Our Space Field Activity in Chantilly, Va., is the Navy adjunct to the National Reconnaissance Office (NRO) and performs extensive space research and intelligence work. Lastly, we have a small liaison office, Washington Operations, to keep abreast of and perform tasks that require a presence in the Washington, D.C., area.

CHIPS: Considering the sizable number of Navy activities in San Diego, is SPAWAR's location beneficial in terms of supporting operational forces and the regional facilities network? Why?

Mr. Randall: I feel fortunate to have moved out here when the command did. I was stationed at China Lake and just completing

... I would like to see us make FORCEnet a reality as soon as possible...

a major source selection on a new cruise missile system, when one of my previous bosses called and asked me to move to SPAWAR during its relocation to San Diego. As he put it, it was an opportunity to reinvent the command with a majority of new people and with a mission that was just starting to be recognized as a major transformational force. It was an offer too good to refuse. We recruited good people, developed new processes and took on some new roles — remember, the IT-21 concept was just taking form at that time. I think anyone who was with the command during that period will tell you this has been a most rewarding and energizing experience.

One of the most consistent focuses and approaches in the SPAWAR organization is the constant focus on the customer. We are able to interact with the warfighters on a day-to-day basis. If the fleet has a problem with a system, we can literally walk down the street and find a platform with the same system on it, investigate the issues, bring it immediately to our laboratories, test it, come up with a solution, run it in to our program managers and field it relatively quickly. That is a huge advantage for us, not only on the Navy side of things, but on the joint side as well — the Marine Corps is up the street from us at Camp Pendleton, and we also have access to U.S. Air Force activities and U.S. Army testing facilities. We are right in the middle of the test complex on the West Coast, which really facilitates getting products to the warfighters and doing it both efficiently and quickly.

While there are benefits to being in the Washington, D.C., area, I believe we more than make up for that with our ability to quickly respond and field capabilities to the fleet. In the end, that is what this business is all about and there is no better place to execute that mission for the Navy than right here in San Diego.

CHIPS: What would you like to see SPAWAR accomplish over the next five years?

Mr. Randall: I would like to see a couple of things get accomplished. If you speak with the warfighters in Afghanistan or Iraq, they will tell you that we have a lot of advantages because of the way we can operate. They will also tell you that one of the biggest advantages is the information operations superiority that we can bring to bear in any conflict around the world. That is in large part due to what we do on a daily basis, 365 days a year. In that light, I would like to see us make FORCEnet a reality as soon as possible. We can turn that advantage into a deciding factor in the Global War on Terrorism and that should be a goal for all of us.

The second goal is much more personal and would come as no surprise to most of the people who have worked for me over the years. My father told me long ago to enjoy what you do for a living — if you're not having fun at your job — change it. I want to continue to make SPAWAR a premier workplace, with an opportunity to enjoy the challenges and the achievements that we face everyday serving our country. There is no better job than that.

Mr. Scott Randall is the Deputy Commander of the Space and Naval Warfare Systems Command in San Diego. He was born in Paterson, New Jersey and attended Rutgers, the State University of New Jersey. He graduated with a Bachelor of Science degree in Mechanical/Aerospace Engineering in 1972 and began his career at the Naval Air Systems Command in Washington, D.C. , where he was an armament system engineer. After several jobs of increasing complexity Mr. Randall became the Primary Support Officer for the armament system on the new F/A-18 aircraft. In 1977 he briefly left the Naval Air Systems Command for a tour at the Naval Sea Systems Command as a combat systems engineer for several Foreign Military Sales platforms. He returned to the Naval Air Systems Command in 1978 accepting a job within the Nuclear Munitions Section responsible for the development, test, compatibility and nuclear safety of the Navy's air launched nuclear weapons, and eventually was selected as the head of that section.

In 1982, Mr. Randall became the Technical Director of the Naval Weapons Evaluation Facility in Albuquerque, New Mexico. This activity was responsible for the development, test, compatibility and nuclear safety of all the Navy's nuclear weapon systems, and for the development of weapons loading and handling publications for all air-launched weapons. In 1991, when the Base Realignment and Closure Commission selected the Naval Weapons Evaluation Facility for closure, he moved to the Naval Weapons Center China Lake, in Ridgecrest, California, as the project director for the Tri-Service Standoff Attack Missile (TSSAM). When this program was superceded by the Joint Air to Surface Standoff Missile in 1995, Mr. Randall was selected as the Navy's Program Manager and Joint Service Deputy Program Manager at the Joint Program Office on Eglin AFB in Fort Walton Beach, Florida. In 1996 Mr. Randall became the Deputy Program Manager for the Navy's Command and Control Program Office in San Diego and was responsible for the design, development, integration, test, fielding and support of the Joint Maritime Command Information System (JMCIS). Following his position as Deputy Program Manager, he became the Program Director for the Naval Networks and Information Assurance Directorate for the Space and Naval Warfare Systems Command in San Diego, California.

Mr. Randall is a graduate of the Program Managers Course at Ft. Belvoir and of the Federal Executive Institute in Charlottesville, Virginia. His personal awards include the Michelson Award, the Civilian Meritorious Service Medal, the Civilian Superior Service Medal, and the Secretary of Defense Achievement Medal. Mr. Randall was selected to the Senior Executive Service in 1998.

Lt. Gen. Steven W. Boutelle, USA Army Chief Information Officer/G-6 talks about how technology is supporting ground forces today and helping the Army transform for tomorrow ...

CHIPS: How has the Global War on Terrorism changed the Army's communication priorities or needs?

Lt. Gen. Boutelle: The Global War on Terrorism has reinforced our commitment to a force focused on operating along the full spectrum of conflict. This ranges from humanitarian operations to armed conflict with the capability to always ensure homeland defense and security. Our global and pervasive information systems, the Army Knowledge Enterprise (AKE), will provide leaders with the information they need to make key time-sensitive decisions. Our Army's battlefield success is contingent on the right information reaching the right Soldier at the right time.

We understand that to fight and win our nation's wars, the 21st-century U.S. Army must rapidly transform to a net-centric, knowledge-based force focused on strategic and tactical responsiveness, and enhanced lethality and survivability. We are continually applying operational lessons learned to make and keep the Signal Corps relevant, modular, scalable, deployable and agile, now and into the Future Army Force.

CHIPS: How is the Army adjusting its traditional approach to battlefield communications support?

Lt. Gen. Boutelle: We've recognized that we have some essential imperatives for how we must do business. First, we must manage our network operations and security centers (Active Component, National Guard, and Reserve) as a single Army enterprise. This allows us to exploit synergies and efficiencies from the sustaining base to our deployed tactical networks. As an enterprise, we must apply our Information Assurance (IA) programs across our strategic, operational and tactical systems. We are leveraging the commercial marketplace as we replace aging systems, such as Mobile Subscriber Equipment (MSE), with the suites of equipment like those in the Warfighter Information Network-Tactical (WIN-T) system.

Second, we must consolidate current and future capabilities into an Army Knowledge Enterprise as the Army's portion of the Global Information Grid (GIG). The AKE concept focuses on integration and interoperability of processing, storing, and transporting information over a seamless network, allowing pervasive access to universal and secure Army information (including business information systems) across tactical, operational and strategic levels. The AKE will provide an "on-the-move" battle command capability by exploiting commercial and military satellite-based networks, providing an uninterrupted flow of information to conventional and unconventional warfighters.

Third, our newly created Network Enterprise Technology Command (NETCOM) is evolving as the Army's global information provider and manager for the entire Army Knowledge Enterprise — Active, Guard and Reserve. NETCOM is designated as the single authority to operate, manage and protect the Army's Knowledge Enterprise Infostructure. NETCOM ensures consistent operational policy and investments are strategically aligned to the Army's global networking requirements. NETCOM manages and defends the Army's portion of the GIG, supports the Future Force, and reduces our total cost of ownership as we build and deploy the Army Knowledge Enterprise.

Fourth, the growing cyber threat to the GIG has brought the Army G-2 and G-6 into a synergistic relationship to manage and defend our networks. NETCOM's Army Network Operations and Security Center (ANOSC) has collocated with the Intelligence and Security Command (INSCOM) — this enhances its dynamic role in information management. And it facilitates and synchronizes the Computer Network Operations and Computer Network Defense missions with those of the Joint Task Force for Computer Network Operations (JTFCNO), the Defense Information Systems Agency, and the 1st Information Operations Command and its Army Computer Emergency Response Team (ACERT).

All six Army theaters now have a Network Common Relevant Operational Picture (NETCROP). This provides the ANOSC visibility of the health and operational status of each theater's network. Additionally, it allows NETCOM to provide a near real-time situational awareness reporting capability to Army leadership. To ensure the highest state of network readiness, the ANOSC initiates network operations and computer network defense drills Army-wide. Standardizing and honing cyber-warfare techniques, tactics and procedures into an enterprise-managed information delivery system will continue to increase the availability and robustness of our networks.

CHIPS: How have you applied recent operational lessons learned to current force operations?

Lt. Gen. Boutelle: We continue to rapidly assimilate our experiences from Joint and asymmetrical operations in East Timor, the Balkans, Uzbekistan, Afghanistan and the campaign in Iraq. The most obvious lesson is that today's Army does not deploy alone

to conflicts or humanitarian operations, but as part of a Joint team. During Operation Iraqi Freedom (OIF), as in Operation Enduring Freedom (OEF) in Afghanistan and Uzbekistan, our Army signal Soldiers provided communications for the Army — and also for the Air Force, Marines and our coalition partners. The extensive data network that linked command-and-control headquarters at all levels ensured a more rapid sharing of information through a common operating picture that consistently allowed forces to operate inside the enemy's decision cycle.

Current operations in Afghanistan and Iraq demonstrated that a net-centric, knowledge-based Army is at the very foundation of the Future Force and a significant and profound combat enabler. Interoperability is now not only expected, but it is demanded, in support of Joint and combined operations. In addition, two key points reinforced in those successes were that conventional signal forces will follow contingency or special operations signal forces and that either of those signal forces must be capable of supporting enterprise network connectivity with voice and data, NIPR, SIPR and JWICS [Joint Worldwide Intelligence Communications System]. Bandwidth requirements expanded dramatically and we have taken steps to get more commercial satellite bandwidth and terminals into units. And more is still needed. We continue to work to meet bandwidth requirements.

A variety of signal units in OEF conducted their assigned missions almost unnoticed in the shadows of successful coalition combat operations. This remained the case as their support grew for nearly 7,000 Joint and coalition customers at Bagram Airfield and 5,000 at Karshi-Karnabad (K2), Uzbekistan. In OIF operations, more than 9,000 signal Soldiers have been deployed to support Central Command operations, establishing key communications links along the way to provide command-and-control connectivity both inside and outside the area of operations.

CHIPS: What role did Blue Force Tracking (BFT) play in these operations?

Lt. Gen. Boutelle: The success of Blue Force Tracking is probably the most heralded example of how the Army is transforming itself into a fully net-centric force and it played a significant role. Our Blue Force Tracking capability in support of OEF and OIF was one of the most effective and successful efforts in demonstrating a transformed Army into a net-centric, knowledge-based force. BFT evolved from the Army's FBCB2 program. This program was developed in Task Force XXI and refined in operations in Bosnia and Kosovo. BFT is an FBCB2, satellite-based capability mounted on various platforms, such as tanks, armored personnel carriers, infantry fighting vehicles, Apaches, Blackhawks, etc.

These BFT-enabled platforms transmitted and received battlefield locations, battlefield graphics and overlays, and orders to and from a central information server system for aggregation and retransmission. This provided a near real-time situational awareness common operating picture of friendly forces on the battlefield to Army, Joint and Allied forces. Thus, BFT allowed our combat forces in Iraq and Afghanistan to have a fully integrated COP beyond-line-of-sight. The satellite capability enhancement allowed forces to operate through sandstorms, night and extremely long distances. Forces could zoom in and out, seeing troop locations for 10 miles, 20 miles or the entire country of Iraq. Battle command doctrine is being shaped by the ability to have "live" situational awareness while communicating and collaborating on-the-move

September 2003 - Soldiers of the 101st Airborne Division attach a sling load of food and water onto a UH-60 Blackhawk helicopter. The supplies are being delivered to the division's 1st Brigade in support of an upcoming mission. U.S. Army Photo by Pvt. Daniel D. Meacham.

via a space-based network. The success inspired the Joint Requirements Oversight Council (JROC) to designate the Army as the Lead Service to refine Joint Blue Force Situational Awareness (JBFSA) capabilities for the Services.

With the Army Headquarters reorganization, and the creation of NETCOM, the Army CIO/G-6's mission to transform Army information management is well underway. Resourcing the information management transformation remains a significant challenge, and educating the Army to embrace cultural change is the key to success. The Army Knowledge Management (AKM) strategic goals are in concert with DoD's Network-Centric Operational Warfare (NCOW) reference model announced in FY03. While we continue to support current operations — OEF and OIF, we are also swiftly forging ahead to institute best business practices and to manage our infostructure at the enterprise level. NETCOM plays an essential role as a global communications provider and manager for the entire Army Knowledge Enterprise — Active, Guard and Reserve. All this adds up to creating a net-centric, knowledge-based force enabling information superiority and battle command to increase the combat power necessary to quickly win our nation's wars.

CHIPS: How important to Soldiers in the field is it to collaboratively communicate with Joint warfighters?

Lt. Gen. Boutelle: Collaboration means sharing common knowledge in real-time and these days, that's essential on the battlefield. This is extremely important. Today we can share pictures, graphics, overhead imagery, and plans among decision makers, even when those people are separated by hundreds of yards or globally by thousands of miles. Folks in Qatar can have a real-time vision of people in Afghanistan on a moment-to-moment basis. They put that brainpower to work linked between warfighters in Afghanistan or Iraq and staffs in Qatar and even in Florida, at U.S. Central Command Headquarters at McDill Air Force Base. They are working to find solutions to issues anywhere in the world.

CHIPS: Based on what you've described, is the Army taking a hard look at how Army Signal should be task organized and manned?

With the Army Headquarters reorganization, and the creation of NETCOM, the Army CIO/G-6's mission to transform Army information management is well underway.

Lt. Gen. Steven W. Boutelle, Army CIO/G-6

Lt. Gen. Boutelle: Yes. In order for us to provide the required communications for all recent operations, we learned we must make significant adjustments to our task organization and modernization efforts. The Army has begun a permanent Signal Transformation to address these issues with the Integrated Theater Signal Battalion (ITSB), the largest and most significant organizational change to the Signal Corps in 20 years. The ITSB is a complete, top-to-bottom rewrite of signal doctrine, tactics, techniques and procedures based on lessons learned in OEF, OIF, and other recent deployments, such as in East Timor.

Why are we doing this? After all our tactical signal organization and structure with MSE and TRITAC equipment served us well in the Cold War and Desert Storm. However, our recent operations demonstrate that we do not have the organization, structure or equipment to support today's warfighter requirements. Significant task reorganization is required and some units (battalions and companies) are not relevant today due to the lack of COTS equipment. And although WIN-T is our future system, in the interim, the next five to seven years, we must adjust to stay relevant.

We are doing this by incorporating transmission, switching and systems-control assets into a single signal unit. "Traditional" echeloned signal support rules did not apply in either OEF or OIF. Thus, we are going to modernize all echelons of communication units to support Joint operations with not only voice, but also SIPR and NIPR, VTC and special circuit capabilities.

These designs will integrate beyond-line-of-sight (BLOS) systems, wide-band data and computer-network-management capabilities into its design. This alleviates the need for massive task organization. Additionally, these designs provide unity of command in an organization of Soldiers who live together, train together in garrison and deploy as a unit or in modular teams. As the blueprint for the tactical signal unit of the future, ITSB is an essential component in AKM strategy. AKM is our comprehensive strategy to transform the Army into a net-centric, knowledge-based force. This plan is linked and synchronized with the Army Transformation Campaign Plan to incorporate technology and leverage streamlined knowledge processes into the Army at a cultural level.

CHIPS: This looks like Army Signal has got its hands full.

Lt. Gen. Boutelle: We are going to be very, very busy. We've got a huge task to provide the right information, to the right person, at the right time, but I am confident that we are on the right track. We must (1) Reshape our signal Forces; (2) Restructure our signal equipment; (3) Consolidate our networks into a single enterprise; and (4) provide bridging communication capabilities until we see WIN-T and Future Combat Systems (FCS) networks are fully fielded.

It will take quality, innovative leadership, and continual engagement and good communications within our Regiment. I am confident that our Soldiers, civilians and contractors, as they have proven in every operation, are up to the task and will continue to be so.

September 2003 - Soldiers mark a spot where unexploded ordnance was found in a field in Mosul, Iraq. The air assault troopers are assigned to Headquarters and Headquarters Company, 3rd Battalion, 502nd Infantry Regiment, 101st Airborne Division. U.S. Army Photo by Pvt. Daniel D. Meacham.

Lt. Gen. Steven W. Boutelle assumed the position of the Department of the Army Staff Chief Information Officer / G-6 on July 3, 2003. Previous assignments include Director for Information Operations, Networks and Space, Office of the Chief Information Officer/G-6, Headquarters Department of the Army from 2001 to 2003; Program Executive Officer for Command, Control and Communications Systems (PEO C3S) from 1997 to 2001; Project Manager for Field Artillery Tactical Data Systems (FATDS) from 1992 to 1996, and Chief of Staff for PEO C3S before his assignment as the PEO. From 1996 to 1997, General Boutelle was the PEO C3S "Trail Boss" responsible for software and systems integration for the Army's Task Force XXI.

After receiving an induction notice in 1969, he enlisted in the Army as a Nuclear Weapons Electronics Specialist. In February 1970, he was commissioned as a Second Lieutenant in the United States Army Signal Corps at the Field Artillery Officer Candidate School, Fort Sill, Oklahoma. He attended the Radio Officers Course at Fort Monmouth, New Jersey before his first tour of duty as a platoon leader for the 1st Battalion, 4th Mechanized Infantry Division, and later in the 2nd Battalion, 41st Field Artillery Brigade, 3rd Infantry Division.

Lt. Gen. Boutelle graduated with honors from the University of Puget Sound, Tacoma, Washington, with a bachelor of arts degree in Business and Finance and with honors from Marymount University, Arlington, Virginia, with a master's degree in Business Administration. His military education includes Command and General Staff College, the Defense Systems Management College and Army War College.

Lt. Gen. Boutelle's awards include the Legion of Merit with Oak Leaf Cluster, Defense Meritorious Service Medal and the Army Meritorious Service Medal with four Oak Leaf Clusters.

In 1919, Lt. Col. Eisenhower traveled by motor vehicle convoy from Maryland to California, a trip that took an exhausting 62 days because of poor roads. In 1956, due to mounting pressure, Congress finally approved construction of a 41,000-mile Interstate System of highways. It transformed America's system of public and commercial transportation; then-President Eisenhower stated why: *"Our communication and transportation systems are dynamic elements in the very name we bear: United States. Without them, we would be a mere alliance of many separate parts."*

Today, it is the digital communication system that is the dynamic unifier, and that is what the Department of the Navy seeks to build across the Navy and Marine Corps. It, too, promises transformation: a more efficient and effective DON. And, how we build it is a lot like how America built the Eisenhower Interstate System of highways nearly 50 years ago.

Building a System

America built the Interstate System of highways for many of the same reasons we seek to fix the Navy's digital communications. America's roads were once described as *"wholly unclassable, almost impassable and scarcely jackassable."* They varied in conditions, standards and lagged behind automotive advances. The result was *"loss of time due to congestion,"* with an appalling problem of *"death and danger,"* stated President Eisenhower. Compare that to the Navy's 1,000 incompatible and antiquated shore networks that not only inhibited information flow, but were also vulnerable to attack.

But, the interstate endeavor wasn't about just laying roads; it was about *building a system*. It required an incredible balancing act by the U.S. Bureau of Public Roads, which had to focus on the overall system, regulating standards and ensuring efficiency. The Bureau had to consider the needs of 3,000 counties and 48 states, and match those to road building capabilities. Often, the precise locations of highways, underpasses and overpasses had to be negotiated. Especially contentious was access-control, (where vehicles enter and exit the highway), a radical concept for its time. Not all were pleased with the improvements, either. Some called it the *"great highway bungle"* and a *"multibillion dollar rathole."* Sound familiar?

Today, the Navy isn't just laying an information highway, it is building an information system, or what is known as an "enterprise system." It is consolidating all its networks into the Navy Marine Corps Intranet — its information highway. To operate on it, we are developing such enterprise-wide applications as the New Order Writing System; Navy Recruiting and Accessions Management System; Navy Standard Integrated Personnel System and eventually the Defense Integrated Human Resources System, which the Navy is leading in development for all of DoD.

But, these are not enough. The promise of the enterprise system is greater efficiency and effectiveness. That's what the corporate world achieved by implementing them and that is what we seek for the DON as well. We want to be able to rapidly correlate data, collaborate on experiences, establish a common picture, and *act corporately*. The question is what else is needed to do that — the other applications, servers and services — not just across the Naval service but in each one the Navy's 24 functional areas? Moreover, how can we determine and incorporate them in a cost effective manner?

Building a Partnership

No one organization has all the answers. How we get them, though, is a lot like how the Interstate System of highways was built. It was accomplished through a *"highway partnership,"* a collection of local, state and federal agencies, the Bureau of Public Roads, and industry. *"The highway partnership ...is a model that should be applied to other programs,"* stated Thomas H. MacDonald, Bureau of Public Roads Chief from 1919 to 1953. And, he's right. Building a Naval information enterprise system requires a partnership between users, the Navy's IT acquisition community and industry.

Ultimately, users must decide the requirements. That was the case with the asphalt highway system. *"The highway program must rest upon the essential premise that we are dealing with the lives of people and in the end they will make the final choices,"* stated MacDonald. This is just as true with a digital highway system. Referring to collaboration on IT systems at Electric Boat, President John Welch stated, *"The people have to make all these great tools sing, so they've got to be part of the process."*

Determining IT requirements, though, is often new territory for users. The tendency is to focus on means — technologies and systems — rather than on the end product and what needs to be accomplished. *"Many organizations fail to specify any organizational objectives at all when implementing an enterprise system,"* stated Thomas H. Davenport, professor of Information Management at Boston University. As a result, they either adapt the system to belatedly recognized needs, or abandon it altogether. Whatever the case, it's costly.

Determining IT requirements, therefore, depends on collaboration, and that's where Navy IT acquisition comes in. Essentially, it helps answer the fundamental question, *"Where are you and where do you think you want to go, so we can better lay out the road?"* While some might see such collaboration as slowing acquisition, it is

much better to have a roadmap as opposed to stopping and asking for instructions along the way.

Industry has a key role in this partnership. In building the Interstate System, the Bureau of Public Roads worked with industry regarding the types and technical features of vehicles that would operate on these highways. For example, the automobile's speed and turning radius made previous road patterns obsolete, requiring new ones. The Bureau also had to know where industry was going, which was especially the case with the growing volume of heavy trucks. Building the Interstate System meant knowing every aspect of industry's transport plans — both present and future.

Today, industry is the premiere expert regarding what operates on information enterprise systems. It has already gone where government has yet to go in terms of enterprise systems. We've got to find out from industry how they have done this.

The problem, however, is that industry sometimes doesn't know how to talk to Navy users about their unique requirements. Again, here's where Navy IT acquisition comes in. It must translate between industry and users, enabling industry to provide a realm of possibilities. It may be necessary for us to iterate back and forth until we say, *"Hey, we have a solution."* However, the bottom line is that we form solutions around industry products.

Moreover, Navy IT acquisition must remain abreast of industry advances and educate users. We are much more in a *"technology-/industry-push"* model for the basics of an enterprise rather than *"user-pull."* So, in that regard, it's even more important that we see where industry is going. However, we still need to address and accommodate user pull in those areas where our innovative Sailors and Marines are pushing the bounds of IT capability to address military unique and leading-edge business needs.

The Middlemen

At the center of this partnership is one organization, the Program Executive Office for Information Technology (PEO-IT), that takes responsibility for acquiring the whole, and conducting a massive coordination and execution process. The need for this was recognized with the Interstate System. As one industry expert stated, *"Without such thoughtful coordination of the highway program ... the proposed $100 billion of highway spending will buy as much chaos as concrete."*

An enterprise system requires the same thoughtful coordination; otherwise, the consequences can be chaotic, as well. One natural resources company that decentralized implementation of an enterprise system failed to achieve interoperability across its enterprise. An electronics firm that took a similar approach implemented different versions of the same system in some areas of the company, but not all. Here's another example of uncoordinated IT acquisition — a Navy with over 100,000 applications, many of which are redundant and unnecessary.

The PEO-IT must be at the center of this partnership. It not only translates between industry and users, it facilitates the big ticket items and helps incorporate them into the enterprise system. Using a new application is not just a matter of sticking it on the system. It impacts servers, as well as, other components. It also has organizational and cultural implications. For example, education and skills development can be 25 to 50 percent of an IT project's cost. Someone has to consider the big picture and that someone is the PEO-IT.

The Process

In 1994, the American Society of Civil Engineers designated the Interstate System of highways as one of the *"Seven Wonders of the United States."* It was testimony not only to its engineering, but also the cooperative partnership and massive coordination that made it possible. That's what is needed now to build a Naval enterprise system. It requires users to indicate where they need to go, industry to offer a realm of possibilities, and the PEO-IT to facilitate a solution and lay out a roadmap. It's a process that can lead to the next wonder.

Mr. Ehrler is the Department of the Navy Program Executive Officer for Information Technology (PEO-IT).

NKO EXPANDS ACCESSIBILITY

By Lt. j.g. Amanda Raymond, USN

New and Improved. It is a phrase that is heard everyday. Now, Navy Knowledge Online (NKO) can say it too. NKO, Sailors' one stop shop for career management, is now available on SIPRNET. Since its inception, over 90,000 users have registered in NKO, utilizing the site over half a million times, downloading over 330,000 documents. In June, the classified version of NKO was activated and administrators began migrating content to this site. Now communities that primarily use the SIPRNET, such as intelligence, cryptology and submarine, can connect with the Navy's Revolution in Training and take advantage of all the great tools that NKO offers.

"Obviously being able to access career information in a secure environment is essential to several ratings and communities," said Lt. Eric Morris, Naval Personnel Development Command Knowledge Management Program Manager. *"Likewise, this link is vital to our being able to take training to Sailors, instead of bringing the Sailors to the training."*

NKO's expansion doesn't stop with the classified side of the Navy. A new *lightweight* version of NKO is now being developed for ships. A pilot program started summer 2003 in conjunction with Naval Sea System Command's Distance Support Testing and operates without requiring Internet access. Success will be based on the ability to operate in a disconnected environment as well as the ability to replicate data to and from shore.

Navy Knowledge Online provides a multitude of services to foster and develop Sailors' careers and lives. *"This is a great opportunity for us to partner with NAVSEA and utilize the great work they have already done to create their distance support system,"* said Commander, Naval Personnel Development Command, Rear Adm. Kevin Moran.

To explore NKO tools and opportunities go to www.nko.navy.mil.

Lt. j.g. Amanda Raymond is in the NPDC Public Affairs Office.

Task Force Web...transforming interoperability through Web Services

By Cmdr. Scott Starsman, USN, Cmdr. Tina Swallow, USN and Lt. Cmdr. Danelle Barrett, USN

The Achilles' heel of military operations has traditionally been the lack of interoperability between Command and Control, Communications, Computers and Combat Systems (C5). While improvements have been made to the communications infrastructure, interoperability issues continue to plague the Department of Defense (DoD). Web Services technology is the Navy's solution for overcoming these systemic weaknesses.

To understand how Web Services will improve interoperability, it's important to look at some of the distinctive challenges the Navy has faced with its C5 infrastructure. In the 1980s, interoperability problems were highlighted by the inability of systems to communicate in fundamental ways at the First Layer (Physical Layer) of the Open Systems Interconnect (OSI) reference model. This was characterized by the use of different frequency bands by land, sea and air forces during Operation Urgent Fury in Grenada. As the Services overcame layer one issues and began using common radio frequencies which were deconflicted at the joint level, new issues surfaced.

Once the physical layer compatibility issue was understood and addressed, the next layer of incompatibility came to light. The introduction of operational level geographic displays such as the Joint Operational Tactical System (JOTS), the great-grandfather of the Global Command and Control System (GCCS), led to the requirement for collection and display of data from multiple disparate systems in a single, integrated environment. However, almost every system used unique and system-proprietary mechanisms to communicate data. Some used serial pipes over Ultra High Frequency (UHF) satellites, others used polling mechanisms over UHF and High Frequency radios, and others relied upon the parsing of formatted message traffic. Integrating these multiple data feeds became a tremendous systems engineering and management nightmare. Translators had to be built for the many protocols in use to create links between systems that were highly sensitive to changes in any of the feeder systems.

While these problems may seem esoteric to operators who consider only things that actively engage the enemy to be real combat capability, it must be noted that two frontline Aegis cruisers were put out of commission for several years due to interoperability problems between the two different shipboard combat systems: the Aegis Baseline 6 and the Cooperative Engagement Capability (CEC). The combat systems on both of these platforms were critical to Navy warfighting capability. CEC gathered and shared radar data from multiple ships but could not operate with the Aegis Baseline 6 systems and other legacy systems aboard ship. The problem was not in the operating functionality of either system, but rather that they failed to interoperate.

Ensuring systems interoperability requires that standards and protocols at the different layers of the OSI reference model be addressed with a focus on the enterprise system. The advent and widespread deployment of the joint Non-classified Internet Protocol Network (NIPRNET), Secret Internet Protocol Network (SIPRNET), Joint Worldwide Intelligence Communications System (JWICS) and IP-based coalition networks provide an infrastructure that yields compatibility up through the first four layers of the OSI model.

While DoD application owners have embraced IP networking, this capability has exposed yet another interoperability seam. While IP-enabled applications are easily connected, they are still largely unable to seamlessly share data. This is because they use application-specific mechanisms to format and transmit their data over IP networks. Web Services address incompatibility at Layers Six and Seven (Presentation and Application (see Figure 1)). They provide a mechanism for more rapid and reliable deployment of operational and business applications throughout the DoD enterprise. Historically, operational application development meant hard choices — it could be reliable, cheap or secure, but not all three. Implementing Web-Services architecture and technologies makes this paradigm obsolete.

Implementation of Web Services standards with a supporting enterprise architecture can increase the combat power of the U.S. military by addressing critical interoperability issues that continue to plague joint military operations. By employing Web-Services technology, systems that were previously incompatible as described earlier can become interoperable. A Web Services approach creates a layer of abstraction around the legacy system that will facilitate future development and integration efforts.

What is a Web Service and how is it different from the basic Web page technology that most Internet users are familiar with today? "Web Services" is a term often used in Web technology discussions yet it is seldom understood. For an industry example of Web Services, one need look only as far as your next trip. In a traditional Web environment, a traveler would visit Web sites for American Airlines, Delta, United, US Airways, etc., to compare prices and availability. Now the research is done automatically for a traveler by online commercial travel businesses such as Expedia.com or Travelocity.com. These Web sites are built on a Web-Services architecture. When a traveler wants to find the cheapest fare from Los Angeles to New York, he enters a few bits of information (i.e., departure city and date, and return city and date) and requests feedback. Web Services, using industry standards for describing data (Extensible Markup Language or XML) and moving data (Simple Object Access Protocol or SOAP) do the rest.

Web Services query the authoritative data sources maintained by the airlines and present the information back to the traveler in one Web frame with a common look and feel. No longer do travelers need to individually query a multitude of airline Web pages to do a comparative analysis. This type of powerful Web Services capability is what the Navy is developing as the infrastructure to

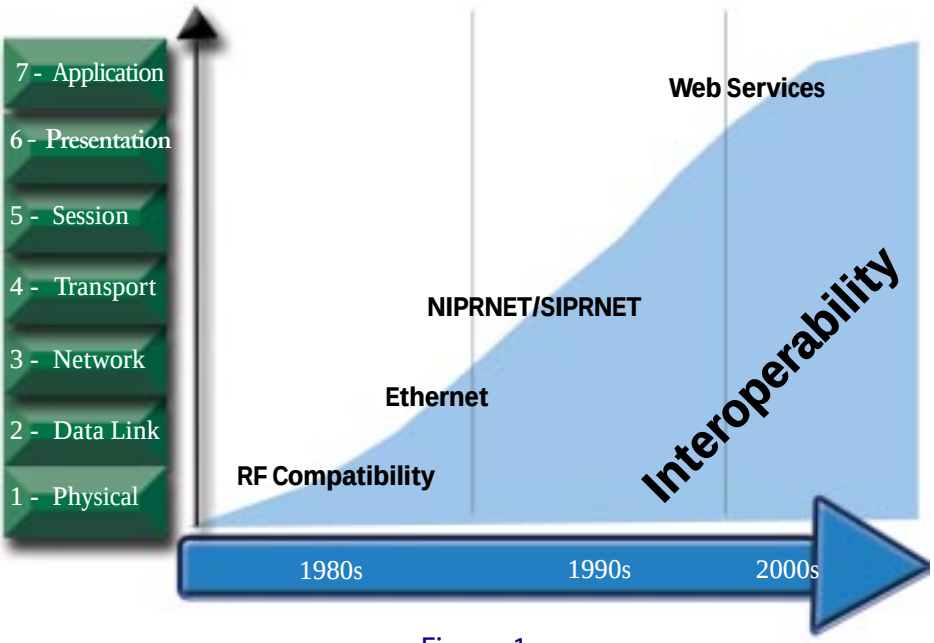


Figure 1.

support all business and operational applications. Web Services will give the Navy the capability to transform their strategic direction by maximizing the capability of our networks to more effectively make command and control and business decisions. The Navy will be able to reach more organizations, information, and do it more rapidly, securely and economically.

Web Services allow exchange of information more reliably and rapidly. At the heart of Web Services is authoritative data and its reuse. Today, there are many duplicative applications in the Navy, and as new functional requirements emerge new stovepipe systems and supporting databases are developed to support them. This duplicative infrastructure results in the same or similar data being maintained in many places, with no one-stop shopping for authoritative data. The result is duplicate, and often conflicting data that seeds user distrust with the entire data infrastructure. Web Services provide the key mechanism to expose authoritative data sources to external applications in an open and well-documented manner. When a command has a new requirement for information, it consults the directory of available Data Oriented Services (DOS) and consumes the applicable authoritative data — no costly new application, no duplicative data or infrastructure, and no lengthy procurement and development process. By using Web Services, it is possible to continuously update reportable information on a near real-time basis, avoiding the danger of making decisions based on stale information. Assigning functional owners to data sources and data elements will provide improved data reliability and accessibility throughout the Navy.

Additionally, in the old client-server approach to sharing information, updating legacy applications took time. Because Web Services are built on commercial standards, all development efforts begin with the same basic design for exchanging data and information. Commercial vendors sell programming products to facilitate development of Web Services based on industry standards. Also, the speed at which updates to services take place dramatically improves over the traditional client-server configurations, shortening the process from months to days.

Web Services enable exchange of information more securely. This is because Web Services use standard ports and protocols on communications equipment, thus mitigating the risks of exploitation by hackers or others with malicious intent. This creates a more secure information exchange over the traditional client-server applications that sometimes rely upon nonstandard and easily exploitable ports to access, replicate and synchronize data. Additionally, firewall concerns that plague any application using atypical ports are addressed as Web Services run over existing ports (typically HTTP/HTTPS). Web Services also allow developers to leverage a common security infrastructure, promising to eliminate the multiple logons that confront users today.

Web Services result in significant fiscal savings. Industry continues to develop products for converting existing legacy applications and databases into Web Services, making this conversion process extremely efficient and economical for commands. Cost savings will also be realized under this architecture by significantly reducing the redundant databases in use by the DON.

Implementation of a Web-Services environment also provides a return on investment. Traditional application development included funding for dedicated operating system hardware and software, separate application servers and database storage, client-workstation licensing and installation costs. In a Web-enabled environment, the operating system hardware and software, client-workstation application software and associated installation costs are avoided by leveraging the existing Web infrastructure. A recent assessment of industry practices by the MITRE Corporation indicated application developers could recoup the cost of Web enablement within the first year of transitioning a legacy application to a Web-based service. Program life-cycle development times and costs would also be reduced depending on the complexity of the application.

Web Services enable speed of transformation. Secretary of Defense Donald Rumsfeld places the transformation of the military as one of his top priorities for this administration. In an article he wrote for the *Washington Post* he states, *"The fact is that the transformation of our military capabilities depends on the transformation of the way the Defense Department operates."*[1] For the Navy, rapid change in the way it operates can be facilitated by a Web-Services environment, where data are exchanged and used in an unprecedented way. Web Services enable the transformation of mission accomplishment mechanisms to occur an order of magnitude faster than with legacy technologies. This will move the Navy in a strategic direction that positions the force to leverage the Semantic Web and achieve true knowledge management.

In April 2001, the Chief of Naval Operations stood up Task Force Web to lead this transformation within the Navy. The challenge was complex: move the Navy from its current stovepipe legacy application development to a cohesive and integrated enterprise of Web-based applications and services that are fully interoperable

and accessible by users anywhere, anytime in the world. Since then, Task Force Web has worked with commands throughout the Navy and DoD to provide a Web-Services framework for transforming legacy applications and building Web Services to meet new data exchange requirements. Examples of Web Services in use today include:

♦Readiness applications - The Director of Command and Control, Communications, Computers and Combat Systems at Commander, Atlantic Fleet has developed Web Services for all readiness and reporting functions. This results in easier and more reliable access to information for warfighters. These authoritative databases for readiness and reporting are now used by other commands to support their Web Services.

♦Meteorological applications - Fleet Numerical Meteorology and Oceanography Center (FNMOC) has exposed almost their entire line of products as Web Services. This open interface has been used to integrate METOC data into various operational applications in support of the Navy's FORCEnet initiative.

♦Commander Second Fleet Briefing Tool - Web Services are being used to provide the authoritative data to automatically update the Second Fleet status briefs to the commander. This results in increased fidelity of information being briefed and a significant time savings for the staff because the brief is automatically updated using Web Services. The commander does not have to wait for updates or travel to a specific location for a scheduled brief — he can view this information whenever and wherever he desires.

♦FORCEnet - During the fall 2003 FORCEnet Integrated Prototype Demonstration Web Services will provide a variety of information and capabilities including collaborative tools, warfare publications and lessons learned, geographic information and readiness data.

♦Medical/Dental Services applications - The Bureau of Medicine and Surgery uses Web Services to provide real-time medical and dental readiness data via XML. Individual and command medical readiness depends on personal demographic data mining and aggregation. Past operations relied on using "copies" of data provided by other systems. Naval Personnel Command owns these types of data. By invoking their Web Services, Naval Medicine can ensure that authoritative, accurate and reliable demographic data are obtained. This technique immediately eliminates duplicate data sources, lengthy update procedures and the grounds for questionable data. Eliminating the need to duplicate Web Service requests by other systems or applications for similar data, through brokering techniques, Naval Medicine is able to further this service within its environment to other applications that need demographic data such as the Dental Access System (DENCAS).

Task Force Web aligns with and facilitates broader Web-enablement efforts led by the Department of the Navy Chief Information Officer (DON CIO). These initiatives include the reduction of duplicative applications via the Functional Area Managers (FAMs) application rationalization process and the identification of data standards through the DON XML Working Group and the DON Functional Data Managers. The rapid pace of technological change and requirement for innovation in the DON necessitates that these efforts occur in parallel, as a serial approach would not enable the speed of transformation desired. The DON CIO will continue to evaluate emerging technologies, set standards and policy for Web Services and Web-enablement across both the Navy and Marine Corps, and will establish common-user interface to Web Services.

Web Services

√ Result in savings
√ Provide return on investment
√ Enable data exchange more reliably and rapidly
√ Enable data exchange more securely
√ Enable speed of transformation
√ Allow data to be used and exchanged in an unprecedented way
√ Will bring warfighting into the Information Age
√ Will remove interoperability barriers
√ Will improve operational and business processes
√ Will deliver decisive combat power

There are those who argue that Web-Services technology is not mature, the standards are still evolving and being an early adopter could result in the Navy choosing the wrong technology and being stuck with "Beta over VHS." However, Web-Services technology is being used throughout industry with increasing frequency. According to a Gartner Group report, there is growing momentum behind Web Services and they estimate that the software and information technology services opportunity specifically related to Web Services will reach $28 billion by 2005.

The Navy's ability to quickly integrate this new technology will overcome many obstacles previously encountered at different layers of the OSI reference model and will provide Navy warfighters and support personnel a more rapid, reliable, secure and economical information exchange. Implementation of a Web-Services-based enterprise architecture will enable the rapid transformation of the Navy from an industrial age warfighting force to a bona fide Information Age warfighting force. Perhaps more important, acceptance throughout Navy of a common set of Web development standards will remove interoperability barriers that have disrupted operations, both internally and with the other Services, agencies and multinational partners. This change in strategic direction will result in vastly improved operational and business processes and will provide the mechanism for delivery of decisive combat power.

References

1. Rumsfeld, Donald. "Defense for the 21st Century," *Washington Post*, 22 May 2003, p. 35.

Cmdr. Scott Starsman, USN, Cmdr. Tina Swallow, USN and Lt. Cmdr. Danelle Barrett, USN are Information Professional Officers formerly assigned to the Task Force Web.

When our warfighters make the call and ask that simple question, "Can you hear me now?" we need to be sure the answer is yes! It certainly sounds effortless in concept, and the technology solutions fielded by the Navy-Marine Corps team routinely respond to this global test. However, our Naval forces operate in vast and dynamic areas. The Navy-Marine Corps team is deployed in all parts of the world on a daily basis, and their environment may change hourly to adapt to commercial or military communication services and varied political climates. These factors often act as invisible barriers and challenges to completing a basic connection. Unheralded groups of people — spectrum managers and engineers — are in the background planning and coordinating to ensure our Sailors and Marines are able to operate efficiently and effectively in all corners of the globe.

In early 2003, many organizations under the Secretary of the Navy staff reorganized. At that time, the Secretary of the Navy established a new leadership team for Information Management/Information Technology (IM/IT) efforts across the Navy and Marine Corps. Describing it as "fundamental" to achieving a network-centric environment and knowledge superiority, the Secretary of the Navy provided enhanced operational insight to the DON CIO, Mr. Dave Wennergren, by designating Rear Adm. Thomas E. Zelibor, USN, and Brig. Gen. John R. Thomas, USMC, to serve as DON Deputy Chief Information Officer (Navy) and (Marine Corps) respectively. Together with the DON CIO, they have the responsibility to link vision and strategy to programmatic and budget guidance. In the Naval Enterprise spread across sea-air-land, spectrum issues have high visibility within this team and in their recommendations to the Secretary of the Navy.

This realignment includes a newly restructured Navy-Marine Corps Spectrum Center, formerly Naval Electromagnetic Spectrum Center, which provides enhanced and dedicated spectrum support to Navy-Marine Corps units. The success of projecting power and influence, as well as developing future Naval capabilities, relies on incorporating advanced spectrum technology. Spectrum needs are especially critical in executing the Naval Power 21 vision. The Secretary's involvement in domestic and international spectrum validates these efforts.

The DON Strategic Vision for Spectrum www.don-imit.navy.mil/spectrumCD/) is clearly committed to incremental improvements. The dynamic adjustment of the DON's spectrum vision responds to ongoing doctrinal changes. Overall, spectrum dependent systems should benefit by policy continuity. As Operation Iraqi Freedom shifts focus and scale, the spectrum scorecard is being prepared. Measuring voice and video communication, data transfer and weapon systems support will provide another input into the assessment process.

Civilian news correspondents reporting on Operation Iraqi Freedom identified wireless devices as key to U.S. warfighters' ability to execute their mission. *Forbes Magazine*, *the Wall Street Journal*, *the Washington Post*, and even *Wired Magazine* confirm the "force multiplier" effect that wireless extensions of the network-centric warfare concept provided. This is consistent with DoD analyses that showed a spectacular increase in spectrum usage from the Gulf War to the recent Iraqi conflict.

A challenge now rests in the realm of strategic planners to gaze into the next decade. The tasks are estimating spectrum growth and identifying possible network-centric warfare platforms to meet the capabilities needed by U.S. warfighters. Battlefield superiority is leveraged by spectrum availability. The DON CIO Spectrum team is addressing these elements with a view toward human factors, occupational training, spectrum planning and management tools, technology modeling, international regulation, and commercially compatible systems.

In a collaborative effort, partnerships with industry, academia, federal laboratories, the Office of Naval Research, the Naval Research Laboratory, Space and Naval Warfare Systems Command, the Marine Corps Warfighting Laboratory, and the Defense Advanced Research Projects Agency are underway. The mission is to jointly identify technology and protocols that might enhance spectrum reuse and increase spectrum efficiency. This effort to identify spectrum advantages for the Department also includes exploring emerging technology in materials, manufacturing, and artificial intelligence.

DON spectrum policy planners are also engaged with the National Telecommunications and Information Administration, the Office of the Secretary of Defense, the Joint Chiefs of Staff, and the Federal Communications Commission, working toward a constructive response to the Presidential initiative on spectrum policy in the United States.

This is the first in a series of articles that will explore the integrated processes of strategic spectrum planning and spectrum dependent system life cycle. Equipment certification, spectrum assignment, host nation approval, frequency planning and the roles and activities of the Department's spectrum policy and management organizations will be highlighted. We intend to spotlight the teams that support the warfighters and confirm that we can hear them now!

You can contact the DONCIO Spectrum Team at M_CYTW_SPECTRUMTEAM_UD@NAVY.MIL.

By Pen Stout, PMP

IT project managers could learn a lot from 17th century European merchants — both have experience with uncertain, *dangerous* ventures that promise great rewards. Over 350 years ago the merchants, with some help from a monastery of nuns outside Paris, founded the modern theories of risk management. Their revelation:

"Fear of harm ought to be proportional not merely to the gravity of the harm, but also to the probability of the event." [1]

To the merchants this meant they could calculate when their fleets would reach port and what returns they could expect. This allowed the merchants to maximize their odds over the long run to make dependable profits. As a result they could fund increasingly risky — but potentially profitable enterprises. This in part contributed to the growth of modern Western economies.

In the 21st century, IT risk management could translate to: backing up critical data, a secure power supply, documenting procedures and delegating authority when absent from the office. In short, we take precautions to secure our essential systems against the unexpected. In this the third article in our series on IT project management we will explore a practical approach to risk management using a common IT experience for an example: the design and implementation of an IT help desk.

A Practical Risk Management Process

Though risk management can involve complex statistics, the heart of the process is common sense: 1) Identify potential threats to the project cost, time and quality goals; 2) Assess each threat as the Parisian nuns suggested: determine both the gravity of the event and its probability of occurrence; 3) Create a proportionally justified plan of action for each threat. In other words, if there is a 1/10 chance of a $1,000 loss you might spend as much as $100 to eliminate the possibility of the threat; 4) Respond to actual problems as they occur. Rigorous risk planning will not make all the problems go away, but you will have fewer and you will be better prepared to handle them. Now let's use our IT help desk project to illustrate this process.

Step One: Identify Threats

It makes sense that once we know about a potential problem we can plan for it, but how can we know what problems we will encounter? Andrew, our IT help desk project manager, uses a common approach: he assembles a cross-functional group of project stakeholders and asks them point-blank, *"What threats do you see to our cost, schedule and quality goals?"* In other words — they brainstorm. Andrew practices two important principles of risk identification:

√ Involve a diverse group of stakeholders because both their perspectives and their tolerance for risk will differ.
√ Encourage them to be pessimistic about the project and to generate as many potential problems as possible.

Other tips for risk identification are: 1) Use a common format for describing risks that distinguishes the event from the impact. Here's a good format: Event causing impact. Andrew followed the format in this risk statement: "Database server infected with virus causing staff to field help calls without access to customer data"; 2) Brainstorm first — use open-ended, concept-expanding, "blinders-off" techniques to encourage divergent thinking and catch the risks that are not obvious; 3) Check results with more convergent methods. Once the open-ended brainstorming is complete, it is good practice to check results against lists of historical risks, particularly those that apply to your specific industry, organization and program. Some project managers find it helpful to create profiles of typical risks they are likely to encounter on different types of projects. Cast a very wide net during this initial stage. The problems that hurt the most are often the ones we didn't identify early due to ignorance, denial, myopic vision or lack of discipline.

At the end of this step you will have a long list of possible problems. Now it's time to separate the wheat from the chaff. Go through the list setting aside the low-probability, low-impact threats. Place these in a tickler file. Things change on projects so you will want to review these threats in the future to confirm they remain low-probability and low-impact.

Step Two: Assess Each Threat

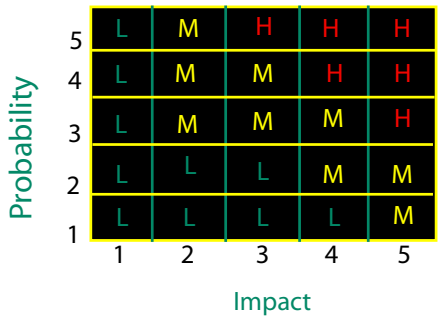
After setting aside the smaller threats you will still have a large number to manage, but you won't have the time and effort available to monitor all of them. How will you decide where to spend your limited time and money?

Andrew sorts the remaining threats into categories matching his functional teams: hardware, software, test, human resources, etc. Gathering the leads of each team together he asks them to analyze each threat in their respective subject areas. *"I'd like you to assign a dollar impact to each threat and an estimated probability of it actually occurring,"* he tells his leads. *"If we have experienced similar problems in the past, use our experience to improve your analysis."* To encourage accuracy, but discourage them from getting caught up in analysis, he continues, *"It will be very helpful if you can put actual numbers into the impact and probability estimates if the numbers can be supported and it doesn't cost too much to figure them out. But don't ignore the threats that would be too hard or costly to quantify. I'd like you to give them a subjective or qualitative estimate based on the Stout- Weidner Matrix ."* (Shown on the next page.)

Andrew has his leads collect the information required to calculate the "Expected Value." Expected Value is the product of the impact multiplied by the probability of occurrence. Here is an example: Kim identified one risk this way, *"If we have too many employees ill at one time, it causes poor response times for our users because we simply can't answer the telephones fast enough. Sometimes*

Stout - Weidner Probability Impact Matrix[2]

Level	Likelihood	Probability
5	Near certainty	>90%
4	Highly Likely	~60% - 90%
3	Likely	~40% - 60%
2	Unlikely	~10% - 40%
1	Remote	<10%



Level	Technical/Scope	Schedule	Cost[3]	Impact
5	Unacceptable	Can't achieve major milestone	> 10%	Unacceptable
4	Acceptable - no remaining margin	Slip in critical path or major milestone	7 - 10%	Major Impact
3	Acceptable - significant reduction in margin	Not able to meet deadlines; float consumed	5 - 7%	Moderate Impact
2	Acceptable - minor reduction in margin	Can meet dates if additional resources are available	< 5%	Some Impact
1	Little or no impact			

callers hang-up and we never hear from them again. I'm sure this is costing us." Andrew agrees that this is a project threat and asks Kim to calculate an Expected Value. Kim reports, *"I've discovered that we lose about $1,000 a day in long-term customer business due to hang-ups whenever we don't have the right staffing levels answering the phones. This usually occurs due to a combination of poor scheduling and illness. It has occurred, on average, about 10 percent of the time."* Andrew says, *"We can multiply the daily impact ($1,000) by the probability (10 percent) and calculate an Expected Value of $100 per day. The help desk will be open 365 days a year so our annual Expected Value for this threat is $100*365 or $36,500 a year. That is a significant risk we better manage effectively."*

Andrew will use the Expected Value of each threat to focus his limited risk management resources where they will do the most good. Andrew also recognized that the analysis of impact and probability can best be performed by the subject matter experts so he delegated these tasks to his leads. This will help the team speed through the analysis step. Andrew followed these risk management techniques: 1) Categorize the threats and delegate assessment to subject matter experts; 2) Assess cost of impact and probability of occurrence; 3) Base analysis on past history when possible; 4) Develop quantitative numbers where it is cost effective.

Additional tips for the assessment step include: 1) Accurate estimating takes time and good data; 2) Balance the need for accuracy with the cost of collecting information; 3) Estimating is better than ignoring a true threat; 4) Different stakeholders have different tolerance levels for risk. Take this into account when determining which risks to actively manage and where to draw the line. Keep in mind that active risk management requires time, effort and resources. These are usually limited so you must select which threats to manage. The size of the Expected Value is very useful for prioritizing and filtering.

Step Three: Response Planning

At this point Andrew's sponsor asks to see the list of threats. She looks it over with a frown. *"Andrew, this is still a very long list. I really don't know if this project is a good idea if so much can go wrong. What do you suggest I recommend to the Chief Financial Officer?"* Andrew responds, *"We are just getting to the big payoff in good risk management. The next step is to plan how the project team can reduce the surprises and control the uncertainty. Can you give me until next week to pull together a complete recommendation?"* His sponsor agrees, but advises that the CFO will want to know if the project still makes good business sense. *"Numbers and dollars will persuade me to take this further. And I need them by COB [Close of Business] Wednesday,"* she says.

When team members gather in the project room they find a list on the whiteboard: "Avoid, Transfer, Mitigate, Fallback Plan and Monitor, Accept and Reserves." Andrew opens the meeting, *"We need to plan how we can reduce our current risk exposure. This is a list of ways (Figure 1) regarding how we might respond to each threat. I'd like each of you to look at your risks, starting with those having the highest Expected Value, and determine which response makes the most sense. I will want to know: 1) What actions you propose? 2) How much they will cost to implement? 3) How much it will reduce the total Expected Value of your threats list? Once you are done we will get back together to decide which actions we can afford as a team and what to do about the remaining risk exposure."*

Response planning process

√Determine the best response for each managed risk. For each approach consider the initial Expected Value of the threat, the cost of the response and the predicted reduction in Expected Value. Select the most cost-effective response. For example: Kim proposes to reduce the probability of poor phone response due to poor scheduling by hiring a consultant to teach the team how to use the software already on their computers. Training costs about $6,000, but it reduces (mitigates) the Expected Value of this threat from $36,500 to $24,000 due to improved planning and coordination. She is also investigating wellness programs that might reduce staff sick days and the resulting poor response rates.

√Add all resulting actions to the project's WBS (Work Breakdown Schedule), budget and schedule to assure they are managed like any other project task.

Avoid
Avoid the threat entirely by changing the way the project is performed or by de-scoping the portion of the project that contains the risk element. Be careful with this approach. Eliminating the risky scope might disappoint a critical stakeholder or degrade the business reason for performing the project.

Transfer
Transfer involves moving the responsibility for a threat to another party usually by payment of a fee (outsourcing to a skilled expert) or a premium (insurance).

Mitigate
Take positive actions to reduce either the impact of a threat or the probability of it occurring. Mitigation usually requires positive action and has a cost. These actions should be reflected in your WBS as new work packages and controlled like any other part of your normal project.

Fallback Plan and Monitor
Sometimes it is too costly to mitigate or transfer a threat but we still want to keep an eye on it. In this case design a fallback plan to put in effect if the event actually becomes a problem. Then implement a method of actively monitoring for occurrence of the problem. Remember that not all problems announce themselves with a loud knock on the door. Some emerge slowly. These will require well-designed trigger events so monitoring can identify the emerging problem at the earliest moment. It is often easier to fix a problem early in its development before it gains momentum.

Accept
After trying to avoid, transfer or mitigate the threats to your projects, you will be left with residual risks, threats you can't reduce further. The final strategy is called acceptance. We will discuss the residual risks and decide together with our sponsor if we can accept them as a potential cost of doing the project.

Reserves
There are two types of reserves: Contingency and Management. Contingency reserves are funds held back for identified threats — the residual risks we have decided to accept (known). Management reserves are those funds held back for unidentified threats (unknown).

Figure 1. Andrew's handout for response planning

√ Review the total residual Expected Value. Determine a contingency reserve sufficient to cover this remaining risk exposure. Negotiate it with your sponsor.

Additional Tips: 1) Reserves should be held separate from the allocated performance budget. They are released as work packages only when a threat becomes an actual problem and requires corrective action; 2) Reserves usually cover financial impacts. Some scheduling approaches, such as Critical Chain Project Management, also attempt to provide extra time to cover the uncertainty in estimating task durations and project schedules. This time reserve is often called a buffer. In some organizations it is standard practice to sandbag or artificially inflate estimates and quotes to assure sufficient resources are available to cover the unexpected. Unfortunately such *fudge* usually gets *eaten* as work expands to fill the time or budget available. This is a poor management practice.

At the next meeting the team reviewed everyone's proposed threat responses. In a couple of cases, two responses to different threats conflicted with each other so the team worked out mutually supporting responses. The required actions were added to the baseline project plan. The next day Andrew brought his risk plan (Figure 2) to a meeting with his sponsor. She was pleased to see that the team had developed a proactive approach for many of the project threats and agreed to help negotiate a project contingency reserve with the CFO. *"He'll be very happy to see that you have identified and taken positive action to reduce the possible surprises in this project. He doesn't like project surprises because they reduce his ability to deliver on his promises to the CEO and Board of Directors. I'm sure he will agree to a good reserve if we can assure him it will not be eroded by poor performance. Oh, and have Kim give me a call. I think we can help with the financial justification for that wellness program if it really works."*

Step Four: Continuous Risk Management

One of Andrew's team members remarks, *"That risk management exercise was interesting, but now it's good that our focus is back on the real tasks of getting this help desk up and running."* Andrew responds, *"I'm glad you are concentrating on the project tasks, but I want to point out that the risk process doesn't go away just because we have performed an initial risk exercise. We will need to stay current with the risk effort just in case things change."* Andrew knows that all risks have not been identified or eliminated. He will follow these principles during the rest of this project:

- Make risk identification a regular part of project team activities.
- Ask for new risks at every project status meeting.
- Update the status of risks. If the probability or impact changes, maybe the response needs to change. If a response works and the risk event passes with no problem, note the success and retire the risk from the log.
- At key project points, such as when a phase ends or at significant changes in scope or personnel, perform another formal risk assessment.

Some Cultural Challenges

Some managers appear to be practicing denial as a form of risk management when they demand a "can do" attitude and accuse those focusing on threats of being pessimistic whiners. They may not understand that risk management is a well-formed, proactive process that delivers value by focusing limited resources on the reduction of surprise. When this is the case the politically savvy project manager will engage in tactful education emphasizing the benefits of improved control.

Implementation of the process will require discipline at several levels including the team and executive levels. The team must realize that risk requires constant attention coupled with routine effort to limit exposure. Executives will have to gauge the long-term benefits of active risk management and balance it against the short-term need to fund risk management activities.

Project leaders managing enterprises like aircraft carriers and

Future event	Poor phone response due to scheduling and illness	Database server down due to virus	Insufficient incoming telephone capacity during crisis
Probability	10%	5%	7%
Impact	$1,000 / day	$750 / day	$25,000
Expected value	$100 / day ($100 * 365 = $36,500 / year)	$37.50 /day ($37.50 * 365 = $13,688 / year)	$1,750
Total expected value of identified risks			$51,938
Response	Mitigate risk by training in scheduling software	Avoid risk by using a system not connected to the Internet and enforcing strict controls on all upgrades	Transfer risk by paying phone company to guarantee available bandwidth
Response cost	$6,000	$5,000	$1,000
Probability - after response	**6.6%**	**0.0%**	**2%**
Impact - after response	$3,650	$0	$25,000
Expected Value - after response	$24,000	$0	$500
Total response cost			$12,000
Total Expected Value			$24,500
Reduction in uncertainty			$27,438

Figure 2. Andrew's risk management breakdown - partial

nuclear power plants, which require very high reliability, have learned that uncertainty is the enemy of reliability. They successfully battle it by creating a culture of mindfulness at all levels. They use both formal and informal methods to constantly scan for potential problems while fully empowering an active threat response by all team members. Move your project team into this culture and deliver better performance with fewer surprises to your sponsor and customers.

Summary

Risk management is a systematic process that reduces the potential for unexpected project outcomes and improves the project manager's ability to meet or exceed the expectations of key stakeholders. It adds value to the project effort by increasing the probability that sponsors and customers will receive what they expect, when they expect it, for a price they expect to pay. Stripped to its essence, risk management is a set of methods for answering a few, common sense questions: What could go wrong? How wrong could it get and what can we do about it?

The ideas are simple. Like most things, the payoff is not in the knowing, but in the routine doing. Discipline and practical, routine application are key. Once you and your teams internalize the process and use it on a day-to-day basis you will find a sustainable improvement in project performance and stakeholder satisfaction. These simple ideas really work wonders because they get the odds working for you — rather than against you — and that's a truly sweet spot to be in.

References

1. Hacking, Ian. *The Emergence of Probability: A Philosophical Study of Early Ideas about Probability, Induction, and Statistical Inference.* Cambridge University Press, 1975. Chap. 8, p. 77. Hacking describes the activity of nuns working in association with Blaise Pascal at the Port-Royal monastery in 1662.

2. Derived from Eric Verzuh, Dr. Harold Kerzner and DoD.

3. These are considered acceptable variances in stable, mature, competitive industries with high selective pressure for accurate estimation. An overrun of 10 percent for a new publicly-funded stadium would be considered terrible, an aerospace firm may or may not consider a 10 percent overrun a problem depending on the type of program, while a software product developer would consider a 10 percent overrun to be the best performance he has ever seen.

Sources:

A Guide to the Project Management Body of Knowledge (*PMBOK® Guide*). Project Management Institute, 2000.

Risk Management Guide for DoD Acquisition. Defense Systems Management College Press, 2000.

Kerzner, Harold. *Project Management/Project Management Workbook.* Van Nostrand Reinhold, 1995.

Leach, Lawrence P. *Critical Chain Project Management.* Artech House, 2000.

Verzuh, Eric. *The Portable MBA in Project Management.* John Wiley & Sons, 2003. Chap. 6.

Weick, Karl and Sutcliffe, Kathleen. *Managing the Unexpected.* Jossey Bass Wiley, 2001.

Pen Stout is a project management consultant and trainer. He coaches firms as they implement project management and he conducts project leader training for the Versatile Company. Contact him via www.versatilecompany.com.

The Navy and the Defense Logistics Information Service

By Connie White and Debra Meyer

History

The history of the Defense Logistics Information Service (DLIS), formerly known as the Defense Logistics Services Center (DLSC), is intertwined with the Federal Catalog System (FCS), which began in 1914 when the Navy first published a Naval Depot Supply and Stock Catalog. At the time, this catalog was the nearest thing to a uniform federal stock catalog — perhaps that is why it became the Federal Standard Stock Catalog in 1929.

Susie Daugherty, a general supply specialist at the Defense Logistics Information Service, checks information for an outlet strip used by the Navy against information in the Logistics Remote Users Network.

During World War II, an enormous number of new items came into the military supply system. This influx often created duplication, lack of uniformity, and inefficiency because each military Service had its own methods of identifying, classifying and numbering its supply items. President Roosevelt recognized the costly duplication and the danger to both national security and the economy, so in 1945 he instructed the Bureau of the Budget to prepare and maintain a U. S. Standard Commodity Catalog. Several laws concerning government cataloging passed since then. The Defense Cataloging and Standardization Act of 1952, Public Law 436 was added in 1952 to establish the FCS.

In December 1961, the Department of Defense announced the change from the Armed Forces Supply Support Center (implemented in 1958) to the new DLSC and established the new organization in Battle Creek, Mich. Throughout its history DLSC continually evolved and transformed to better meet the needs of modern military logistics. The name itself changed from DLSC to the DLIS in 1998 to better reflect the expanded mission of providing logistics information through a wide variety of new media to supply the most current and accurate data possible to support the Services. Key to such efforts has been the DLIS commitment to keep pace with technological developments. At the same time, the appetite for new information and the dominant role it places in logistics has grown dramatically. Meeting those information requirements has led DLIS to develop new systems, use new media, and literally extend our reach around the world.

The decision to begin centralizing Defense cataloging in Battle Creek in 2000 was a milestone event in the DLIS evolution. Today, the FCS has matured into the source of standard logistics data used throughout the supply chain, primarily organized by National Stock Numbers (NSN). The numbers serve essentially as the DNA of materiel management — the key to information needed for acquisition, financial management, demilitarization, hazardous material, freight, packaging, risk of pilferage, etc. Such systems rely on the NSN-related data to make automated decisions about stockage and reordering.

The NSN is simply an official label (whose creation is restricted, by law, to DLIS). These items may be manufactured by scores of different companies, but if the item is ordered by NSN, one can be confident that the parts will work as expected. The NSN has official recognition by the U.S. government, as well as many foreign governments. Each number is the result of a careful review process called "item entry control." Cataloging can be viewed as the blending of a myriad of data about an item, including its name, manufacturing data (such as manufacturer's name and reference number), price, physical and performance characteristics, etc.

Cataloging Directorate - DLIS-K

This directorate is the hub of cataloging. Virtually everything useful to know about an item is collected and encoded by cataloging technicians in DLIS-K and entered into the DLIS computer system. The system then assigns the next available number, and a new NSN is born. There are approximately 7 million active NSNs. Catalogers perform maintenance on the database to reflect ongoing changes such as price, item management, manufacturer changes, etc. The NSN has wrought savings through inventory reduction and reduced acquisition costs. It assists inventory managers in budget reviews and the tracking of expenditures for supplies. The NSN supports readiness by answering the question, "What supplies exist where?" Its claim to fame is that it is the best tool ever invented to answer that question. Because an NSN so precisely identifies an item, it can be used to search automated systems worldwide in mere minutes.

Navy Cataloging - DLIS-KBN

The Navy Cataloging Division, DLIS-KBN, is the cataloging center for the Naval Inventory Control Points (NAVICPs). The division is comprised of an Air Section (DLIS-KBNA), which services NAVICP Philadelphia; and a Sea Section, (DLIS-KBNB) which supports NAVICP Mechanicsburg. Both sections provide services for the Navy's management of supply items such as Emergency National Stock Number assignments, maintenance actions for user information, classification and naming, characteristics and reference numbers, supply support request processing, and cataloging collaboration requests processing.

Both the DLIS Air and Sea offices are dedicated to providing logistics management data and services in support of the Navy by partnering with the Navy and industry early on in the acquisition process to establish NSNs and associated logistics data. This support continues during the sustainment phase with DLIS insuring ongoing data quality and maintenance support to the Navy. Additionally, the Air Section executes the Navy's Defense Inactive Item Program (DIIP) Focal Point duties.

The program was established to systematically consider inactive

items for elimination from the supply system when there is a high probability that no future requirements will occur. Items are identified and considered for elimination annually. For an item to be a DIIP candidate, it must be in the supply system or the Master Data File for at least seven years; have no demand for the past five years; have been under the Integrated Materiel Manager's (IMM's) cognizance for two years; and must have been under the IMM's cognizance for one year following the previous inactive item review. One Service or all can ask for an item to be removed. If all users request removal, the item becomes inactive and removed from the Federal Logistics Information System (FLIS).

The Sea Section prepares the Navy Afloat Shopping Guide (ASG). The guide is tailored to Navy afloat supply items. It contains more than 28,000 NSNs and 2,000 graphics. It is a valuable tool used to assist fleet personnel in identifying common shipboard or shore-based items in an easy to read format. It is distributed to over 3,000 recipients. The guide uses cataloging technical information and informally describes the items for everyday use by Sailors, storekeepers, shipbuilders and maintenance personnel. It contains information on critical Navy programs such as Buy Our Spares Smart, Plastic Removal in the Marine Environment, Level 1 Fasteners, Navy Habitability Equipment Program and Hazardous Material Control Office. The ASG consists of three volumes and is available in hardcopy, online and compact disc. It is published annually.

DoD EMALL

The Department of Defense Electronic MALL, known as DoD EMALL, is a single entry point for buyers to find and acquire commercial-off-the-shelf goods from suppliers and government sources. The Naval Supply Systems Command (NAVSUP), Mechanicsburg, Pa., entered into a partnership with DLA during February 2002 to use DoD EMALL as the online hosting and ordering system to support Navy Purchase Card users. To date, the Navy Fleet and Industrial Supply Centers (FISC) have added more than 289 commercial catalogs in support of historical Purchase Card buying patterns to meet the Navy's needs. Users can access DoD EMALL through One Touch Support (OTS) using a single sign-on.

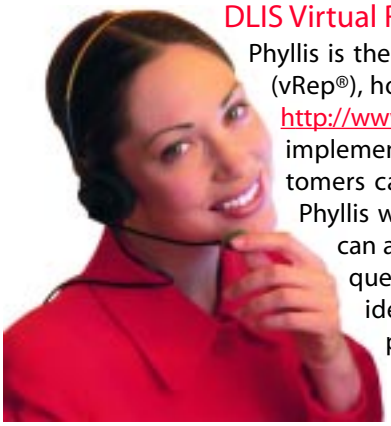
EMALL provides a number of benefits such as reduced prices through negotiation with the vendor for discounted prices that more closely match wholesale rather than retail. Secondly, the customer will often see competition on commercial items. The customer can identify mandatory source items such as those that must be obtained from Javits-Wagner-O'Day (JWOD) suppliers. The customer can also see Material Safety Data Sheets for hazardous items, if included by the supplier. Finally, customers are provided the convenience of online ordering, rather than the inconvenience of driving from store-to-store or calling vendors. Navy One Touch Support offering an initial 75 Navy commercial catalogs will be available through the Defense Medical Logistics Standard Support (DMLSS) sites. This data, previously provided on compact disc, is now provided to DMLSS sites via Extensible Markup Language, or XML-enabled Web Services.

The DLIS Battle Creek Customer Contact Center (BCCCC)

This center is a unique partnership of government and private industry dedicated to supporting the Armed Forces in war or peace. This partnership has led to the creation of a Customer Contact Center that exceeds world-class standards for customer service.

As the Global War on Terrorism was taken to the mountains of Afghanistan, warfighter calls to the BCCCC increased dramatically. In one instance, an Air Force C-5 aircraft was grounded in Spain due to a ruptured hydraulic line. In less than four hours, customer agents were able to resolve the issue so that the aircraft could continue its mission. Numerous calls for support from all military Services were also received as weapon systems pounded suspected terrorist strongholds.

DLIS Virtual Representative



Phyllis is the DLIS Virtual Representative (vRep®), hosted on the DLIS Web site; http://www.dla.mil/dlis, this service was implemented on May 21, 2001. Customers can ask questions as though Phyllis were a human agent. Phyllis can answer common or most frequently asked questions (FAQs) identified from an analysis of past customer contact responses. She provides the unique capability to help a customer navigate through layers of Web pages to locate the information they need by simply responding to a question phrased in natural language.

In addition, Phyllis has been successfully linked to several DLIS databases that provide a customer with the unique ability to ask a question and have the vRep® search the appropriate database for a response. Example questions are: What is the FSC 5820? What data is available for NSN XYZ? What is the CAGE Code for General Motors? Who is CAGE Code 80063? Phyllis can also provide suggested topics identifying to the customer what she knows about a given topic. A comical example is to ask her "Is CCR a rock band?" She will provide a list of what she knows regarding CCR, also known as Central Contract Registration.

The future of the vRep® is wide open. We are constantly evaluating customers' needs through telephone conversation logs and building the knowledge base. Additionally, the level of expertise we have achieved in vRep® development and management could be successfully expanded throughout the entire DLA organization.

As a field activity of the Defense Logistics Agency, DLIS creates, obtains, manages and integrates data from several sources. It shares this data through user-friendly products and services that support logistics operations throughout DoD, other federal agencies and elements of the private sector. DLIS expertise in cataloging and information management makes it an important contributor to electronic commerce between the U.S. government and its many suppliers. For additional information about DLIS, visit http://www.dla.mil/dlis or call (269) 961-7019.

Connie White is the branch chief for Navy Cataloging at DLIS.
Debra Meyer is a section chief for the Navy Cataloging - Air Section at DLIS.

Access Approved: Biometrics and Smart Cards Open Doors to Improved Efficiency

By Capt. Robert Conway, USNR, Fleet Liaison Officer, DON eBusiness Operations Office

DON eBusiness Operations Office

The DON eBusiness Operations Office is an innovative eBusiness center encouraging the adoption of eBusiness technologies in the Navy and Marine Corps by providing funds and management expertise to requesting commands. The DON eBusiness Operations Office mission is to find new ways to use eBusiness technology to support warfighters, improve work processes, enhance quality of life and increase efficiency. The eBusiness Operations Office accepts ideas for pilot projects from any Navy or Marine Corps command. Ideas are screened for impact and scalability to the entire DON, and selected projects are funded. To date, 53 pilot projects have been funded in this way. The eBusiness Operations Office provides project management expertise for each pilot project.

eBusiness Pilot Project

The DON eBusiness Operations Office and SPAWAR Systems Centers Norfolk and Charleston are working with the DoD Biometric Management Office and the Department of the Navy Chief Information Officer (DON CIO) to determine future technologies that the Common Access Card (CAC) will support. The CAC (sample shown at right) contains multiple data storage technologies, including barcode, magnetic stripe and contact smart chip, which allow cardholders logical access to computer networks and can be used for physical security for controlled areas.

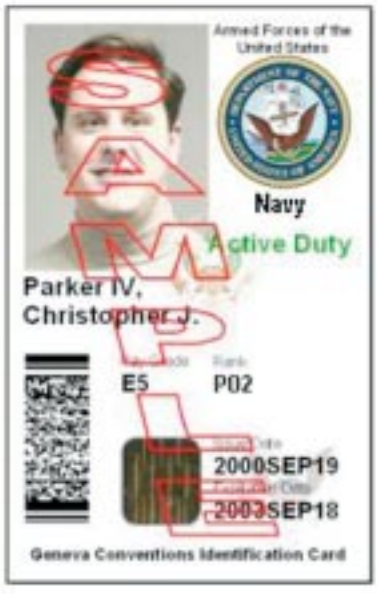
There are thousands of physical access control systems deployed throughout the Navy. The convergence of the CAC and biometric technology has the potential to enhance physical access control security with the benefit of integrating seamlessly into the legacy systems. The cost of upgrading existing physical access control systems to utilize biometrics is reduced by reusing much of the existing security system infrastructure.

Biometric technologies are being incorporated in secure personal identification and verification systems. Biometrics are automated methods to recognize a person based on a physiological or behavioral characteristic. These methods include fingerprints, voice patterns, iris scanning, finger and hand geometry, facial recognition and other techniques. The Navy and Marine Corps are evaluating several biometric applications, some of which include the use of smart card technologies for physical access to certain areas and buildings. These smart card applications are being evaluated to help shape the future of the DoD CAC card.

Biometrics in Access Control

In the past year, the DON eBusiness Operations Office in Mechanicsburg, Pa., partnered with SPAWAR Systems Center Charleston to test two different biometric access systems. Both projects included smart card technologies with biometrics. The tests were executed at SPAWAR Systems Center Norfolk, and Camp Smith, Hawaii. The Camp Smith project, which included existing U. S. Pacific Command Headquarters (USPACOM) spaces (shown in the photographs above), assisted in determining which access control technologies to include in the new PACOM Headquarters building currently under construction. In both locations, stronger user authentication and a non-obtrusive method of achieving access control were desired.

Photographs at right illustrate tests conducted at U.S. Pacific Command Headquarters (USPACOM) spaces. Tests assisted in determining which access control technologies to include in the new PACOM headquarters building currently under construction. Sample Common Access Card (CAC) shown below.



Both projects tested "contactless" smart card technology. Many existing card readers require the card to be swiped through or inserted into a card reader to retrieve information stored on the magnetic stripe on the card, or on a chip. The physical wear shortens the life of the card, requiring more frequent reissuance of cards. Recent advances in technology store access information on a chip and use an integrated radio frequency transceiver to transfer data without the need for direct physical contact. This

technology is commonly referred to as a contactless card. The technology is available in a standard card size or in the form of a Radio Frequency Identification (RFID) tag that can be attached to cards and other devices.

When properly implemented, biometrics can exploit technology to reduce manpower. Biometrics can also be very cost effective, particularly when existing infrastructure is reused and the system uses an open architecture that allows use of many technologies. When integrated with the CAC, the system is very unobtrusive, and nearly transparent to users.

Technology Standards

Balancing the existing installed base with a contactless requirement, the SPAWAR Norfolk team piloted a card configuration with two contactless technologies. The first was a proximity smart card from HID Corporation for use with legacy systems. The second used the new ISO 14443A, defined by the International Organization for Standardization, for contactless and dual interface smart cards, known as MIFARE®. With a large worldwide installed base, it is a proven RF communication technology for transmitting secure data between a card and reader. It is also an open platform, available to any company willing to develop compatible products under conditions of common industry practice. This will ensure many manufacturers provide competing technologies all based on an open standard. This competition makes feature-rich products available at lower cost to the Navy and Marine Corps.

The federal government standard for future systems is ISO 14443 parts 1 through 4, which is equivalent to NIST IR 6887, defined by the National Institute of Standards and Technology Interagency Report. To enhance the level of authentication for entering controlled spaces, the Norfolk project team added fingerprint biometrics. The biometric templates, a mathematical representation of the fingerprint, were stored on a chip on the smart card. This had two significant benefits. First, it eased concerns about the use of fingerprints, since the entire verification occurred between the smart card and the reader. That is, the reader was simply verifying that the fingerprint read by the biometric scanner matched the mathematical representation of the fingerprint provided by the card. This eliminated the need to transfer employee fingerprint files over communications lines each time an employee entered a space thus providing personal security to employees as well.

The second advantage was that the existing infrastructure remained unchanged: there was no need for additional servers, databases and communications lines to verify fingerprints. Using the existing infrastructure reduced the cost of the pilot by over 60 percent. The existing card readers were upgraded to contactless smart card and fingerprint readers.

The Camp Smith project also used the current security infrastructure. It used contactless smart card technology and multiple biometric measurements including fingerprints and hand geometries (shown above). The original access system included a badge-based access control system layered in depth throughout the spaces. The major deficiency was that system verified the authenticity of the badge and did not verify the identity of the individual using the badge. Compromise of this system would disable access control and require the use of manned access control points.

At right: Illustration of hand geometry identification for physical access control.

Since current guidelines prohibit modifications to the CAC, the Camp Smith project used a modular RFID tag to store the biometric credentials. The RFID tag was attached to a plastic sleeve holding the CAC. Many systems currently use magnetic badge swipe and PIN entry via a keypad. The use of biometrics allows access without entering a PIN. The project provided useful metrics for evaluating the feasibility and implications of incorporating contactless technology into future releases of the CAC.

"These projects were a major step in testing biometrics coupled with the CAC as a smart card," stated Rick Caldwell, Pilot Project Manager at the DON eBusiness Operations Office. He added, "We tested two different types of biometric systems and contactless smart cards in different locations, with different legacy systems, and even tested to the new open architecture standard. That's quite a big step in such a short time, and we did it for a very small investment. We learned a lot about fielding these systems, and the problems and solutions you can only experience by actually doing [testing] it with people. When the Navy and DoD are ready to deploy these technologies, we can use the knowledge and experience from these pilot projects to make these solutions work enterprise-wide. That's the real power and value of doing a pilot project before full deployment."

Systems Center Norfolk Testing

In Norfolk, physical access using the CAC with a contactless smart card reader and fingerprint reader was evaluated over a two-month period. Of 260 users, only two had initial difficulty enrolling biometrically, and they were able to fully participate in the pilot. Users were pleased with the system with some mild concerns about how their biometric data were being used. Those concerns were resolved by explaining that the biometric template resides on a contactless chip on the user's personal smart card and not in a database. Biometric awareness increased by 44 percent during the evaluation. Users were granted access 97 percent of the time within one to two attempts. These results were in alignment with the users' expectations.

SPAWAR Systems Center Norfolk management was pleased with the backwards compatibility of the solution and the enhanced security from the layered approach. The pilot is still in operation, and SPAWAR Norfolk is considering using the same approach to enhance security for their warehouses and SIPRNET spaces.

Camp Smith Testing

In Hawaii, some problems were encountered with fingerprints due to a recognized phenomenon: some women of Asian heritage have fingerprints with very low ridges. This can cause more false rejections than expected, denying access that should be authorized. Creating a unique configuration for these individuals solved this problem. Another cause for fingerprint errors can be occupation or hobby related. In one case, an individual who was an avid fisherman presented difficulties for the fingerprint reader simply because the constant use of his hands wore down the fingerprint ridge structure. The systems at Camp Smith are continuing in operation and users and security personnel are pleased with the unobtrusive nature of the system, and with the enhanced, layered security it provides.

Project Results

The results of both projects were very encouraging. The complete report on the Norfolk installation is available on the DON eBusiness Operations Office Web site, www.don-ebusiness.navsup.navy.mil. The report for the Camp Smith installation will be added to the site in the near future.

Future Applications

There is enormous potential to reduce the number of physical security tokens used throughout DoD to move toward standard interoperability. In these projects, the decision to use the CAC as the primary token in physical security has generated healthy debate between the physical security community and the CAC community. The challenge for the Navy and Marine Corps is to standardize the technology that supports a variety of installed electronic security systems, enhances the level of security and is scalable throughout DoD. There are many more technologies to evaluate, and operationally test prior to procuring the next generation of CAC.

The Norfolk and Camp Smith projects demonstrated that biometrics in an open architecture, embedded chip can meet the functional demands of the physical security community for access control. There are other maturing contactless and biometric technologies that need to be evaluated. As with all technologies, there are vulnerabilities that need to be investigated, and efficiencies, benefits, risks and costs to be weighed. As the Navy and Marine Corps move ahead and adopt more high-tech solutions at an accelerated pace, the lessons learned from these pilot projects serve to guide aggressive adoption of biometrics.

Other eBusiness Solutions

As with the biometric technology pilot projects, the DON eBusiness Operations Office has delivered new technologies to many areas, including communications, readiness, training, maintenance, logistics, engineering and procurement. One technology tested by the Seabees (Naval Construction Force) in Operation Iraqi Freedom, provided a secure battlefield network for transmittal of text and photographs, resulting in greatly enhanced combat communications.

Information on how commands can submit eBusiness ideas for pilot funding is available on the DON eBusiness Operations Office Web site, www.don-ebusiness.navsup.navy.mil.

Interested in pursing a Masters or Doctorate? If you are, then you should read on.

The Information Assurance Scholarship Program (IASP), now in its third academic year, is a relatively new program that is expected to grow in the coming years to meet the increasing demands for information technology professionals with an information assurance focus. IASP was authorized by Chapter 112, Title 10, United States Code, to respond to DoD's recognized dependence on information technology for warfighting and the security of its information infrastructure.

This year, DoD will focus on enabling qualified civilians and military members to participate in both full-time and part-time study to complete master's degrees or to begin full-time doctoral programs in information assurance disciplines.

Department of the Navy (DON) civilian and military members may apply for IA scholarships through their Service chain-of-command to the DON CIO. Detailed instructions on the DON nomination process for a scholarship are available at www.doncio.navy.mil/iasp and general information is available at www.dod.mil/nii/iasp. The institutions offering full-time academic programs leading to a master's or doctoral degree are the Information Resources Management College (IRMC) of the National Defense University (NDU) in cooperation with IRMC's partner universities located throughout the United States, the Naval Postgraduate School (NPS) and the Air Force Institute of Technology (AFIT). Part-time academic programs leading to a master's degree are available only through IRMC and selected partnering institutions. These part-time programs may be completed in residence or via distance learning. Partner universities continue to grow as the program matures. The DoD IASP Web site www.dod.mil/nii/iasp is the best source for the most current information.

The cost of tuition, fees and books at IRMC and IRMC's partnering institutions, and at NPS and AFIT will be covered by the program. Additionally, TDY expenses are funded for students attending the full-time IRMC program. Any other TDY and/or PCS costs must be covered by the nominating component. Participants will continue to receive their military pay or civilian salaries from their component throughout the course of study. In the future, DoD may expand the program to include associate and undergraduate degrees, and certificate programs, as permitted by the statute.

For more information go to www.doncio.navy.mil/iasp.

The previous article in this series provided an overview of the Capability Maturity Model Integration[SM] models (CMMI[SM]). This article will focus on appraising organizational practices using the CMMI[SM].

There are several possible reasons for performing an appraisal: 1) Identification of improvement opportunities or weaknesses; 2) Evaluation of the performance risk of an organization; 3) "Certification" of a Maturity or Capability Level (i.e., determination of a rating for publicity purposes).

With regard to the latter, it is important to note that there is no official certifying body for the various CMMI appraisals. The strongest statement that should be made is that an appraisal was conducted by a specific team under certain conditions and a given rating was determined.

Beginning process improvement: An organization just beginning process improvement should do some sort of appraisal to determine where their major problems are so they can address the most critical issues first. This can be a fairly simple review of organizational processes relative to the CMMI, done either by the organization itself after study of the reference model, or led by an experienced process improvement professional.

Benchmarking: After an organization has been doing process improvement for a while it may want to verify its progress by doing a formal appraisal. This can result in the determination of a Maturity Level or Process Capability Profile if so desired.

Source selection: An organization considering using a supplier may want to determine the risk that the chosen supplier will not be able to meet its commitments. One way of doing this is by using an appraisal to determine the maturity or capability of the supplier's processes.

Monitoring: An organization may want to understand over time how its process improvement program is progressing. Or if it has selected a supplier, it may want to verify supplier performance.

There is a range of appraisal methods available, ranging from less costly techniques such as a self-appraisal or mini-appraisal to a full-blown SCAMPI[SM] (Standard CMMI[SM] Appraisal Method for Process Improvement). In choosing a method the organization should consider the appraisal objectives and desired outputs, the accuracy of the results, the cost to prepare for and conduct the appraisal, and the anticipated extent of organizational disruption.

The Appraisal Requirements for CMMI, Version 1.1 contain requirements considered essential to appraisal methods intended for use with CMMI models. It defines three classes of appraisal methods: A, B and C. Class A, SCAMPI, is suitable for benchmarking and comparison, while Classes B and C have more limited objectives. Table 1 provides a comparison of the methods.

Table 1. Characteristics of CMMI Appraisal Method Classes

Characteristics	Class A	Class B	Class C
Amount of Objective Evidence Gathered (relative)	High	Medium	Low
Ratings Generated	Yes	No	No
Accuracy	High	Medium	Low
Resource Needs (relative)	High	Medium	Low
Cost	High	Medium	Low
Team Size (relative)	Large	Medium	Small
Appraisal Team Leader Requirements	Lead Appraiser	Lead Appraiser or trained and experienced person	Trained and experienced person
Organization Disruption	High	Medium	Low

How does an organization know which appraisal method to use and when? Choosing an appraisal method, like choosing metrics, should be conditioned by the questions you want to answer. Do you want to benchmark current processes (rate at a Level), develop a process improvement program, check on improvement progress, allocate improvement resources or select a subcontractor? Various appraisal methods have significantly different costs, accuracies, and impacts on the organization, as noted in Table 1. Table 2 describes the applicability of various appraisal methods.

What is Involved in Performing an Appraisal?

Any appraisal generally has at least two objectives:

1. Gather accurate data in an efficient, minimally disruptive way.
2. Help to identify and prioritize improvement opportunities or weaknesses.

These objectives can be achieved in a number of different ways, with varying degrees of cost and accuracy as noted above. Sometimes a third objective is appropriate:

3. Signal to the organization that a new way of life is beginning.

This third objective is particularly applicable when the organization wants to institute a change in its culture — its customary way of doing things. In this case, disruption is good.

Most appraisals have two major categories of outputs:

Findings

- Provide an accurate picture of processes, using the CMMI as a framework.

Recommendations

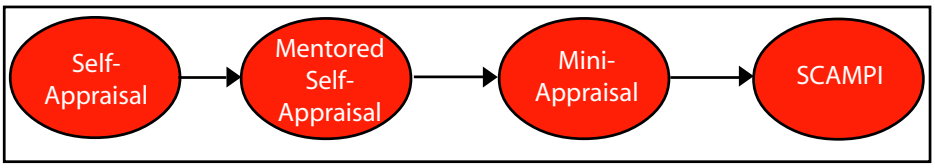
- Provide guidance on process improvement activities appropriate to the current state of the organization's process.
- Provide a framework and catalyst for action.
- Build ownership of results.
- Develop organizational commitment and energy.
- Sustain sponsorship and establish commitment.
- Facilitate continued process improvement.

An organization embarking on a process improvement program should consider a phased sequence of appraisals to provide identification of appropriate improvement opportunities at a relatively

Table 2. Applicability of Appraisal Methods

Type	Basis	Begin Process Improvement	Benchmark	Source Selection	Monitor
Self-appraisal (Class C)	Self-study questions, gap analysis	Yes	No	No	Yes
Mentored Self-appraisal (Class C)	Group interview	Yes	No	No	Yes
Mini-appraisal (Class B)	Group interview document reviews	Yes	No	Maybe (mini-Source Selection SCAMPI)	Yes
SCAMPI (Class B)	Questionnaire or other instrument, interviews, document reviews	Yes (But this is an expensive way to begin)	Yes	Yes (Source Selection SCAMPI)	No (Too expensive)

Figure 1.



low cost. Beginning with a self-appraisal (see Figure 1) followed by a mentored self-appraisal helps the organization establish its process improvement program. A mini-appraisal can be used to determine progress and readiness; a full Class A SCAMPI can be used for benchmarking and determination of the organization's Maturity Level or Capability Profile.

Appraisal Activities

An appraisal is a series of planned steps designed to elicit information about organizational practices relative to a reference model. It has a life cycle similar to any other project. It typically includes a review of documentary evidence and interviews with managers and practitioners to ascertain how processes are implemented within the organization. Table 3 describes an appraisal project life cycle with the SCAMPI activities associated with the various appraisal steps.

Preparing For an Appraisal

The most critical issues in planning and preparing for an appraisal are establishing high level senior management sponsorship and carefully defining the objectives and scope of the appraisal. The business needs and goals of the sponsor have a major impact on how extensive an appraisal needs to be. The major determiners of appraisal scope are: 1) the questions the sponsor wants answered and the actions he is anticipating taking as a result of the appraisal; 2) how much he is willing to pay; and 3) how much disruption the organization can afford to support the appraisal. The appraisal team leader, organizational unit coordinator and appraisal sponsor need to meet fairly early (possibly by telephone or video teleconference) in order for the team leader to ensure that the sponsor fully understands what an appraisal involves and what kind of results he can expect.

The organizational unit coordinator is in charge of all the appraisal logistics for the organization being assessed and is a member of the organization being assessed. The organizational unit coordinator has responsibilities in areas of sponsorship, appraisal participants, members of the appraisal team, facilities, equipment and supplies, documentary evidence and team support.

A major decision to be made is which Process Areas will be reviewed in the appraisal, and how much of the organization will be examined. This is particularly critical if the organization is located at more than one geographic site. The form of results documentation also needs to be determined. Will just the final briefing slides be sufficient, or is a formal written report also desired? Does the sponsor desire recommendations as part of the final findings briefing?

There are two different approaches to collecting the data required for an appraisal. A verification appraisal requires the organization to provide a detailed mapping of documentary evidence to CMMI practices. That mapping is then verified by the appraisal team. In a discovery appraisal the team does most of the "digging" to determine evidence in support of the model practices. Choosing whether to do an appraisal in verification or discovery mode is a critical decision which has a major impact on the effort required by the organization and the team.

If a Class A SCAMPI is being performed, a number of site personnel receive appraisal team training provided by the Lead Appraiser. Training more members than are required will allow for backup in case some people are not able to participate in the onsite appraisal. Appraisal team members should be:

- Very knowledgeable about the organization
- Well-respected within the organization (particularly those team members who are part of the organization being assessed)
- Motivated to improve the organization's software process
- Willing to accept change and have the ability to help implement change (be a change advocate or change agent)
- Sensitive to people and able to address questions to appraisal participants in a clear and nonthreatening way
- Capable of making a positive contribution as appraisal team members

Team members should be opinion leaders (other people listen to what they have to say) as well as team players. Members should preferably have at least 8 to 10 years experience as software or system engineering professionals. They should represent a wide variety of process areas such as requirements, design, implementation, test, configuration management, metrics, quality assurance and process definition.

Site appraisal team members must not occupy positions within the organization that may lead to a conflict between the appraisal principles and their job function. For example, if appraisal participants believe that information they volunteer has the potential to affect them adversely after the appraisal, they may not speak freely or not speak at all. Nor should there be a conflict between their function on the appraisal team and their regular job function. To help ensure a free flow of information, organization appraisal

Table 3. Appraisal Project Activities in order of performance

Appraisal Steps	SCAMPI Version 1.1 Activities
I. Plan and Prepare for Appraisal	
A. Scope Appraisal	1.1 Analyze Requirements
B. Plan Appraisal	1.2 Develop Appraisal Plan
C. Prepare Team	1.3 Select and Prepare Team
D. Prepare Participants	1.4.1 Prepare Participants
E. Administer Instruments	1.4.2 Administer Instruments 2.1.1 Examine Objective Evidence Documents
F. Review initial set of documents	1.4.3 Obtain Initial Objective Evidence 1.4.4 Inventory Objective Evidence
G. Determine readiness	1.5.1 Perform Readiness Review
II. Conduct Appraisal	
H. Conduct Opening Meeting	(No specific activity applies)
I. Observe Presentations	2.1.2 Examine Objective Evidence from Presentations (optional)
J. Review Documents	2.1.3 Examine Objective Evidence from Documents
K. Conduct Interviews	2.1.4 Examine Objective Evidence from Interviews
L. Consolidate Information	2.2 Verify and Validate Objective Evidence 2.3 Document Objective Evidence
M. Prepare and present draft findings	2.2.3 Validate Practice Implementation Gaps
N. Rate: Prepare Final Findings	2.4.1 Derive Findings and Rate Goals 2.4.2 or 2.4.3 Determine Maturity or Capability Levels (depending on which was used) 2.4.4 Document Appraisal Results
III. Report Results	
O. Present Final Findings	3.1.1 Present Final Findings
P. Conduct Executive Session	3.1.2 Conduct Executive Session(s)
Q. Wrap-up	3.1.3 Plan for Next Steps 3.2 Package and Archive Appraisal Assets
R. Prepare Final report (optional)	3.1.3 Plan for Next Steps

team members should not hold positions that involve any of the following activities: 1) Acting as manager of a project included in the appraisal, nor the manager of such a person; 2) Working on or directly involved with reviewing or supporting a project under assessment; 3) Currently serving in a software audit or quality assurance position for any of the projects under review. This last requirement might be waived, depending on the relationship between QA and the projects. However, keep QA representation to one or two people at the most. Too many QA personnel could create an audit atmosphere.

Note: Depending on the organization culture, the Lead Appraiser may decide it is possible to violate some of the above restrictions without impacting the integrity of the appraisal.

Action Planning

Action planning is a necessary follow-on to any appraisal and the lead-in to implementing changes. The organization needs to review the findings and recommendations and decide what actions it will take as the next step in the improvement process. The plan sets the stage and establishes the priorities for implementing the next set of changes. That action planning should be based on the organization's strategic objectives, the critical "market drivers," those factors which ultimately determine success or failure.

Business leaders determine critical business drivers and associated strategic objectives to answer the question, "What do we want to achieve as an organization?" Action plans based on business goals and appraisal findings and recommendations drive the improvement project. An improvement project should be managed like any other project (but not Level 1). Leaders should model the expected behaviors and prepare the organization for the upcoming changes. In developing the action plan three factors should be considered:

Results - What desired results do we want to achieve? How much improvement can we expect? Desired results should be prioritized by impact on the organization.
Needs - What do we need to change to effect this result? How soon do we need this result to improve? Needs should be prioritized by urgency.
Activities - What tasks do we expect to be done to effect the needed change? Can this be done in time to get the desired results? Activities should be prioritized by cost/feasibility.

These three factors can then be combined (algorithmically, if desired) to come up with a prioritized list of actions to be implemented.

Process Action Teams (PATs) are a good choice for actually defining and implementing specific process improvements. Getting PATs up to speed quickly is easier with a defined process. One such process is documented in ETVX (Entry-Task-Verification-eXit) format, which is also used by the team to document the model of the process they are working on. In addition to assorted templates and guidelines for both project outputs and for project planning and status reporting, each step in the process has entry and exit criteria, roles, measures, standards and tools.

Conclusion

The first two articles described the CMMI models and associated appraisal methods. The next article will deal with issues involved in implementing the CMMI and transitioning from the Software CMM to the CMMI.

Sources:
Appraisal Requirements for CMMI. Ver.1.1. CMU/SEI-2001-TR-034. December 2001.
Standard CMMI℠ Appraisal Method for Process Improvement (SCAMPI℠). Ver. 1.1. Method Definition Document. CMU/SEI-2001-HB-001. December 2001.

Richard B. Waina, P.E., Ph.D., Principal of Multi-Dimensional Maturity, has over 35 years of IT experience. He worked for five years at White Sands Missile Range, and worked on a number of missile programs at Hughes Aircraft Company, including Maverick for the USAF, Phoenix for the DON and TOW for the USA. At EDS he was responsible for deploying process maturity assessment methodologies globally. Dr. Waina is a SEI-authorized CMM and CMMI Lead Assessor/Appraiser and Instructor for the Introduction to CMMI. He has conducted over 70 CMM/CMMI assessments in nine countries since 1990. He holds engineering degrees from Carnegie Mellon University, New Mexico State University, and Arizona State University. The Multi-Dimensional Web site is www.mdmaturity.com.

Defense Collaboration Tool Suite Enables Warfighter Planning During Operation Iraqi Freedom

The Defense Collaboration Tool Suite (DCTS) is the DoD/Joint Staff tool suite for interoperable collaboration built to standards mandated by the Office of the Secretary of Defense (OSD). Its capabilities meet operational and administrative requirements across echelons, joint mission areas and national boundaries. The Collaboration Management Office (CMO), and DISA's Center for Combat Support Capability, serve as the DCTS program office.

DCTS provides combatant commands, military Services and Defense agencies with an interoperable, real-time, asynchronous collaboration capability that includes voice and video conferencing, document and application sharing, instant messaging, virtual meeting, and whiteboard capability in support of defense planning.

DISA was initially tasked by the Joint Staff to field 40 DCTS systems to the nine combatant commands, but once the value of DCTS was recognized the requirement grew. Initial fielding of the original DCTS sites began in April 2002. A little more than a year later DCTS is installed at 104 sites worldwide, and another 51 sites will be installed by the end of 2003 at all combatant commands, their major components and in all military Services.

"The DCTS program management organization serves as the proponent for DCTS and leads and manages the DCTS effort DoD-wide," said the program manager for DCTS. "It ensures that DCTS policies, processes, plans, programs and procedures are fully synchronized, integrated and institutionalized." The DCTS PM's management strategy is designed to be as streamlined as possible while maintaining the discipline of configuration management required to have an effective and secure collaboration system. The system is designed to enhance the exchange of information and meet current and emerging operators' needs for collaboration.

Initially, U. S. Central Command (CENTCOM) was provided with six DCTS systems by DISA to support operations within their area of responsibility. However, as war preparations progressed, CENTCOM recognized the benefits of DCTS and purchased a number of additional systems. At the onset of Operation Iraqi Freedom (OIF), 14 DCTS systems had been fielded in geographically dispersed rear and forward CENTCOM and component locations.

After hostilities began, DISA provided another DCTS system to support mobile military operations. In addition to CENTCOM staff, elements of U.S. Army V Corps deployed to OIF with 10 ruggedized DCTS systems. Six additional DCTS-equipped tactical Army units from the United States flowed into the theater of operations to support V Corps.

DCTS program office collaboration with CENTCOM and V Corps was considerable. Prior to OIF, DISA personnel supported DCTS during Exercise Internal Look at CENTCOM and V Corps' Victory Strike exercises, held as precursors to hostilities. The exercises provided both commands an opportunity to develop DCTS tactics, techniques and procedures for wartime use, while at the same time giving the DCTS program office team an opportunity to apply lessons learned to ensure DCTS met warfighter needs.

Deployed members of CENTCOM use the Defense Collaboration Tool Suite. CENTCOM photo.

Both CENTCOM and V Corps used DCTS extensively during OIF. According to CENTCOM personnel, DCTS enabled them to conduct mission planning at a new level. DCTS was used daily to coordinate numerous operational requirements between CENTCOM (forward) and many of the component commands' headquarters. The use of DCTS grew exponentially as more and more operational elements requested DCTS accounts to collaborate within and to the CENTCOM (forward) headquarters daily.

CENTCOM staff personnel cited DCTS as a combat multiplier to users that directly supported combat operations. CENTCOM (rear) not only used DCTS for combat operations, but also used DCTS to conduct real-time collaboration to a large number of Army officers attending senior Army leadership schooling at the Army War College, Carlisle, Pa. This use of DCTS enabled the students to conduct collaboration sessions with a wide variety of CENTCOM war planners who were involved in OIF planning operations.

V Corps used DCTS to conduct "battle rhythm" updates twice daily when not conducting combat operations. (Battle rhythm describes those events that a unit conducts on a recurring basis to facilitate conditions for success.) Each major subordinate command joined the conference from their remote location via the V Corps tactical network. The V Corps commander and staff used DCTS during ongoing operations and to plan future operations.

Using the Joint Enroute Mission Planning Rehearsal System (JEMPRS), which includes DCTS components, V Corps command and control vehicles (C2V) gave the commander the capability to do everything on the move including using DCTS. As explained by a V Corps officer, DCTS provided the warfighter with greater capabilities. He marveled at these capabilities and said, "Think of it, we are in the TAC (tactical) command post in Iraq and our G-3 is working the next operation with the main command post in Kuwait ... pretty powerful stuff."

DISA support to the success of DCTS during OIF was extensive and a great example of the teamwork between CENTCOM and V Corps staffs, DISA National Capital Region (NCR), DISA field offices, and Regional Network Operations Security Centers (RNOSCs). The DCTS program office provided 24x7 government and contractor support to CENTCOM headquarters, rear and forward, and to the RNOSC in Bahrain and Joint Task Force-Southwest Asia. In addition, the DCTS team quickly responded to support emerging requirements and technical issues.

Naval Reservists Shape the Future Fleet Aboard Dahlgren Laboratory's Virtual DD(X)... Next Generation Network-Centric, Multi-Mission Destroyer

By JO1(AW) John J. Joyce, USNR

Navy Reservist, IS1 Sally Jo Sasser, saw the fleet's future on a two-week annual training exercise that took her to Northern Virginia where Civil War battlefields dot the historic landscape. She helped shape the future every day she stepped aboard the virtual (v) DD(X), the next generation destroyer Combat Information Center (CIC) during the recent Naval Fleet Battle Experiment Kilo (FBE-K).

Navy reservists staff a CIC complex at Dahlgren during training. Photo by NSWC Dahlgren.

The imagery analyst, aboard a U.S. Navy ship yet to be built, prosecuted, nominated and sent the geo-coordinates of several simulated enemy targets to shipmates. Suddenly, the Land Attack Warfare Officer (LAWO), Lt. Cmdr. Jennifer Wright's, words: *"Greyhound away. Gulf, x-ray, one, zero, zero, one. Time on target, 29 seconds,"* boomed throughout the vDD(X) node manned by warfighters at Commanding Officer (CO), Tactical Action Officer (TAO), Officer of the Deck (OOD) and Intelligence Group CIC positions. Smoke appeared at the point of impact on a big screen that displayed the total operational picture.

It is vDD(X) shock and awe on the banks of the Potomac River — at a Naval Base named after Civil War Rear Adm. John Dahlgren, the "Father of Naval Ordnance" and the Dahlgren Gun. Two hours of free-play simulation ensued, as the CIC crew tested the mock surface combatant's sea-based precision-strike and volume-fires capability. *"The determination to shoot the time sensitive target (TST) with a Tactical Tomahawk Land Attack Missile (TTLAM) was based on intelligence analysis of a film feed simulating an unmanned aerial vehicle (UAV) on a reconnaissance patrol,"* explained Sasser. *"We nominated the target by identifying the platform — a SCUD launcher. After confirming the geo-coordinates, I snapped a picture off this imagery, and sent it over to the TAO and LAWO. Their decision was decisive and effective."*

Such free-play combat scenarios, as well as DD(X)'s engagement of high-value targets in support of the Marines ashore, enabled Sasser, Wright and a team of officers from Naval Reserve Program Executive Office for Ships, NR PEO(S) HQ 306, to help shape the future of the Navy's first truly network-centric surface combatant. *"We're here on the cutting edge of technology bringing to bear our civilian expertise in land attack warfare, communications and maintenance,"* said Capt. William Sposato, the reserve unit's commanding officer. *"... We are influencing the design of a multi-mission ship and the integration of combat suites."*

With advanced multimission ship and combat systems optimized for littoral environments, the DD(X) design will exploit enemy vulnerabilities on, above, and below the sea while offering long-range precision firepower in support of networked Naval and joint forces ashore — all with a smaller CIC crew. Sposato's team also tested their interface with DD(X) combat systems and the Joint Fires Network (JFN) to simultaneously plan, target and execute multiple fires missions during a myriad of FBE-K scenarios. JFN, a network-centric warfare family of sea, air, land and space-based intelligence gathering systems, will eventually allow all U.S. military commanders and those of certain allied nations to share a common battlespace view.

The main objectives of FBE-K emphasized the Global Concept of Operations and the testing of virtual systems that support the fundamental concepts of the Chief of Naval Operations' (CNO) Sea Power 21 vision: Sea Strike (projecting offense), Sea Shield (projecting defense) and Sea Basing (projecting sovereignty) — all networked through the integration of warriors, sensors, weapons, networks and platforms, referred to as FORCEnet. *"DD(X) and its associated transformational technologies will be at the core of U.S. Navy capabilities and missions for the 21st century,"* CNO Adm. Vern Clark recently said. *"These great ships and other members of the family of surface combatants will transform the Navy fleet, multiply our combat effectiveness, and play a crucial role in dominating the future battlespace."*

"We're on the cusp of shaping the future of DD(X) when it comes to the warfighter and how the ship is going to fight," said Wright, who, as the Navy Warfare Development Command (NWDC) Liaison Naval Officer (LNO) at the vDD(X) node, reported directly to FBE-K's fires initiative lead aboard the Seventh Fleet command and control ship, USS Blue Ridge (LCC-19), on station in the Pacific. *"We are working out concepts, practicing doctrine and protocol. Future crews will be smaller than we're used to. The CIC will have only a few people running highly technical systems. We are learning how that will work out operationally. In addition to the human systems integration (HSI) picture, we're helping to determine how it's all going to flow."*

The design agent team, led by Northrop Grumman and Raytheon, interacted with reservists and studied HSI in the FBE-K network node they helped to establish aboard vDD(X). *"Since the systems are so complex, it was extremely important for us to sit right next to the warfighters and observe, interact and listen,"* said Raytheon Technical Director, Roy Johnson. *"The warfighters tested several simulations during the fleet battle experiment that we intend to build. Their tests gave us the advantage of receiving feedback on what works and what doesn't work, what we had right, and what we had to improve. To work with experienced and knowledgeable reservists who could spend time with us was a great learning opportunity."*

"The reservists in Dahlgren had a direct impact on FBE-K and Sea

Power 21," exclaimed PEO Ships project manager, Lt. Cmdr. Ivan Pierce. *"Without their ability to man and operate the systems, we can't get the data we need to proceed with our design. On their drill weekends at PEO Ships, reservists receive training as each type of sea strike system is introduced. We also have to test the systems which gives the reservists a chance to interoperate with the DD(X) node's Sea Strike capabilities prior to the FBE."*

DD(X) was not the only virtual platform testing systems and participating in the three-week joint warfighting experiment. The ship was part of an expanded Amphibious Group that included a virtual next generation E2-C Hawkeye, a virtual submarine, an unmanned underwater vehicle (UUV) from Naval Undersea Warfare Center in Newport, R.I., and a simulated Royal Australian Navy destroyer (virtual or vANZAC) in Canberra, Australia. The simulations networked live video feeds from a Predator vUAV to ships operating in the Pacific Fleet where shipboard systems were stimulated with actual radar, acoustic and electronic data as if actual platforms were participating in the event.

Dennis Warne of Naval Surface Warfare Center Dahlgren Division (NSWCDD) Theater Warfare Systems Department, who led a team of technical experts who configured the DD(X) node said, *"It was a challenge to network with NWDC (Naval Warfare Development Center) in Rhode Island and the fleet 14 time zones away. We developed artificial tactical systems and made them operate with real networks such as the Naval Fires Control System (NFCS) in the experiment. Our team of technicians — a majority are former military — understood the experiment's environment and worked behind the scenes to make sure the node's warfighters were connected with ADOCS/LAWS (Automated Deep Operations Coordination System/ Land Attack Warfare System), JSAF (Joint Semi-Automated Forces) Simulation, AFATDS (Advanced Field Artillery Tactical Data System), ANGuSS (Advanced Naval Gun Simulation System), NFCS and JFN."*

"This is an evolution of fleet battle experiments that we started as a reserve unit last year," said Capt. Sposato. *"We're working this in conjunction with mobilization readiness. It supports our gaining command, the Program Executive Office for Ships, who oversees the acquisition of the DD(X)."*

As their technical expertise helps to transform the fleet, the PEO Ship reserve unit is expected to undergo a transformation themselves from the Navy's DD(X) testing team to the Navy's DD(X) training team focusing on Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems.

Sasser's work with the PEO(S) HQ 306 reserve unit and the design agent during fleet battle experiments will help introduce combat and C4ISR systems integration, precision strike and volume fires capabilities aboard the DD(X). Making the fleet's future a reality by helping to build ships is a Sasser family tradition started by her great grandfather a century ago. *"In the late 1800s and early 1900s, his family business built diesel engines for the Navy,"* said Sasser, a Raytheon mission planner from Aurora, Colo. *"Now, here I am, in the Naval Reserve on assignment in this historic part of the country where George Washington was born, helping the design agent build DD(X) and preparing to train our active duty counterparts to become proficient on the Joint Fires Network."*

For more information go to www.nwdc.navy.mil/Products/FBE/FBEKilo.

Coalition Interoperability Tested at Dahlgren During JWID 2003

By JO1(AW) John J. Joyce, USNR

A Spanish soldier sent U.S. Army Staff Sgt. Timothy Knoblach an Artillery Systems Cooperation Activity (ASCA) message from Madrid via a global wide-area network that called for fire on a specific target out of reach. Instantaneously, a dozen military and civilian visitors on tour at Joint Warrior Interoperability Demonstration (JWID) 2003 in Dahlgren, Va., witnessed a demonstration of coalition interoperability action — if they didn't blink an eye.

The U.S. Army fire support sergeant used the Advanced Field Artillery Tactical Data System (AFATDS) to respond decisively to the request by coordinating artillery support with a U.S. Navy warship through the Naval Fires Control System (NFCS).

"Spain is proving they have interoperability with our systems," said Knoblach. *"In the past, we had to run back and forth to use a radio. This new digital exchange of information gives us complete control, overcomes language barriers and does not allow us to fire on friendly troops ... it forces prior coordination before conducting fire missions in a friendly area."*

"ASCA enables the Spanish field artillery tactical system to become interoperable with the U.S. Army and U.S. Marine Corps tactical fire support system," said JWID 2003 Dahlgren Site Manager Dennis Warne. *"... We have to correctly and quickly provide data to a multitude of users — to various nations and cultures that act and think in a different context."*

Information sharing across multiple domains — a critical capability in the Global War on Terrorism is the main concern in coalition interoperability. At the Dahlgren site, many new information technologies and methodologies were tested to determine their usability in a myriad of combat situations that depend on fast, accurate and secure coalition interoperability. JWID, an annual exercise between the U.S. Joint Chiefs of Staff and the international community focuses on Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR). This exercise provides an opportunity for government, private industry and coalition partners to demonstrate new and effective joint warfighting technologies globally.

"This area of interoperability is vital to our warfighting success," said Barry Dillon, head of NAVSEA's Theater Warfare Systems Department. *"We have got to improve and stay ahead of our adversaries who have equal access to hardware technologies."*

With a focus on JWID 2003's theme, "Coalition Interoperability, the 21st Century Warfighter's Environment," JWID's 42 Coalition Interoperability Trials (CIT) assessed at various sites offered a full spectrum of solutions to improve combatant commanders near-term coalition interoperability. Each CIT, conducted in a simulated operational environment to provide context for warfighter

validation of C4ISR solutions, received a comprehensive assessment. Depending on the CIT, evaluations included the warfighter, technical and/or security assessments. Some of the 19 CITs demonstrated at Dahlgren included:

•The Collaboration Gateway illustrates how coalition forces in different security domains can securely share information in real-time.

•Coalition Blue Force Situational Awareness provides commanders improved awareness of friendly force environments, enabling rapid decision-making ability. The system allows tracking of U.S. and coalition forces using a Global Positioning System (GPS) tracking device, and will be integrated into the Global Command and Control System (GCCS).

•Language Translation Services allow U.S. warfighters to automatically transmit information to other coalition members in English, Japanese, Korean and Spanish, and vice-versa.

•The Coalition Information Assurance Common Operational Picture facilitates multilateral sharing of technology information yet protects national sovereignty, at the same time analyzing critical technical infrastructure supporting a coalition mission. It allows early warning of potential attacks on supporting coalition forces infrastructure.

Left to right: Lt. Col. Paul Willem Van Den Broek, New Zealand Army; Lt. Cmdr. Joseph Sposato, USNR; Maj. Martin, Australian Army and Capt. Ives, USNR, during JWID 2003 exercises at NSWC Dahlgren's Theater Warfare Department. Photo by NSWC Dahlgren.

JWID's six core objectives, conducted over the worldwide Combined Federated Battle Laboratories Network (CFBLNet), covered multiple levels of security, logistics, language translation tools, situational awareness, coalition network vulnerability assessment capability and core network services.

The Secondary Navy Site at Dahlgren was a virtual cruiser; USS Chancellorsville (CG-62), manned by a coalition of U.S. Navy and Royal New Zealand Navy sailors, was instrumental in demonstrating methods of sharing situational awareness information with nations via coalition networks in a Multinational Naval Task Group (MNTG). The Naval Fires Control System (NFCS), a Dahlgren demonstration, also expanded JWID's warfighting capabilities and helped to examine the ability of different nations' logistics systems to support the planning and execution of naval fires.

"From the Combat Information Center (CIC) aboard this virtual ship, our communication with seven different nations over 17 different time zones is instantaneous," said Royal New Zealand Navy Lt. Cmdr. Shane Arndell. Arndell demonstrated the MNTG trial, an amalgam of command and control, communications and computer capabilities operating in a low-bandwidth, high-latency maritime IP environment typical of allied and coalition operations. The MNTG, composed of Australia, Canada, New Zealand, United Kingdom and United States (AUSCANNZUKUS), uses the Maritime Tactical Wide Area Network to provide multinational warfighters with a force multiplier that promotes situational awareness in an allied/coalition environment.

Several tools, designed to increase the speed of imagery analysis and targeting by a quantum leap, were introduced at Dahlgren. For example, the Pilot Aircrew Cockpit Management (PACMAN) system and the Precise Tactical Targeting (PTT) system, are expected to enable aircrews and infantrymen to interoperate and respond within minutes to active targets.

To have a product that allows you to communicate directly with a pilot or a base station or artillery area is absolutely incredible," said Naval Reservist and former Marine, IS1 Robert Williams, who demonstrated the PACMAN system and the PTT system. *"It speeds up the process of targeting from days to minutes — literally. The interest in this system has been one of the greatest in JWID, especially among staff officers. PACMAN is a product that lets you forward what you see on a map, chart or imaging data to someone else so they know exactly what you're looking at and can target that area. It's fantastic."*

While planning and executing coalition operations, warfighters found JWID's real-time or near real-time language translation tools invaluable to share situational awareness information among different nations' logistics systems.

"When I return to the UK, I will be submitting a full post exercise report on JWID," said British Army Major Stuart Heaton. *"My recommendation will be that — time and money allowing — the UK Army might adapt some of the software applications that I've utilized over the last two weeks. The technology does cut down on mistakes and certainly there is quicker collaboration between the coalition partners. The TRiM [Translingual Instant Messaging] language application tool is an example of a marvelous application that crosses the language barrier. As the Fire Support Coordinator (FSC) for JWID 03, responsible for all ground artillery, naval gun and close air support, I was required to work with the Spanish Army. TRiM effectively enabled me to write my message on a whiteboard ... and send it straight to Spain. They receive it in Spanish and can then respond to ... me and I receive it in English."*

In conjunction with the JWID CITs, Dahlgren demonstrations included:

♦The Naval Fires Control System (NFCS), an automated mission planning system designed to allow surface combatants to provide timely and effective fire support to U.S. Army and Marine Corps forces ashore;

♦COLLABORATOR a common collaboration environment that can provide the warfighter with a chat room equipped with a synchronized multilayered, multimedia whiteboard; that allows intelligence analysts to post information on the whiteboard for limited distribution.

Interoperability solutions were tested with coalition members, including participants from 10 NATO nations: Canada, France, Germany, Italy, Norway, Poland, Spain, Turkey, United Kingdom, United States, and Australia and New Zealand. The Pacific Rim nations of Japan, Singapore, South Korea and Thailand supported JWID's host, the Pacific Command (PACOM), as coalition task force members and multinational task force staff. □

The Lazy Person's Guide to Command and Control

By Retired Major Dale J. Long, USAF

Command: To give orders to.
Control: To exercise authority or influence over.

Command and Control (C2): Together, these two words represent the foundation of the military environment. Without C2 a large mass of armed people is simply a mindless mob. In this article we will look at the process of C2, some of the ways technology has affected command and control over the years, and a view of what it might become in the future.

As is my habit, this article will cover the social aspects of C2 as much or more than the technical side. There are many people who can describe the intricacies of the Global Information Grid, or the Navy's Common Operating Environment far better than I can. What I would like to do here is give you some history and insight into how we got where we are and where we might want to go with C2 as a system that includes humans as the key component.

C2: The Basics

The basic unit of force, military or otherwise, has always been a single person. Pretty much every human activity can be measured against what one person can do with their bare hands. So, at its core, C2 begins with a single person's ability to observe, orient, decide, and act (known as the OODA loop). You see a threat or opportunity and respond to it. At the next level is cooperative action between two or more people. A group must reach a consensus of some type as a prerequisite for successful action. This can either be by conscious agreement or conditioned reflex. In the case of the best performing teams, be they military units or basketball players, they do both. Effective C2 systems facilitate cooperation.

Another key principle of C2 is simplicity. First, this means that the people should only have to deal with the minimum amount of information they need to get the job done. The challenge here is that the amount and type of information a task force commander needs is radically different than that needed by a Marine platoon leader or a fighter pilot. Some part of the C2 system, either human or automatic, has to sort and aggregate information appropriately for every participant.

Second, people in the middle of battle have a limited attention span for anything that is not directly related to shooting and not being shot. The signals sent need to be simple, clear and direct. Anything that distracts frontline troops for more than a few seconds is likely to get them killed.

Here is one last piece of philosophy before we get into a more specific discussion of C2. According to an old Warren Zevon song, the three sources of power in the world are "Lawyers, Guns and Money." While that may seem the case in today's news, I am inclined to a more generic description of these three factors. In his book, *Powershift: Knowledge, Wealth and Violence at the Edge of the 21st Century*, Alvin Toffler proposes three basic types of power: knowledge, force and wealth. All three of these play a role in the effectiveness of projecting power.

Force is what people provide, enhanced by whatever technology they have. A rifle shot does more damage than a fist, and a bomb more than a rifle. However, a human still has to initiate the action. A horse can carry more than a person, a truck more than a horse, and a C-17 can carry about 85 tons of all of them. But a person has to tell them where to go and decide what they carry. The rifle, bomb, truck, ship and airplane are all simply extensions of someone's ability to project force in their environment. Wealth is what we have that we can apply to a task. How many trucks, ships, or planes are available? Can we get more? Add in food, munitions, and yes, even people, and you have the assets that allow you to project force. Knowledge is what directs the employment of force and wealth. Without it, you are like Bruce Lee fighting blindfolded. Unless you can see your opponents and where to apply your assets, your luck will eventually run out no matter how good you are.

Simply having force, wealth, or knowledge, however, doesn't guarantee a successful operation. That's where C2 comes in, to monitor and control your environment and operations. But C2 is more than just a communications system tied to big databases. Effective C2 requires three things: reliable sources of data, a means to communicate, and a sense of community and trust.

Reliable data, either from sensors, databases or personal observation is the lifeblood of operations. However, this data is generally a passive part of the system until someone starts culling and applying it to answer questions and solve problems. Automated systems can provide greater amounts of data in less time than human observers, but automated systems usually aren't that good at distinguishing useless data from useful data. They just collect everything. Data entered by people, while it can be of a higher quality, may also be subject to the limits or biases of the person involved. The goal is to make data collection as objective and comprehensive as possible and then develop effective and efficient methods of extracting what you need.

Communication is absolutely vital when giving orders. There are both technical and social aspects to this, but for most of human history the sound of a leader's voice

has been the principal method of C2. I believe this is still largely true today. However, one voice can only carry so far, so there have been many enhancements that have allowed a leader's commands to reach larger and larger forces. In *The Art of War*, Sun Tzu described the basics of managing larger forces on a battlefield 3,500 years ago in the following passages:

♦ *The control of a large force is the same principle as the control of a few men: it is merely a question of dividing up their numbers. (V-1)*

♦ *Fighting with a large army under your command is in nowise different from fighting with a small one: it is merely a question of instituting signs and signals. (V-2)*

♦ *The Book of Army Management says: On the field of battle, the spoken word does not carry far enough: hence the institution of gongs and drums. Nor can ordinary objects be seen clearly enough: hence the institution of banners and flags. (VII-23)*

♦ *Gongs and drums, banners and flags, are means whereby the ears and eyes of the host may be focused on one particular point. (VII-24)*

♦ *In nightfighting, then, make much use of signal-fires and drums, and in fighting by day, of flags and banners, as a means of influencing the ears and eyes of your army. (VII-26)*

Communication also requires a common frame of reference and that's where the community aspect of C2 comes in. The participants have to know the language, signs and signals being used to understand and act upon the message. It's also helpful if the enemy does not, thus the use of codes, encryption, and other forms of obfuscation used to make sure that only your team gets the message.

The community also prescribes the boundaries that the C2 system can affect. There are many ways of describing communities, but for C2 I will narrow it down to a group of people with common goals and interests. This can be anything from eight people in a squad trying to secure a building to 100,000 people invading another country. Community is a social rather than a technical issue, but it is a linchpin of C2. If the people receiving orders do not feel themselves bound to the larger community, they may not follow these orders.

Ultimately, though, it all comes down to trust. You can have all the force, wealth, knowledge, community and communication you want, but if the person receiving the order does not trust its source, C2 will fail. Trust becomes more of an issue the farther away we get from direct, face-to-face conversation with someone we know well and respect. There is a huge difference between receiving a telegram telling you to move an army 150 miles in 19 hours and General George S. Patton personally telling you to move an army 150 miles under heavy-fire to relieve Bastogne in 19 hours. Wars have been won or lost on such differences.

C2: The Electronic Age

Flags, trumpets and lights served C2 well for most of human history, but the introduction of electronic communications brought a whole new dimension to commanding and controlling. For the first-time ever, humans had a reliable way of communicating beyond line-of-sight. Early use of electronic communications was limited by the requirement for a wired connection. The telegraph saw some use during the Civil War, but tactical C2 still depended primarily on more traditional signaling devices like flags and bugle calls. The first real impact from electronic communications came with the introduction of the radio. Portability and the range of early field radios were issues, but by WWII radio played a significant role in C2.

During my research I found a wonderfully comprehensive article about the development of C2 capabilities and doctrine in the first part of the 20th century: "History of Communications-Electronics in the United States Navy" (http://earlyradiohistory.us/1963hw.htm), by retired Captain Linwood S. Howeth, USN. Howeth describes the early development of radio technology and the development of radio use in the Navy. I invite you to read through the entire work. If you only read one part of it, however, read the introduction by Fleet Admiral Chester Nimitz. If that doesn't inspire you to read at least some of the rest of the article, nothing will. Some of the things I found most interesting in Howeth's article were the stories about the reactions and opinions of the Naval officers involved with early trials of wireless equipment 100 years ago. There was apparently great resistance to the first attempts to introduce radios into Naval operations. Among the arguments used against employing radios were:

♦ Using it would give away your ship's position.

♦ The enemy might break your codes and steal your plans.

♦ Even if the enemy couldn't understand your signals, they could jam your frequencies and render your radios useless.

While all of these were (and still are) potential problems, Howeth suggests that captains and admirals may have also resisted because they were used to having considerable autonomy. They may not have relished the idea of having someone on shore calling up and interfering with their command while they were out at sea. Howeth notes 1911 as a low point in the history of Naval radio use. The first major tactical tests under battle conditions were apparently a complete failure. What was noteworthy was that very few of the problems were related to the technology, rather the problem was with the *people* struggling to use something new and unfamiliar. Equipment was not installed properly and training was weak — if it was done at all.

It may be easy to look back knowing what we do today about frequency management, radio discipline, and radio-based C2 and congratulate ourselves on how smart we are. But please understand that we are currently attempting to integrate technologies into today's C2 that are as radical to us as radio was 100 years ago. There are some important lessons to be learned from their experiences about how to adapt and evolve C2 based on a new communications environment. First, don't assume everyone will automatically embrace new technology. This is usually more a function of habit than conscious resistance. People trust what they know, particularly where it involves life or death situations

like combat. Second, beware of people who embrace new technology too enthusiastically. Uninformed optimists can wreak far greater havoc and chaos than stick-in-the-mud pessimists. At least the pessimists won't make things any worse than they already are. Third, not all technologies can be applied equally across the board. What works at home may not work deployed. What works deployed may cost too much to install at home. The trick is finding a balance so you get one, seamless system. Finally, take into account how your target audience wants to work, because if the system does not match their style, they will likely try to bypass it.

Once the Navy got past some initial hurdles, the effects of radio on C2 were profound. At first, the radio was only used to duplicate orders issued by flags and other visual signals. Over time, however, as Sailors became more familiar with it, radio eventually became a primary means of transmitting orders between units ashore and at sea. By World War II, radio was an integral part of C2 for all U.S. military forces. Today, radio transmissions blanket the globe and the medium serves as a backbone of modern analog and digital communications. It is hard to imagine operating today without radio in some form, but as with many of the technologies used in modern warfare, radio has been part of C2 for less than 100 years.

C2: Sensors

Radio gave us a way to control modern forces and direct them to where they need to be. But how do you know where you need them? Locating targets, or even your own position relative to a target, is a function of sensors, the eyes and ears of the command function. While we are in historical mode, it is important to note the development of two other technologies during WWII that also have a key role in C2: radar and sonar.

Radar is short for "radio detecting and ranging." It locates objects by beaming pulses of radio waves and reading the echoes that bounce back off the objects in the path of the waves. Direction is determined by sweeping pulses around the antenna transmission arc and then seeing which ones will come back. Distance is determined by timing how long it took a pulse to return. The radar systems used in WWII could locate targets at a distance of 33 miles and distinguish between multiple targets at around 26 miles. This gave U.S. forces, particularly in the Pacific, a tremendous advantage in conventional Naval combat and anti-aircraft operations, particularly at night and in bad weather.

Sonar is short for "sound navigation ranging." Its importance as a sensor can be seen by the progress made by Allied anti-submarine operations in the Atlantic from 1940-1944. In 1940, Axis submarines were sinking an average of 80 Allied ships per month. When the Germans began their "wolf pack" operations 1941, that average went up to 93 Allied ships per month. However, thanks to improvements to both sonar apparatus and anti-submarine tactics, the tide began to turn. In November 1942, the Allies lost only 23 ships to Axis submarines out of 1,065 assorted Allied vessels that traveled from the United States and United Kingdom as part of the North African invasion. In 1943, the Allies were dropping sonobuoys from aircraft, increasing their detection ability. That year, the number of Allied losses dropped. During the winter of 1944, the Allies sank more submarines than the Axis sank ships. The final proof of the value of electronic sensors came during the D-Day invasion. Due to tight radar and sonar screens, the Allies did not lose a single vessel to submarines for over three weeks. The Germans never regained the upper hand.

Today, we have high altitude reconnaissance and satellites that can give us a detailed view of the entire planet. Our sensor technology has become so sensitive that we can tell how many living creatures are crossing a particular patch of ground and whether they are walking on four legs or two. They are all sources of data, but each new advance adds more complexity to the system. Life is still full of little trade-offs.

C2 Today

Much of modern C2 doctrine was developed during WWII and the basic principles remain the same: observe, orient, decide and act, the OODA loop I mentioned earlier. The force that accomplishes this faster will have the advantage in battle. Improvements in our sensor systems, communications gear and tactics have improved the speed with which we complete this loop. Increased trust, both in new systems and in cooperating forces, also help the OODA cycle. More than one submarine commander in WWII, for example, plotted his torpedo bearings manually for every shot instead of using the analog target data computer containing prefigured firing solutions provided to every submarine in the fleet. Eventually, we came to trust computers enough to calculate firing solutions for us.

But there are two things that distinguish modern C2 systems from their predecessors. The first is the sheer volume of data they can convey. Field and task force commanders have access to huge, detailed stores of information related to every aspect of their operations and logistical support. The challenge today isn't so much getting information to commanders, but reducing or aggregating it to usable size. Also, we are developing systems capable of linking everyone right down to the basic infantryman in the field. They also need to know a piece, but only their piece, of the battlefield. As the principal function of a C2 system is to deliver trustworthy, useful information, a large part of that process will be how the system handles and presents information to all the individual participants.

The second difference is an increased use of autonomous C2 systems that can "OODA" far faster than a human can aspire to. I'm sure anyone reading this article is aware of cases where anti-

aircraft systems set on automatic have, unfortunately, fired on friendly aircraft. It's a difficult dilemma. Modern combat happens so fast that humans simply can't react to some threats fast enough. On the other hand, setting a weapon system on automatic without an ironclad way to have it identify friend from foe carries a certain amount of risk.

Today's "sensor to shooter" C2 systems are global webs of interconnected observers (radar, sonar, satellites, people), communications systems (wired and wireless), content (voice, data, video and images) and people. They include projects like the Global Information Grid, Force XXI, and the Army's Future Combat Systems. There are probably a lot of very bright people with an opinion about how to go about successfully integrating all the different C2 systems and components under development. Here are my two cents on the subject.

Replicating Human Cognition

Evolving our C2 systems beyond what we had in the 20th century will require a certain amount of autonomy. What I believe we need are large-scale cognitive systems that have the ability to solve all the small everyday problems that we mere humans handle without a second thought. We will need systems that do not just act on sensor data, but are capable of assessing the results of their actions and learning from them.

Impossible? Well, a few years ago cognitive experts claimed that a computer would never be capable of beating the best human chess grandmasters. In the last three matches with the world's top chess champions, though, computers have earned two draws and a win. We are not quite to the point of a HAL 9000 or Mr. Data from *Star Trek*, but computers are demonstrating increasingly sophisticated capabilities and behavior.

What kind of behaviors will automated C2 systems require? There are inherent differences between organic and machine behaviors. An aircraft, for example, does not flap its wings to fly like a bird does. They are two very different solutions to the same challenge: taking flight. However, when you are conserving energy while gliding through the air, the design solutions between bird and plane are, as Leonardo da Vinci illustrated, remarkably similar.

Developing the autonomous control systems of the future will depend on adapting our systems to operate in an environment that is currently suited primarily for human cognition and behavior. The best solutions will include design strategies that we already know work in our environment. An automated anti-aircraft system, for example, should be able to distinguish between hostile and friendly aircraft. It should also be able to make a decision on what battery should fire and whether it should use a heat-seeking or radar-guided missile to take out a hostile aircraft based on the target's type and knowledge of what munitions it has available. Humans have developed doctrine and tactics to deal with this over many years of experimentation. What we know can be programmed into a system.

However, it may be a bit like a bird trying to teach an aerospace engineer how to fly. Humans make value judgments and decisions every day, but try to diagram how we arrived at a decision that took two seconds and it can take days to describe all the parameters. It is probably why it took us so long to get into the air with the birds. Until we figured out a way to get airborne without flapping our arms, we were stumped, and even then it took us a few centuries before the Wright brothers made da Vinci's plans work.

A key challenge for 21st century C2 is to develop all of these individual sensor and control systems to cooperate together automatically when they come in proximity to each other, like the automatic wireless peer networking you can get from some 802.11b wireless Ethernet systems. Let's make these systems smart enough so that when a squadron of Air Force A-10s is attacking the same target as a squadron of carrier-based A-6s near a Marine armored assault force, the C2 system automatically groups them, gives them common radio frequencies, and provides a fused picture of the battlespace, even if the participants didn't know ahead of time that they would be operating in the same space.

In short, I want what I used to see on the *Star Trek* television series: a system that knows where everyone is and can put me in touch with them simply by saying my name and theirs. We can buy a $100 cellular telephone that will call Pete Hess when I push a button and say, "call Pete Hess." Why not do the same thing with C2 and have a system that automatically sets up a secure voice circuit when a task force commander says, "Task Force One to Abraham Lincoln?" While it may be labor-intensive programming everyone into the system, it should be no more complex than the one your Web browser uses to locate one IP address out of the millions on the Internet.

Final Words

If we compare this point in our history with the development of the signs and signals codified by Sun Tzu, we are at roughly 2400 B.C. as far as electronic C2 is concerned. We have a long way to go and a lot of potential to work with. We will probably pull a few "Zippys" along the way. But as long as we keep our focus on operational goals and don't become obsessed with technology for its own sake, someday we will get that *Star Trek* C2 system.

Until then, Happy Networking!

Long is a retired Air Force communications officer who has written regularly for CHIPS since 1993. He holds a Master of Science degree in Information Resource Management from the Air Force Institute of Technology. He is currently serving as a Telecommunications Manager in the U.S. Department of Homeland Security.

ViViD Contracts

N68939-97-D-0040

Contractor: Avaya Incorporated

N68939-97-D-0041

Contractor: General Dynamics

ViViD provides digital switching systems, cable plant components, communications and telecommunications equipment and services required to engineer, maintain, operate and modernize base level and ships afloat information infrastructure. This includes pier side connectivity and afloat infrastructure with purchase, lease and lease-to-own options. Outsourcing is also available. Awarded to:

Avaya Incorporated (N68939-97-D-0040); (888) VIVID4U or (888) 848-4348. Avaya also provides local access and local usage services.

General Dynamics (N68939-97-D-0041); (888) 483-8831

Modifications

Latest contract modifications are available at http://www.it-umbrella.navy.mil

Ordering Information

Ordering Expires:
26 Jul 05 for all CLINs/SCLINs
26 Jul 07 for Support Services and Spare Parts

Authorized users: DoD and U.S. Coast Guard

Warranty: Four years after government acceptance. Exceptions are original equipment manufacturer (OEM) warranties on catalog items.

Acquisition, Contracting & Technical Fee: Included in all CLINs/SCLINs

Direct Ordering to Contractor

Web Link

http://www.it-umbrella.navy.mil/contract/vivid/vivid.html

TAC Solutions BPAs Listed Below

TAC Solutions provides PCs, notebooks, workstations, servers, networking equipment, and all related equipment and services necessary to provide a completely integrated solution. BPAs have been awarded to the following:

Compaq Federal, LLC (N68939-96-A-0005); (800) 727-5472, ext. 15515

Control Concepts (N68939-97-A-0001); (800) 922-9259

Dell (N68939-97-A-0011); (800) 727-1100, ext. 61973

GTSI (N68939-96-A-0006); (800) 999-4874, ext. 2104

Hewlett-Packard (N68939-97-A-0006); (800) 352-3276, ext. 8288

Sun (N68939-97-A-0005); (800) 786-0404

Ordering Expires:
Compaq Federal: 08 Oct 05 (includes two one-year options)
Control Concepts: 03 May 04
Dell: 31 Mar 05 (includes two one-year options)
GTSI: 01 Apr 05 (includes two one-year options)
Hewlett-Packard: 28 Oct 05 (includes two one-year options)
Sun: 22 Aug 04

Authorized Users: DON, U.S. Coast Guard, DoD, and other federal agencies with prior approval.

Warranty: IAW GSA Schedule. Additional warranty options available.

Web Link

http://www.it-umbrella.navy.mil/contract/tac-solutions/tac-sol.html

Enterprise Software Agreements Listed Below

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

In September 2001, the ESI was approved as a "quick hit" initiative under the DoD Business Initiative Council (BIC). Under the BIC, the ESI will become the benchmark acquisition strategy for the licensing of commercial software and will extend a Software Asset Management Framework across the DoD. Additionally, the ESI was incorporated into the Defense Federal Acquisition Regulation Supplement (DFARS) Section 208.74 on October 25, 2002.

Authorized ESI users include all Defense components, U.S. Coast Guard, Intelligence Community, and Defense contractors when authorized by their contracting officer. For more information on the ESI or to obtain product information, visit the ESI Web site at http://www.don-imit.navy.mil/esi.

ASAP (N00039-98-A-9002) for Novell products; (N00104-02-A-ZE78) for Microsoft products; and (N00104-03-A-ZE88) for Adobe products; Small Business; (800) 883-7413 for Novell products and (800) 248-2727, ext. 5303 for Microsoft and Adobe products

CDW-G (N00104-02-A-ZE85) for Microsoft products; (847) 968-9429

COMPAQ (N00104-02-A-ZE80) for Microsoft products; (800) 535-2563 pin 6246

Crunchy Technologies, Inc. (N00104-01-A-Q446) for PageScreamer Software (Section 508 Tool), Crunchy Professional Services and Training; Small Business Disadvantaged; (877) 379-9185

Datakey, Inc. (N00104-02-D-Q666) IDIQ Contract for CAC Middleware products; (301) 261-9150

DELL (N00104-02-A-ZE83) for Microsoft products; (800) 727-1100 ext. 37010 or (512) 723-7010

GTSI (N00104-02-A-ZE79) for Microsoft products; Small Business; (800) 999-GTSI or (703) 502-2073

HiSoftware, DLT Solutions, Inc. (N00104-01-A-Q570) for HiSoftware (Section 508 Tools); Small Business; (888) 223-7083 or (703) 709-8450

Micro Warehouse (N00104-03-A-ZE87) for Microsoft products; Large Business; (703) 262-6704

Northrop Grumman (N00104-03-A-ZE78) for Merant PVCS products; Large Business; (703) 312-2543

PeopleSoft USA, Inc. (N00104-03-A-ZE89) for PeopleSoft products; (800) 380-SOFT(7638)

Schlumberger (N00104-02-D-Q668) IDIQ Contract for CAC Middleware products; (410) 723-2428

Softchoice (N00104-02-A-ZE81) for Microsoft products; Small Business; (877) 333-7638 or (703) 469-3899

Softmart (N00104-02-A-ZE84) for Microsoft products; (610) 518-4000, ext. 6492

Software House International (N00104-02-A-ZE86) for Microsoft products; Small Business Disadvantaged; (800) 477-6479 or (732) 537-7131

Software Spectrum, Inc. (N00104-02-A-ZE82) for Microsoft products; (800) 862-8758 or (509) 742-2308 (OCONUS)

Spyrus, Inc. (N00104-02-D-Q669) IDIQ Contract for CAC Middleware products; (408) 953-0700, ext. 155

SSP-Litronic, Inc. (N00104-02-D-Q667) IDIQ Contract for CAC Middleware products; (703) 905-9700

Ordering Information

Ordering Expires:
Adobe products: 30 Sep 05
CAC Middleware products: 06 Aug 05
Crunchy products: 04 Jun 04
HiSoftware products: 16 Aug 04
Merant products: 15 Jan 06
Microsoft products: 26 Jun 04
Novell products: 31 Mar 07

Authorized Users: CAC Middleware, Merant products, Microsoft products, Adobe products and Section 508 Tools: All DoD. For purposes of this agreement, DoD is defined as: 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; non-appropriated 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.

Warranty: IAW GSA Schedule. Additional warranty and maintenance options available. Acquisition, Contracting and Technical fee included in all BLINS.

Web Links

Crunchy Technologies, Inc.
http://www.it-umbrella.navy.mil/contract/508/crunchy/crunchy.html

Datakey, Inc.
http://www.it-umbrella.navy.mil/contract/middleware-esa/datakey/index.html

Government Technology Services, Inc. (GTSI)
http://www.it-umbrella.navy.mil/contract/enterprise/microsoft/gtsi/gtsi.html

HiSoftware, DLT Solutions, Inc.
http://www.it-umbrella.navy.mil/contract/508/dlt/dlt.html

Microsoft Products
http://www.it-umbrella.navy.mil/contract/enterprise/microsoft/ms-ela.html

Northrop Grumman
http://www.feddata.com/schedules/navy.merant.asp

PeopleSoft USA, Inc
http://www.it-umbrella.navy.mil/contract/peoplesoft-esa/peoplesoft.html

Schlumberger
http://www.it-umbrella.navy.mil/contract/middleware-esa/Schlumberger/index.html

Spyrus, Inc.
http://www.it-umbrella.navy.mil/contract/middleware-esa/spyrus/index.html

SSP-Litronic, Inc.
http://www.it-umbrella.navy.mil/contract/middleware-esa/litronic/index.html

Department of the Navy Enterprise Solutions BPA
Navy Contract: N68939-97-A-0008

The Department of the Navy Enterprise Solutions (DON ES) BPA provides a wide range of technical services, specially structured to meet tactical requirements, including worldwide logistical support, integration and engineering services (including rugged solutions), hardware, software and network communications solutions. DON ES has one BPA.

Computer Sciences Corporation (CSC) (N68939-97-A-0008); (619) 225-2412; Awarded 07 May 97; Ordering expires 31 Mar 06, with two one-year options

Authorized Users: All DoD, federal agencies and U.S. Coast Guard.

Web Link

http://www.it-umbrella.navy.mil/contract/tac-don-es/csc/csc.html

Information Technology Support Services BPAs
Listed Below

The Information Technology Support Services (ITSS) BPAs provide a wide range of IT support services such as networks, Web development, communications, training, systems engineering, integration, consultant services, programming, analysis and planning. ITSS has five BPAs. They have been awarded to:

Booz Allen Hamilton Inc. (N68939-97-A-0014); (415) 281-4942; Awarded 02 Jul 97; Ordering expires 31 Mar 04

Lockheed Martin (N68939-97-A-0017); (240) 725-5950; Awarded 01 Jul 97; Ordering expires 30 Jun 05, with two one-year options

Northrop Grumman Information Technology (N68939-97-A-0018); (703) 413-1084; Awarded 01 Jul 97; Ordering expires 11 Feb 05, with two one-year options

SAIC (N68939-97-A-0020); (703) 676-5096; Awarded 01 Jul 97; Ordering expires 30 Jun 05, with two one-year options

TDS (Sm Business) (N00039-98-A-3008); (619) 224-1100; Awarded 15 Jul 98; Ordering expires 14 Jul 05, with two one-year options

Authorized Users: All DoD, federal agencies and U.S. Coast Guard.

Web Link

http://www.it-umbrella.navy.mil/contract/itss/itss.html

Research and Advisory BPAs
Listed Below

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

Gartner Group (N00104-03-A-ZE77); (703) 226-4815; Awarded Nov 02; one-year base period with three one-year options.

Acquisition Solutions (N00104-00-A-Q150); (703) 378-3226; Awarded 14 Jan 00; one-year base period with three one-year options.

Ordering Expires:
Gartner Group: Nov 06
Acquisition Solutions: Jan 04

Authorized Users:
Gartner Group: This Navy BPA is open for ordering by all of the DoD components and their employees, including Reserve Components (Guard and Reserve); the U.S. Coast Guard; other government employees assigned to and working with DoD; non-appropriated funds instrumentalities of the DoD; DoD contractors authorized in accordance with the FAR and authorized Foreign Military Sales (FMS).

Acquisition Solutions: All DoD. For purposes of this agreement, DoD is defined as: 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; non-appropriated 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.

Web Links

From the DON IT Umbrella Program Web Site: Gartner Group
http://www.it-umbrella.navy.mil/contract/r&a/gartner/gartner.html

Acquisition Solutions
http://www.it-umbrella.navy.mil/contract/r&a/acq-sol/acq-sol.html

The U.S. Army Maxi-Mini and Database (MMAD) Program Listed Below

The MMAD Program is supported by two fully competed Indefinite Delivery Indefinite Quantity (IDIQ) contracts with IBM Global Services and GTSI Corporation. The Program is designed to fulfill high and medium level IT product and service requirements of DoD and other federal users by providing items to establish, modernize, upgrade, refresh and consolidate system environments. Products and manufacturers include:

	IBM Global Services	GTSI
Servers (64-bit & Itanium)	IBM, HP, Sun	Compaq, HP
Workstations	HP, Sun	Compaq, HP
Storage Systems	IBM, Sun, EMC, McData, System Upgrade	HP, Compaq, EMC, RMSI, Dot Hill
Networking	Cisco	Cisco, 3COM, HP, Enterasys, Foundry

Ancillaries include network hardware items, upgrades, peripherals and software.

Services include consultants, managers, analysts, engineers, programmers, administrators and trainers.

MMAD is designed to ensure the latest products and services are available in a flexible manner to meet the various requirements identified by DoD and other agencies. This flexibility includes special solution CLINs, technology insertion provisions, ODC (Other Direct Cost) provisions for ordering related non-contract items, and no dollar/ratio limitation for ordering services and hardware.

Latest product additions include HP Itanium, HP storage, HP networking, HP Openview software, Sun products and services, Remedy software, Foundry and Enterasys networking.

Awarded to:

GTSI Corporation (DAAB07-00-D-H251); (800) 999-GTSI

IBM Global Services-Federal (DAAB07-00-D-H252); CONUS: (866) IBM-MMAD (1-866-426-6623) OCONUS: (703) 724-3660 (Collect)

Ordering Information

Ordering: Decentralized. Any federal contracting officer may issue delivery orders directly to the contractor.

Ordering Expires:
GTSI: 25 May 06 (includes three option periods)
IBM: 19 Feb 06 (includes three option periods)

Authorized Users: DoD and other federal agencies including FMS

Warranty: 5 years or OEM options

Delivery: 35 days from date of order (50 days during surge period, August and September)

No separate acquisition, contracting and technical fees.

Web Links

GTSI
http://pmscp.monmouth.army.mil/contracts/mmad_gtsi/mmad_gtsi.asp

IBM
http://pmscp.monmouth.army.mil/contracts/mmad_ibm/mmad_ibm.asp

The U.S. Army Enterprise Software Initiative BPA DAAB15-99-A-1002 EP07 (Oracle)

As of February, 28, 2002, the Navy holds inventory of Oracle Database Enterprise Edition (9i and 9ias) perpetual licenses (either named-user, multi-server or processor), and additional options and tools (i.e., security options, partitioning, spatial, clustering, diagnostics management packs, Tuning Management Pack, Change Management Pack, Internet Application Server Enterprise, Internet Developer Suite, and Balanced Scorecard). Initial orders will include software support for the period June 1 through May 31, 2003. Placing orders early will result in the best deal for end users. Four (4) additional out years of Silver Technical Support and product update support have also been negotiated.

The initial purchase price for end users is an average of a 64 percent discount off GSA prices and total package discounts (including out year technical support) average a 70 percent discount off GSA prices. Customers with small requirements can benefit from discounts normally reserved for customers with orders over $10 million. These licenses can be distributed throughout the Navy. In accordance with the Federal Acquisition Regulations (FAR) and DoD policy, Navy customers who have selected Oracle to satisfy new requirements must purchase the "new" Oracle licenses from the inventory.

This virtual inventory was established through the Department of the Navy Chief Information Officer (DON CIO) Enterprise Licensing Team and the Department of Defense Enterprise Software Initiative (DoD ESI). The DoD ESI is a joint initiative, which has been approved by the DoD Business Initiative Council (BIC). This inventory will be managed by the Department of the Navy Information Technology (DON IT) Umbrella Program Office at Space and Naval Warfare Systems Center, San Diego.

Web Link

http://pmscp.monmouth.army.mil/contracts/deal-o/deal-o.asp

The U.S. Army Enterprise Software Initiative BPA DAAB15-99-A-1003 (Sybase)

Through the contract, Sybase 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.

Ordering Expires: 15 Jan 08

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 non-appropriated 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

http://pmscp.monmouth.army.mil/contracts/deal-s/deal-s.asp

The U.S. Army Enterprise Software Initiative BPA BPWin/ERWin (Computer Associates) DAAB15-01-A-0001

This Enterprise agreement provides Computer Associates Enterprise Modeling tools including the products, upgrades and warranty. ERwin is a data modeling solution, that creates and maintains databases, data warehouses and enterprise data resource models. BPwin is a modeling tool used to analyze, document and improve complex business processes. The contract also includes warranties for these two products and upgrades for older versions of the products. In addition, there are other optional products, services and training available.

Ordering Expires: 30 Mar 06

Authorized Users: DoD and DoD contractors.

Web Link

http://pmscp.monmouth.army.mil/contracts/bpwin-erwin/bpwin-erwin.asp

The U.S. Army Enterprise Software Initiative BPA DABL01-03-A-0001 (Popkin Software & Systems Inc.)

The Department of the Army Architecture Modeling Solution initiative provides Architecture Tools including: the System Architect software license for Enterprise Modeling and all Popkin add-on products including the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Extension, Envision XML, Doors Interface, and SA Simulator as well as license support, training and consulting services. The main product on the BPA, System Architect, includes a C4ISR option that provides specific support for the U.S. Department of Defense's Architecture Framework (DODAF). Products vary from 3 to 15 percent off GSA depending on dollar threshold ordered.

Ordering Expires: 13 April 04

Authorized Users: DoD and their direct support contractors as well as the U.S. Coast Guard and the Intelligence Community.

Web Link

http://pmscp.monmouth.army.mil/contracts/ams-p/ams-p.asp

The U.S. Army Enterprise Software Initiative BPA DABL01-03-A-0002 (IBM Global Services)

The Department of the Army DEAL-I/D (Database Enterprise Agreement Licenses - I/D) initiative provides IBM/Informix database software licenses and maintenance support at prices discounted 2 to 27 percent off GSA schedule prices. The products included in the enterprise portion are: IBM Informix Dynamic Server Enterprise Edition (version 9), IBM Informix SQL Development, IBM Informix SQL Runtime, IBM Informix ESQL/C Development, IBM Informix ESQL/C Runtime, IBM Informix 4GL Interactive Debugger Development, IBM Informix 4GL Compiler Development, IBM Informix 4GL Compiler Runtime, IBM Informix 4GL RDS Development, IBM Informix 4GL RDS Runtime, IBM Informix Client SDK, IBM Informix Dynamic Server Enterprise Edition (version 7 & 9), and IBM Informix D.M. Gold Transaction Processing Bundle.

Primary Goods & Services: IBM/Informix database software licenses & maintenance support.

Ordering Expires: 30 Sep 04

Authorized Users: DoD and their direct support contractors as well as the U.S. Coast Guard and the Intelligence community.

Web Link

http://pmscp.monmouth.army.mil/contracts/deal-ibm/deal_ibm.asp

15 years of Delivering Significant Savings to DON and DoD customers

http://www.it-umbrella.navy.mil

The Umbrella Program provides easy-to-use, pre-competed acquisition vehicles that give you better life-cycle prices, higher quality, timely delivery, and guaranteed integration and interoperability with the standards-based technology you already have in place. We offer thousands of IT products, as well as an entire range of IT services to help you meet your mission needs. We leverage DoD and DON buying power and commercial best practices with a focus on industry trends to bring you the easiest acquisition solution and best savings available — anywhere!

www.it-umbrella.navy.mil

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

PERIODICAL
POSTAGE AND FEES PAID
SSC CHARLESTON
CHIPS MAGAZINE
USPS 757-910
ISSN 1047-9988