

Winter 2004

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. E-mail address: chips@spawar.navy.mil. Web address: www.chips.navy.mil.

Disclaimer. The views and opinions contained in CHIPS are not necessarily those of the Department of Defense nor do they constitute endorsement or approval by the DON CIO, DON IT Umbrella Program Office or SPAWAR Systems Center, Charleston. The facts as presented in each article are verified insofar as possible, but the opinions are strictly those of the individual authors.

Features

Page 6



"If any of you have any questions about the patriotism and the determination of the young men and women who wear the cloth of the nation I want to tell you to not worry about it."

**Admiral Vern Clark, USN
Chief of Naval Operations**

Page 8

"The application of advanced technology and innovative processes has time and again delivered results once considered unachievable."

**Admiral Walter F. Doran
Commander, Pacific Fleet**



Page 12



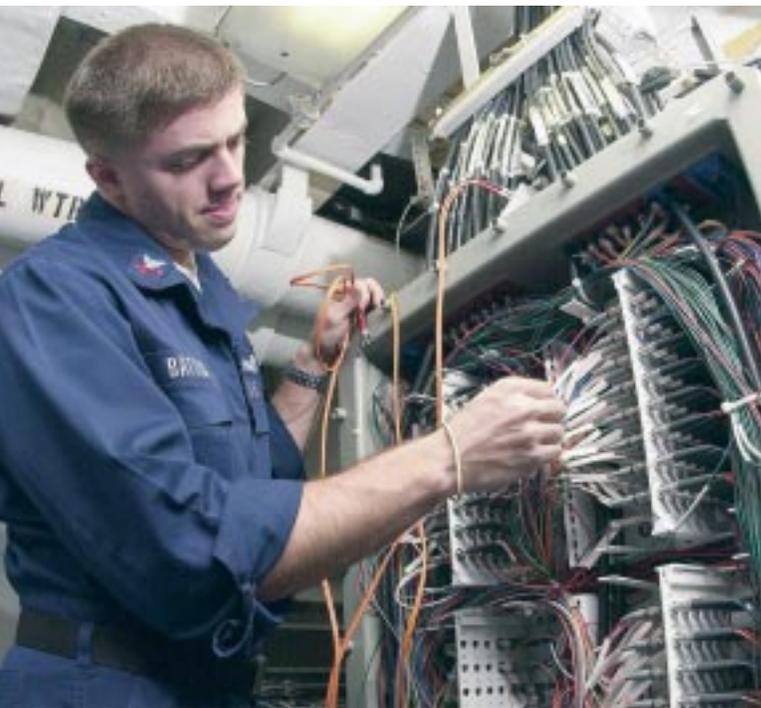
"The role of the IP Officer will continue to grow and mature as the needs of the Navy for technological innovation, information dominance and network-centric operations evolve."

**Lt. Cmdr. Danelle
Barrett, USN**

CHIPS WINTER 2004

Volume XXII Issue I

- | | | | |
|----|--|----|---|
| 4 | Editor's Notebook
By Sharon Anderson | 29 | Phase Gate Development for Project Management - Part IV
By Eric Verzuh, PMP |
| 5 | From the DON CIO
By Dave Wennergren | 32 | Are You Ready to PK-Enable?
By Rebecca Nielsen and Kenya Spinks |
| 6 | Lessons From the Desert
By Adm. Vern Clark, USN
Chief of Naval Operations | 34 | Can You Hear Me Now?
Managing the Electromagnetic Spectrum
By the DON CIO Spectrum Team |
| 8 | Overcoming the Tyranny of Distance
By Adm. Walter F. Doran, USN
Commander, U.S. Pacific Fleet | 36 | How do I implement the CMMI?
Part III
By Richard B. Waina, P.E., Ph.D. |
| 10 | The Air Force Leverages the Power of IT
By Brig. Gen. Glenn F. Spears, USAF
Director of Plans and Programs,
Headquarters Pacific Air Forces | 40 | Ensuring C4 for the Warfighter
By Lt. Col. Karlton D. Johnson, USAF |
| 12 | IPs In Action
By Lt. Cmdr. Danelle Barrett, USN | 42 | Portal Technology For Military
Supply Chain ERP Solutions
By Robert L. Sullivan and Robert B. Stevens |
| 16 | Realizing FORCENet: A Practical Example
By Lt. Cmdr. Edwin L. Armistead, USN,
Earle Kirkley, Andrew Mansfield, Dave Huff,
Ryan Hofschneider and Ben Holt | 44 | Teamwork Solves NMCI Problem
By Bob Bloudek |
| 18 | Therminator
By John McEachen, John Zachary and
David Ford | 45 | The Lazy Person's Guide to Voice Telephony -
Part I
By Retired Major Dale J. Long, USAF |
| 22 | The Federal Information Security
Management Act of 2002
By James E. Collins | 48 | Under The Contract
By the DON-IT Umbrella Program |
| 23 | The DON eGov Awards Fall 2003 | | |
| 24 | Civilian IT Workforce Skills Assessment - Part I
By Sandra J. Smith | | |
| 26 | First U.S. Navy Installation of DMS Afloat
By SPAWAR PMW 162-2, Tactical
Organizational Messaging for
Program Executive Office C4I and Space | | |
| 27 | A Perfect Fit: NMCP and XML
By Jack Gribben | | |



The Arabian Gulf (May 2, 2003) — Information Technician 2nd Class George Battistelli repairs Local Area Network (LAN) connections aboard the aircraft carrier USS Nimitz (CVN-68). U.S. Navy photo by Photographer's Mate Airman Shannon Renfro.



Information Systems Technician 2nd Class Ricardo Velazquez works aloft performing maintenance on one of the radars aboard USS Harry S. Truman (CVN-75). U.S. Navy photo by Photographer's Mate 2nd Class Andrea Decanini.

Editor's Notebook

As I'm writing to you most Americans are busy with holiday preparations, but many of our U.S. military personnel are deployed and serving far from home. I want to dedicate this issue of CHIPS to the brave men and women of the Armed Forces, who daily risk their lives for our freedom. I know that I join all Americans in saying thank you — we pray for your safe return.

In this issue we are delighted to feature the Information Professional (IP) Officer Community. Lt. Cmdr. Danelle Barrett provides a fascinating glimpse into their work and expertise in information, command and control and space systems. Please go to page 12 to read about IPs at the "tip of the spear."

The photos at left illustrate Information Systems Technicians (ITs) in action. ITs use state-of-the-art multi-media technology to execute information transfer, working with fiber optics, digital microwave, and tactical and commercial satellites on a global basis. They operate, manage and provide hardware and software support to multi-media Automated Information Systems (AIS) including: mainframes, mini and microcomputers, Local Area Networks (LAN), Wide Area Networks (WAN) and much more. IPs and ITs work together to execute the Department of the Navy IT vision.

It is a fascinating time to be working in any area of information technology in the Navy, and in the larger community of the Department of Defense. We are always eager to hear your IT success story so please contact us at chips@spawar.navy.mil.

Back at home — CHIPS Assistant Editor, Nancy Reasor has been working on a massive undertaking updating our subscriber addresses. Nancy does this continually and she has just finished consolidating mailings for several large commands. We want to thank Chuck Little from SPAWAR Headquarters, who updated the list of headquarters subscribers for us. Please contact Nancy at chips@spawar.navy.mil with address changes or if you are having any problems receiving your issue of CHIPS.

CHIPS was on the road fall 2003 to a few technology conferences where we were delighted to meet new subscribers and many longtime readers. Welcome to our new subscribers and thank you to the readers who stopped to say hello.

Sharon Anderson

"We must build forces that draw upon the revolutionary advances in the technology of war — one that relies more heavily on stealth, precision weaponry, and information technologies."

***George W. Bush
Commander in Chief***



Just reading through this issue of CHIPS Magazine highlights the fact that information technology (IT) is woven into the very fabric of our Naval mission and organization. "The Lazy Person's Guide to Voice Telephony" explores the telephone and its evolution from analog to digital technology over the years. "Are You Ready to PK-Enable" discusses enhancing both our security and enabling our eGovernment transformation through the use of Public Key Infrastructure (PKI) digital certificates. "Managing the Electromagnetic Spectrum" describes the process for identifying, allocating and employing electromagnetic spectrum to support the use of wireless IT systems and devices by our Sailors and Marines deployed around the world. From the desktop to the deckplate, everyone in the Department of the Navy is touched by IT.

Recognizing that technology is an enabling force across the organization, the recently released Department of the Navy (DON) Information Management/Information Technology (IM/IT) Strategic Plan for FY2004-2005 is a document that applies to everyone in the Department — not just our IT professionals. The vision and mission statements set the tone for a united team in support of our warfighting mission. Vision: A joint net-centric environment that delivers knowledge dominance to the Naval warfighting team. Mission: Transform Naval Information Management/Information Technology to provide affordable, next generation capabilities to the warfighter.

The strength of the Strategic Plan is that it truly is the result of a team effort, with ideas generated and drafts of the plan vetted throughout the Navy and Marine Corps organization. Six goals that support the vision and mission provide focus and clarity to our efforts. They are:

- ◆ Develop and maintain a secure, seamless, interoperable Naval IM/IT infrastructure
- ◆ Transform applications and data into Web-centric Naval capabilities
- ◆ Provide Full Dimensional Protection that ensures Naval warfighting effectiveness
- ◆ Ensure Naval IM/IT investments are selected, resourced and acquired to optimize Naval mission accomplishment
- ◆ Create optimized processes and integrated systems that enable knowledge dominance and Naval transformation
- ◆ Shape the IM/IT workforce of the future

As a member of the Naval team — whether Sailor, Marine, civilian or commercial partner — I hope that you will see the IM/IT Strategic Plan as your personal guide to help make the vision of network-centric warfare and knowledge dominance a reality throughout the Navy-Marine Corps team.

Dave Wennergren



DEPARTMENT OF THE NAVY - CHIEF INFORMATION OFFICER
W W W . D O N C I O . N A V Y . M I L



Lessons From the Desert

By Admiral Vern Clark, Chief of Naval Operations

you need them — take eight,” because that’s how many were ready — because we invested in readiness — and it wasn’t just carriers... I remember talking with the ACMC [Assistant Commandant of the Marine Corps] about potentials and if our amphibious structure was ready. They weren’t on the list, but in the third week in December we offered up Amphibious Task Force East and West, the U.S. Marine Corps-Navy team, and on the 6th of January they were rolling out the gate — and they weren’t on alert.

One of the things that we’re talking about is to make sure that as institutions we establish...attitudes that reinforce that we are going to live the lifestyle of readiness. We are going to exist in a culture of readiness.

Lesson number two: joint warfare is decisive. I’m tremendously impressed with the joint team and I press this point to everybody who wears a uniform. If you’re thinking about lessons learned and you’re not thinking joint — recalibrate. The future is about the Navy-Marine Corps team and the rest of the joint structure and — how we’re going to respond to give the president options.

... One of the tasks I have is talking to groups about why we need a Navy. I have a 30-, 20-, 15- and 10-minute speech — and sometimes I don’t even have that long. Sometimes I just have 30 seconds and the 30-second version is: credible combat power, far corners of the earth, sovereignty of the United States of America, anywhere, anytime, options for the president without a permission slip... My new favorite word is persistence. So now it’s not credible combat power, far corners of the earth, etc., it’s — credible, *persistent* combat power, far corners of the earth...

Lesson number three: access over flight and basing are not guaranteed. It fits in with the without a permission slip thing. Maneuver is a key part of Army discussions, but I don’t think we talk about maneuvers enough in the Navy, and we happen to have a pretty good-sized maneuver space. Lesson number three is about exploiting that maneuver space to the fullest. It’s about the freedom to maneuver.

We need to understand that maneuver

space allows us the opportunity to distribute our force in ways that we never thought about before, for example: a three-axis attack from the Red Sea, the Mediterranean and the Arabian Gulf. I’m convinced that to truly understand and get at the lessons in warfare — we must understand *LIMFACS*, the limiting factors that we confront in crisis. Access is going to be an issue everywhere we go.

For the U.S. Navy what it means to me at the strategic level is that this is what Sea Basing is all about. Sea Basing is about the ability to exploit the freedom to maneuver. So when the 4th Infantry Division couldn’t go in the East Med — we took it south and someplace else. When it was necessary to alter course for a long-range strike with TLAMs [Tomahawk Land Attack Missile] we just moved to where we could get the job done. These are examples, but the lesson for us is that in everything that we think about for the future we must understand the value of freedom to maneuver in the international domain. Very soon, you will see a report from the Defense Science Board that talks about the third leg of the triad in our Sea Power 21 strategy called Sea Basing. We need to think about Sea Basing in a very joint construct and what it does for the entire military structure...

The next lesson is inherent in operating from the sea base and it’s about reach. Reach equates to persistence... I’m going to be very careful about investing in anything that doesn’t have greater reach than we currently have. In Afghanistan, when we had a dozen Special Forces troops on the ground, it became imperative to have somebody close by in case they got in trouble. For the first time in our history we conducted routine operations, 7, 8 — 900 miles from the carrier. If you were an aviator in those experiences, it was an awesome experience in more ways than one. It’s like launching from 100 miles south of New Orleans, flying to Chicago, orbiting over the Great Lakes and waiting for the call on station. Now we couldn’t have done this without the U.S. Air Force and their tanker fleet. Those guys are going to the tanker four or five times then... landing on a “postage stamp” at 2 a.m.

We had the first operation with F-18 E/Fs. E/Fs are important for a whole lot of reasons, but I was excited that they could go all the

It is absolutely necessary for the Navy and the Department of Defense to dissect, study, analyze and determine the effects and causative factors of what we are accomplishing in Afghanistan and Iraq.

...We need to challenge every assumption — everything that we think about the way we conduct our business. It’s healthy for us to challenge those assumptions and see where the future takes us. In the course of these discussions it is absolutely appropriate that you examine tactical, operational and strategic perspectives. It would be inappropriate for me to talk about the tactical level perspectives and I’m not going to...but I will share this piece... First and foremost is that we are ready.

Strategic lesson number one is that readiness counts... It’s necessary to say that because we have not always had the discipline to finance a ready force. I think that as an institution it’s wrong to identify the requirement and then fund 85 percent of it. In my confirmation hearing, I said to Congress that it was my view that we had fundamentally understated the requirements and then we fundamentally underfunded the understated requirements — and we’ve done it for a long time.

So we invested in readiness... in the tools to see to it that the men and women who wear the cloth of this nation would be ready... We were in the tank in the third week of December [2002] and the plan was fundamentally set, but the force selection was not. I will never forget the Chairman asking me, “Vern, how many carriers can I have? Can we have four?” There have been times in the past that mustering four fully ready, in the green, all the way across and ready would not be possible. We have been famous in the past for crossdecking things. It was such a thrill to be able to say, “Yes General, you can. In fact, if

way to Baghdad without going to the tanker. We found the value of the E/F and it's ability to reach... We flew airplanes forward while Nimitz was en route and we flew them forward to the fight and brought them on board with the rest of the E/Fs from the Lincoln. The 26th Marine Expeditionary Unit was able to fly more than a 1,000 miles into northern and western Iraq from Suda Bay. Reach translates to persistence. *I don't want to buy any more stuff that doesn't go at least as far as what we own today. That's not a hidden message.*

Speed is a force multiplier. We have talked a lot about FORCENet. FORCENet is the key to the realization of Sea Power 21. We cannot have Sea Power 21 without reinvigorating our focus on interoperability and command and control structures that allow us to have and share knowledge. I'm disappointed that we are still building systems that stovepipe. Part of this is structure, part of this is cultural — the stovepipe Service system. Talk to Vice Adm. John Nathman, Deputy CNO (Warfare Requirements and Programs) (N6/N7), about things he is doing with the Air Force, Army and Marine Corps about this problem.

... We talk frequently about the enemy's asymmetric advantages. I am absolutely convinced that future enemies aren't going to go toe to toe with us... I'm concerned that asymmetries are something that we have to understand and live with every day in a comfortable way. We have to expect it. It has to be part of what we're about. We often think that they're the only ones who have asymmetric advantages. We have at least two. The first greatest advantage that we have is the ability to introduce and exploit technology to the advantage of the young men and women who are committing themselves to taking it to the enemy. Number two is the genius of these young men and women.

Sea Shield is about ensuring that we cannot just take the fight to the enemy, but that we can climb into the ring with the enemy. I just think you've got to be able to do that. I don't believe that you can win them all from over the horizon. There were some important things that happened in this conflict and one of them was the way ahead for theater ballistic missile defense. I can't give you exact numbers because it's classified, but the connection between the Army Patriot battery and its system, and our prototype system that was on the USS Higgins (DDG-76), produced a very satisfying result.

... In an article for the October 2003 issue of *Proceedings* magazine, "Rethinking the Principles of War," by Rear Adm. John G. Morgan, there is a phrase that I really like — "persistent precision." I'm absolutely convinced that persistent precision is going to change the way we fight... What I see happening in the future is that ground forces will fight differently... As we figure out how to exploit the technological advantages that come from the maneuver systems, persistent ISR will change the conduct of warriors on the ground... The future is about persistent precision fighting coupled with persistent ISR that allows one of our Soldiers or Marines to be able to bring precision to bear in ways that we do not understand today.

I want to say that predictability can be a liability. The Navy has been too predictable. If you want to know what we are planning to do next, go to the Navy Exchange, ask the cashiers, and they will give you our schedule... I commanded three ships and I learned that our current model, where we deploy ships, come home and put them in the shipyard has some disadvantages to it. In fact, I never deployed one that wasn't in better shape the day I brought it home than it was the day I took it out the gate.

Our model said, we can take this ship that's in better shape than it was the day we sailed into the shipyard and see if they can tear it up? Do you know what? They can. This is not denigrating to them [the shipyard], I'm poking fun at the model that we have used for 30 years, and it's time for us to rethink this. We need to think in terms of our ability to respond and to surge... We are going to rethink our maintenance concepts... We're going to rethink what it means to be ready. Instead of thinking about a ship or an aircraft squadron (or you name it) being ready to go, we want to recognize that the world of tomorrow is a more uncertain world than the world we live in today — and we are going to be ready to respond.

The military operates in support of diplomacy. When that methodology fails it flips around and then diplomacy operates in support of the military... I fundamentally do not see the value in six-month heel-to-toe deployments just for the sake of deployments. I would much rather have a Navy that is able to respond and give the president options. So if a country is acting up — it's far better to think in terms of surge ready. How many do you want Mr. President? A strong message to follow and four or five [ships] show up that are capable of doing real work. That's what the future is about ladies and gentlemen — and that's where we're going.

... You cannot do these things without a ready force. The first week of this journey we established the number one priority in our Navy and that is we were going to win the battle for people. I just want to share with you that it's very fulfilling and rewarding to be able to tell you that we are winning it. At the top of my list of challenges is that our retention is too high and we have too many people. Congress gives us a window for how many people we can have. Up until 9-11 they gave us a small cushion. On 9-11 they changed all the rules and said, Navy, Army, Air Force, Marine Corps, you can have a two percent surge and if you get special permission you can have three. Oh, by the way, we didn't give you money for that... We were counting noses in September [2003] getting to where we needed to be.

When I took command of the Atlantic Fleet in September 1999 our first term retention in the Atlantic was 19 percent. All my life it ran in the 20s and once in a while it would creep into the 30s. Last year I said we are going to reduce attrition by 25 percent. We didn't make it. We only made 23. In FY03, through September 1, first term retention in the U.S. Navy was 64.2 percent. If any of you have any questions about the patriotism and the determination of the young men and women who wear the cloth of the nation, I want to tell you to not worry about it. These young men and women are absolutely fantastic... We are winning the battle on people.

So the lessons are these: If you can win the battle for people and we are; and if you can establish a culture of readiness and an operational construct that allows you to be surgeable and deployable as opposed to extraordinarily predictable — we will have the strategic level tools coupled with the injection of all of the technology that we're talking about creating for the future. That is what we are investing in — to be the right kind of team player in the joint force of tomorrow. And that's the number one lesson from the desert.

Editor's Note: Admiral Clark's article has been edited from his remarks to the U.S. Naval Institute Eighth Annual Warfare Exposition and Symposium, October 8, 2003. The full text of his remarks is available at www.chinfo.navy.mil/navpalib/cno/speeches/clark031008.txt. □

Overcoming the Tyranny of Distance

In 1789, it took George Washington eight days to travel from his home in Mount Vernon, Va., to his Presidential inauguration in New York City. The fact that it took George Washington eight days may seem incredible to us today, but what is more amazing is that it would have taken roughly the same amount of time throughout the previous 2,000 years to cover that distance. No real progress was made in over 20 centuries! Moses, Aristotle or Julius Caesar could have traveled those same 200 miles about as quickly as our first President did.

Why was that? Lack of talented engineers? Complacency? Did the distance barrier seem insurmountable?

In today's terms, I think we have an abundance of talented engineers. As for complacency, the race to set new standards and reap its rewards usually eliminates that issue. And from a military and force protection standpoint, September 11 reminds us of the consequences of complacency. I would also say that no barrier is insurmountable, however, it is logical that we will continue to encounter new barriers as we overcome others, especially in the information arena.

I'd like to talk about some of the ways we are overcoming the barriers we are faced with and then discuss a few future initiatives that will help us continue breaking down all the distance barriers we encounter. As you know, the Pacific region is both vast and diverse; it covers over half of the earth's surface and ensures that we are constantly challenged by what we call the "tyranny of distance." We've dealt with this tyranny many ways in the past — often with help from you.

When I joined the Navy, we overcame the distance barrier through sheer numbers. At the height of the Cold War we were deploying a nearly 600-ship fleet and pushing them forward in waves and spreading them across the oceans. Those days have passed, and for good reason — our technology pushed forward. With the advent of link technology, we transformed from a force needing to transit in close quarters — to Carrier Strike Groups able to spread their ships out over hundreds of miles.

Today with satellite communications, advanced communication systems like EHF, and now satellite links and chat rooms, a Strike Group leaving San Diego for the Arabian Gulf can achieve situational awareness by tapping into critical, real-time information even before they leave homeport. Once they have gotten underway, ship technicians overcome the distance barrier through reachback maintenance support. They are able to gain assistance in diagnosing and repairing casualties through existing technology like the Internet, chat or VTC, keeping ships on station and minimizing downtime for critical equipment.

The impact of information technology addressing the distance barrier isn't limited to deployment operations. It has also enabled us to leap forward in the way we train our forces. The Fleet Combat Train-



Admiral Walter F. Doran
Commander, U. S. Pacific Fleet

ing Command Pacific is currently using the Battle Force Tactical Training system during inport exercises to improve the training of Strike Group command and control elements from simple reporting procedures to the correct application of rules of engagement in a realistic environment. With this improved technology, our Strike Groups can practice and evaluate their tactics, techniques and procedures inport — before getting underway.

These training exercises have traditionally been designed to train a single Strike Group on each coast separately. But this February, we will conduct our first "Multi-Strike Group Inport Exercise" and break that distance barrier. Three Carrier Strike Groups separated by thousands of miles (Stennis Strike Group in San Diego, Vinson in the Pacific Northwest and the Truman Strike Group in Norfolk) will train simultaneously, utilizing a collaborative training scenario.

Everyone on the ships from the petty officers on the consoles to the admirals and their staffs will train through the same simulated combat scenario.

And the technology just keeps getting better, as is the case with the Navigation, Seamanship and Shiphandling (NSS) Trainers being implemented throughout the Pacific Fleet this fiscal year. Our fleet concentration areas will be outfitted with "bridge mock-up" simulators for complete navigation team training, and our ships will be equipped with a version that includes virtual reality hoods designed to train individual watchstanders, enabling Sailors to see precisely what they would see from the bridge of their ship. Soon a ship heading into a port they haven't been to before will be able to practice by plugging into an onboard simulator. The use of advanced simulation has much potential in every aspect of our business and will allow us to sharpen our skills and more effectively train our force for the real-world operations we'll face.

As you know, today we are fighting a new kind of war — a global war where we need every advantage we can get — and technology is giving us an edge. Our adversary is now spread throughout the theater; hiding, making our task more challenging, but we will ultimately defeat this asymmetric enemy by capitalizing on our asymmetric advantage. That asymmetric advantage is in the brilliant minds of America's technical community and our brave men and women in uniform working toward the same goal of winning the Global War on Terrorism.

Information Technology enables transformation. An example of this is our approach in the Pacific to developing a Standing Joint Task Force, known as JTF-519. This task force, under the command of the Pacific Fleet Commander represents every Service and is spread throughout the Pacific region — from Japan to Alaska — with elements as far east as Fort Bragg, N.C., and Fort Meade, Md.

Clearly, the distribution of our team creates quite a distance barrier, but we have overcome that challenge by applying the technology

you've provided. While geographically separated, Task Force members stay connected by training and planning via the Internet and tailored Web sites. I bring the staff together twice a year to test our planning and nurture the relationships we've established from afar. The results have been outstanding and the staff is an important warfighting resource for the Combatant Commander.

That's one example of how technological efficiencies are breaking distance barriers, and enabling your military to carry out our nation's mission. Many more examples are on the horizon. Another way to conquer distance is to have faster ships. That sounds rather simple, but the current technology that has emerged in the form of high-speed surface vessels, which we call HSVs, is anything but simple. These HSVs have already proven their worth as transports, and with their shallow drafts, as Special Forces insertion platforms. HSV technology can also help enable the development of our Littoral Combat Ship — a ship that can go 40 or 50 knots, outfitted with tailored combat mission modules and unmanned vehicles, to influence their area of operations.

Another important initiative, still in its formative stages in the Pacific, is the Regional Maritime Security Program (RMSP). First and foremost, this program depends upon the establishment of enhanced Maritime Domain Awareness — essentially knowing what is traveling on our waterways. There are capabilities and systems already in place, and others in development that can help us improve our situational awareness of the high seas.

One example is the Commercial Satellite Communications System, which comprises the various commercial communication systems that routinely operate over water including Inmarsat, the Argos system and Iridium communications satellite systems among others. These systems either currently have or could be easily modified to develop position reports from GPS and transmit reports containing time and position. Communications ground stations could receive these messages from mobile units and generate identification, position reporting and tracking data at user-determined intervals. As the CNO, Adm. Vern Clark has said, we need to network Navy assets with the Coast Guard and other intelligence agencies to identify, track and intercept threats long before they threaten this nation.

Another very promising example of progress in interoperability is the CENTRIX (Coalition Enterprise Regional Information Exchange) system, which continues to evolve and improve coalition interoperability. Currently CENTRIXS allows us to share with our allies, time-critical, tactical information at the SECRET releasable level through e-mail, chat and Replicated Web Site capabilities, with Common Operational Picture Tools in development. CENTRIXS-J, which we tested with the Japan Maritime Self-Defense Force during ANNUALEX in November 2003, has a built-in language translator — helping us overcome not only the distance barrier, but also the language barrier, which can often be every bit as challenging.

The Asia-Pacific Area Network (APAN) has already been tested to help share information with other responsible navies on simulated motor vessels suspected of trafficking terrorists or weapons of mass destruction. With systems like CENTRIXS and APAN, we're on the verge of realizing real Maritime Security. I know that you will help get us there — and FORCENet may be the piece that brings all of this together. At my Commander's Training Symposium last month [October 2003], Vice Adm. Dick Mayo shared his vision of FORCENet

bringing us complete battlespace awareness, space access to all satellite data at the unit level and dynamic real-time intelligence on critical areas of interest. Knowing the location of all ships, planes and submarines (friendly, neutral or otherwise) is the ideal vision sought by FORCENet.

Joint interoperable information sharing will be commonplace as well as mission analysis and information exchange with our coalition partners. We will be a fully networked, combat capable, joint fighting force. The realization of this vision will depend on the technical community and your ability to develop these enabling technologies. The result could go a long way to enabling our forces to achieve victory in the Global War on Terrorism. We have made incredible progress over the years developing transformational capabilities, but we need to keep pushing.

Barriers often exist only because we don't believe improvement is possible. As World War II drew to a close, there was much debate as to whether a fixed-wing aircraft could fly faster than sound or if a human pilot could survive the experience. Conventional wisdom held that this invisible threshold would forever serve as an impediment to aircraft development and contemporary aircraft structures. But the innovative minds of the men and women at Reaction Motors Inc. built their rocket-propelled engine anyway, and engineers Robert Woods and Larry Bell designed the X-1 aircraft — and then, on October 14, 1947, a brave Air Force officer, Captain Chuck Yeager climbed aboard and became the first man to fly faster than the speed of sound. Today, what was once thought impossible is a routine occurrence.

The application of advanced technology and innovative processes has time and again delivered results once considered unachievable. We've experienced similar record-breaking performance through the application of advanced technology and innovative processes. During the first Gulf War, TLAM strike planning took on average, four days and extensive coordination between all operating units. During Operation Iraqi Freedom, strike planning was generally accomplished in less than four hours while sharing a Single Integrated Operations Picture nearly simultaneously with all participating units.

These are but a few examples of advancements made in recent years. Innovative minds and determined spirits find ways to overcome the insurmountable distance barriers — and change the world in the process.

There is a story about Ronald Reagan that his wife Nancy liked to tell. He was speaking at the University of California, and a student got up to say that it was impossible for people of Ronald Reagan's generation to understand the next generation of young people.

"You grew up in a different world," the student said. "Today we have television, jet planes, space travel, nuclear energy, computers..."

When the student paused for breath, President Reagan said: "You're right. We didn't have those things when we were young. We invented them."

Editor's Note: Adm. Doran's article has been edited from his remarks at TechNet Asia-Pacific, November 5, 2003. □



The Air Force Leverages the Power of IT

Brig. Gen. Glenn F. Spears is Director of Plans and Programs, Headquarters Pacific Air Forces, Hickam Air Force Base, Hawaii. In this capacity he serves as the PACAF focal point for developing theater contingency plans; command input for the Department of Defense planning, programming and budgeting system; and regional security and international affairs assistance. He also oversees doctrine development and command arrangements and manages resources, force development and modernization.

General Spears is a command pilot with more than 3,200 flying hours in 13 types of Air Force aircraft. The general's awards and decorations include the Legion of Merit with two oak leaf clusters, the Bronze Star Medal, the Defense Meritorious Service Medal, the Meritorious Service Medal with two oak leaf clusters, the Air Force Commendation Medal with oak leaf cluster and the Kosovo Campaign Medal.

As the PACAF Director of Plans and Programs, my team develops the command's long-range, deliberate plans to implement national, military and theater strategy in support of our nation's interests. All of these plans rely heavily on information technology. Furthermore, we develop and oversee the PACAF program, our long-range budget. In doing so, we attempt to take full advantage of IT to leverage its nearly boundless capabilities to save dollars, save manpower and reduce risk. However, I'm also an operator. While currently desk-bound, I've spent most of my career in the field, and I depend very much on the information technology that you engineer and provide. Let there be no doubt — I am a believer in the value of IT!

From the origins of our Air Force there has been a unique connection between our Service and technology. In fact, from the defining moment of powered flight in 1903, to the creation of the Air Force as a separate Service in 1947, to the present — the Air Force and technology have been inexorably linked.

I'd like to review for you the major components of PACAF's mission and what information technology means to us here in the Pacific. Then, I'll discuss how IT was used as a force multiplier during our recent conflicts in Afghanistan and Iraq. After that, I'll bring you up to date on some of PACAF's IT programs. And lastly, I'll present some of our future plans that involve IT.

First of all, as many of you know, PACAF's primary mission is to provide U.S. Pacific Command and our global, expeditionary Air Force with ready air and space power. As General William Begert (Commander, Pacific Air Forces) often says, we are a full service Component Command, providing PACOM with the full range of Air Force capabilities. This includes combat strike, mobility, intelligence, information operations, expeditionary combat support and space capabilities. We promote U.S. interests in the Asia-Pacific region during peacetime, through crisis and in war.

We accomplish this mission across the vast PACOM AOR. It extends from the west coast of the continental United States to the east coast of Africa and from the Arctic to the Antarctic. In total, this area of responsibility covers more than 100 million square miles. While some 70 percent of the AOR is covered by water — all of it is covered by air and space! This AOR is home to nearly 2 billion people who live in 43 countries, and includes some 16 time zones. Do we rely heavily on IT to do our job? You bet we do. Information technology helps us prevail over the tyranny of distance.

Today, information may be the world's hottest commodity. However, the military wants more than information; it wants and needs information superiority. Information technology is a crucial area that helps us to gain information superiority, improve readiness and

enhance mission performance. Advanced information technologies allow us to engage any target, anywhere in the world, at any time. IT impacts virtually every functional area within PACAF — from medical to personnel, engineering to operations and everything in-between. Information, itself, is considered a weapon.

The second point I want to emphasize is the importance of information in the way we conduct combat. During our recent conflicts, IT was a true force multiplier. Information technology reduced risk, saved manpower and money, increased efficiencies and improved effectiveness. Many heard the story of young Airmen riding horseback in Afghanistan using a laptop, GPS and a laser designator. They successfully directed surface attack and close air support. They leveraged technology to employ strikes from B-52s, a mid-20th century designed platform engaged in a 21st century battle. Better still, we used data links and feeds to employ an unmanned aerial vehicle (UAV) with air-to-ground missiles in a close air support role. Can you imagine the enemy's shock as we confidently relied upon a UAV to attack them within 50 yards of our coalition forces? The raw power of IT available to our forces today is staggering.

One of our key lessons learned from recent operations in Afghanistan and Iraq is the criticality of our air operations center — another IT-powered force multiplier. The AOC enabled commanders to employ joint and coalition airpower, destroy strategic leadership targets and prosecute time critical targets with speed precision never seen before in combat. And, we could do it day or night, in all weather conditions. Today, the Air Force considers our AOCs as weapons systems — just like a B-1, C-17 or F-16. The AOC is the embodiment of network-centric warfare. It remains the nerve center for all air component missions in support of operations in Afghanistan and Iraq.

In today's AOC, warriors translate the Joint Force Commander's guidance to produce the effects desired across the battlespace, which often involves identifying and analyzing targets. Some of those targeteers are traditional "steel on target" conventional planners. However, today we also include space warriors and information warfare warriors in the AOC. We place the kinetic warriors side-by-side with the non-kinetic warriors. And, they're leveraging IT to make sure we achieve the right effects on the right targets.

Let me now shift gears to discuss some of PACAF's IT initiatives and programs. We assign IT to the principal-supporting role in the command and control of air and space operations. The Pacific Operations Support Center, Air Mobility Operations Control Center and our AOCs are key command and control nodes. PACAF commands two of the five CSAF-designated "Falconer" AOCs around the world. We have a permanent one in Korea, and it is unarguably the most developed AOC we have in the Air Force. The processes are mature,

although we constantly upgrade the equipment and the software. Our other AOC is deployable and located at Hickam AFB. We call this the Pacific AOC or PAOC. Where the Korean AOC is focused on conflict on the Korean peninsula, the PAOC supports crises or conflicts in the rest of the AOR. The personnel in the PAOC are capable of planning and executing thousands of combat support sorties daily. They can orchestrate detailed airspace deconfliction between hundreds of aircraft and conduct simultaneous time critical targeting. But what really makes this staggering is that we plan on doing all of this — thousands of miles away from the battlespace. To do that, we must have uninterrupted and secure communication and bandwidth. Where we require the most help from you is managing our data to maximize existing bandwidth, and also to help us increase our bandwidth.

On another note, many of our PACAF C2 networks have been developed as ad hoc, nonstandard systems consisting of stovepipe connectivity. These limit our capability to provide C2 across the command. As a result, we created a C2 Network Modernization and Revitalization plan. We will upgrade and expand the network infrastructure supporting C2 systems at all nine main operating bases. Our blueprint calls for growth and modularity for future upgrades, expanded bandwidth and bigger switch port capacity.

In the communication and computer area, we implemented a server consolidation at all nine of our bases on the classified and unclassified sides. You helped us be the first major Air Force command to do that. We moved the command to WIN2K directory architecture. Additionally, we created a secure Web portal with collaboration capability. And you helped us be the first Air Force MAJCOM to do that as well. Currently, all our functional areas are populating the portal to make it a world-class tool.

We've begun our first command-wide personal computer replacement program, which will aid every combat and combat support mission area. Our networks have evolved into command and control systems with the Defense Messaging System and the way we use e-mail. Soon, all PACAF bases will regularly backup over 10 terabytes of data. Now, I don't know a terabyte from a pterodactyl, but our IT experts tell me that it's a boatload of ones and zeroes! Without a doubt, every combat sortie and virtually every action taken by PACAF forces has one thing in common: They all rely on IT to get the job done. From desktop computers to GPS to tactical data links — IT is an integral part of every PACAF mission area.

Lastly, what does the future hold for IT in PACAF? As recently as five years ago, few could have predicted: a Global War on Terror, record setting OPSTEMPO, and Operations Iraqi Freedom and Enduring Freedom. The asymmetric terrorist attacks demonstrated that some of our adversaries do not require standing armies or a vast industrial base to inflict harm on American people. We've all witnessed what a few evil and deluded men can do. And the dangers have not passed. Today, we face threats from weapons of mass destruction and global terrorism, wielded by state and non-state actors. We live in an era of highly unpredictable threats. That is why we need robust and flexible IT that can rapidly adapt to any contingency. We are just beginning to fully leverage IT to help us improve our readiness and boost mission performance.

Our future emphasizes an integrated space and C4ISR architecture. This will streamline the power of IT for better predictive battlespace awareness and better real-time targeting. Horizontal integration of intelligence, surveillance and reconnaissance assets with striker as-

sets on a network-centric environment integrated with the AOC is a top priority. In this respect, I want to highlight three areas. First, as mentioned, AOC standardization is becoming a reality in today's Air Force. We will soon baseline all of our AOC Weapons Systems to the same standards — a common configuration. Furthermore, at the Korean AOC we will soon upgrade the supporting communication infrastructure, secure systems upgrades and field a new data wall. All of these capabilities will speed our decision-making processes and command and control capabilities.

Second, we are considering a possible force buildup at Guam. One piece of this initiative includes the possible bed down of Global Hawk UAVs at Andersen AFB. However, while the launch and recovery will be executed from Andersen, the mission control elements would be based at Hickam, and the feeds would stream into our new Distributed Ground Station, DGS-5. In other words, the personnel launching and landing the Global Hawks and those processing and analyzing the intelligence collected would be separated by over 4,000 miles. But to the commander, that tyranny of distance just won't matter. Data links, UAV streaming video and collaborative tools in our ISR Ground Stations are all examples of ongoing engagement chain improvements.

And lastly, our future emphasizes advancements in smarter, smaller and more accurate weapons. That's why we equipped all of our F-16s on the Korean peninsula with GPS-guided Joint Direct Attack Munitions (JDAM). JDAMs, in combination with laser-guided munitions, give us the flexibility to engage various targets in multiple scenarios and in all weather. We need to integrate all of these systems, new and old, to provide information rapidly, speed the decision processes — and prosecute the enemy quicker. Our imagination is the only limit, OK, dollars may be the limit, but many of our recent initiatives have paid for themselves and will save money and personnel for years to come. We must continue to develop seamless joint and combined operations, systems connectivity and interoperability. We must be trained and equipped to fight as one force.

IT should be transparent to users. The real trick is to make sure we have the right information provided to the warfighters at the right time. Users don't want to be burdened with the magic that goes on behind the scenes. The warfighter just wants to push to talk or point and click, and be confident that he has secure and reliable communications. Recently, Secretary of Defense Rumsfeld asked the U.S. Senate Armed Services Committee to consider this, "Imagine for a moment that you could go back in time and give a knight in King Arthur's court an M-16. If he takes the weapon, gets back on his horse and uses the stock to knock his opponent's head, it's not transformational. Transformation occurs when he gets behind a tree and starts shooting." The mutual progression of technology and our Tactics, Techniques and Procedures (TTP) is an absolute essential.

The U.S. Air Force is unquestionably a Service born of technology and transformation. The Wright brothers realized the impossible 100 years ago. What's over the next horizon? We are a nation of doers and thinkers. Much of our attitude about technology is a direct result of the close bonds the warfighters share with scientists and engineers — great men and women like you. These ties are deeply rooted in our Service culture. I look to this audience to help mold and shape our future. Your collective knowledge is priceless in effectively applying leading-edge technologies. □



IIPs in Action

By Lt. Cmdr. Danelle Barrett, USN

"We are the Navy's community of Information Warriors with expertise in information, command and control, and space systems. We own the Naval Network, the foundation of information dominance and successful execution of Naval, joint, allied and coalition operations. We plan, acquire, operate, maintain and secure the Naval Network and the systems that support Navy's operational and business processes to ensure they are reliable, available, survivable, and secure. We evaluate and integrate leading edge technologies, innovative concepts, and essential information elements to ensure a warfighting advantage. We will aggressively foster development and maturation of the skills needed to conduct network-centric operations, both afloat and ashore."

Information Professional Mission Statement

In July 2001, the Chief of Naval Operations formally announced the creation of the Information Professional (IP) Community (1600 restricted line designator) in NAVADMIN 182/01. With the help of the Fleet Commanders, the number of afloat and operational billets (where C4 expertise was most needed) was increased, a training and qualification program was implemented and a sense of community emerged among the newly formed cadre of IP officers.

A reserve counterpart (1605 designator) was added shortly thereafter. Semiannual lateral transition boards for active duty officers have grown the IP community to over 440 strong. These officers are playing important roles in billets heavily focused on operational C4 expertise and technological innovation. Below are just a few examples of IPs in action around the world, providing the warfighting advantage.

IPs at the Tip of the Spear in Operations IRAQI FREEDOM and ENDURING FREEDOM

Lt. Cmdr. Angie Albergottie was recently forward deployed from March through August 2003 in Baghdad, Iraq. While there, she put her extensive talents to work for the Iraq Coalition Provisional Authority (CPA) staff in support of Operation Enduring Freedom (OEF) and Operation Iraqi Freedom (OIF) and postwar Iraq reconstruction. She provided a broad range of support services for a multinational, interservice coalition, as well as an interagency headquarters supporting a presidential envoy and the CPA administrator for the nation of Iraq.

Lt. Cmdr. Albergottie was appointed the Officer in Charge of the Intermediate Staging Base where she coordinated C4 support to the Joint Task Force. Additionally, she oversaw the requisition, configuration and installation of communications and computer equipment supporting a joint staff in combat operations that grew exponentially from a planned 250-person headquarters to well over 2,800 personnel, including 25 ambassadors, 16 flag officers and numerous presidential appointees. Despite the arduous environment, tenuous supply system and ever-changing priorities, Lt. Cmdr. Albergottie was instrumental in leading her joint team of 20 personnel. She ensured the Communications Sup-

port Office provided the timely and reliable support that enabled successful command and control of forces throughout the region. Lt. Cmdr. Albergottie laid the foundation for those who will follow her. Currently there are five other IP Officers assigned in Baghdad supporting CPA and JTF 7 Command and Control.

Cmdr. Jack Steiner, Cmdr. Pamela Wynfield, Lt. Cmdr. Mike Thrall, Lt. Cmdr. Suzanne Prose and Lt. Cmdr. Ron Hanson were five IP Officers who led the way in providing expert communications planning, direction and execution for afloat units participating in the OEF and OIF. While deployed in the Arabian Gulf and Mediterranean, they were instrumental in ensuring their commanders had the communications infrastructure in place to effectively command and control forces, and they coordinated critical reachback support for targeting via various communications channels. Innovation and resourcefulness characterized their efforts as they worked diligently to ensure small bandwidth disadvantaged units and coalition partners were able to effectively communicate within their respective groups.

During OIF, Cmdr. Steiner, the USS Harry S. Truman Carrier Strike Force and Commander Task Force Six Zero (CTF 60) Communications Officer, conducted communications planning and resolved the day-to-day communication challenges of a two-carrier striking task force comprised of the Harry S. Truman and Theodore Roosevelt carrier strike groups. His orchestration of this effort required close coordination with Lt. Cmdr. Ron Hanson, the Communications Officer on Commander, Cruiser Destroyer Group Eight, Lt. Cmdr. Suzanne Prose of Commander, Cruiser Destroyer Group Two, communications planners at Commander Sixth Fleet (C6F), as well as with the critical shore communication nodes at the Naval Computer and Telecommunications Area Master Stations Atlantic and Europe (NCTAMS LANT and NCTAMS EURCENT).

Cmdr. Steiner's innovative ideas led to dramatic improvements in operational capabilities for the strike group staffs. He coordinated with the staff and carrier intelligence teams onboard the USS Harry S. Truman to establish a Global Broadcast System (GBS) imagery delivery capability, which afforded the carrier a five-fold increase in available bandwidth for image delivery and enabled reutilization of bandwidth on other channels. Cmdr. Steiner's



Lt. Cmdr. Angie Albergottie at work in Iraq.



Lt. Cmdr. Ron Hanson, IT2 Dianne Ruiz Torres and IT1(SW) Mahogany Moore in Radio aboard USS Theodore Roosevelt.



Cmdr. Jack Steiner



In the CCDG1 war room on CV-64 in the Arabian Gulf, March 2003 (left to right), Capt. Mitch Schwecker, CCDG1 N6; IT2 Darryl Goodloe, CCDG1 Knowledge Management and Coalition Comms. Technician; ITCS Rick Shute, CDS7 C4I Officer; Stacey Minor, FSET representative; Cmdr. Pamela Wynfield, CCDG1 Deputy N6 and Knowledge Manager; Cmdr. Mike Daly, CV-64 CIC Officer; ITCM Paul Sigmon, CCDG1 Asst. Comms. Officer; Ensign Keith Berens, CV-64 CMS Officer; Lt. Cmdr. Gary Myers, CV-64 Combat Information Systems Officer.



Lt. Cmdr. Suzanne Prose aboard USS George Washington (CVN-73) going through the Suez Canal.

innovative leadership in C4 led to his selection as a 2003 Copernicus Award winner by the Armed Forces Communications and Electronics Association and the U.S. Naval Institute.

To support OIF, C6F, NCTAMS EURCENT, NCTAMS LANT and CTF 60 established a communication architecture which relied upon commercial and military satellite communications for network and telephone services, including SIPRNet chat and e-mail for tactical operations and coordination, and unclassified e-mail for embedded media support. Systems were used in new ways to increase command and control effectiveness. For example, Lt. Cmdr. Ron Hanson working with Cmdr. Wendy Bransom at NCTAMS LANT, successfully tested the use of the GBS within the Theodore Roosevelt Strike Group for delivery of record message traffic. This capability is extremely important and can be used to eliminate backlogs and ensure timely delivery of operational orders for units in the GBS satellite footprints.

The GBS also served as the primary imagery delivery workhorse. Extremely High Frequency (EHF) MILSTAR satellite communications provided essential unit-level Tomahawk strike command and control. Connecting the multiple systems into a tactically reliable command and control infrastructure required close coordination among experts in multiple disciplines to work toward a common vision and architecture. These experts included Information Systems Technicians (ITs), Electronics Technicians (ETs), Operations Specialists (OSs), Intelligence Specialists (ISs), and their khaki leadership. Senior IT, IP, Limited Duty Officer and Intelligence personnel developed a command and control infrastructure, which they presented to the commanders. Once the commanders agreed upon the final architecture, the experts quickly put it in place.

The system was built around a theater-wide plug-and-play concept with resources allocated to meet mission needs within the theater. Key IP communication personnel, such as Cmdr. Steiner, Lt. Cmdr. Prose, Lt. Cmdr. Hanson, Cmdr. Wynfield, Lt. Cmdr. Thrall and others, coordinated daily to maintain the architecture, adapt to emergent changes and conduct long-range planning — always with a focus on task force mission execution.

As Commander, Cruiser Destroyer Group One (CCDG1) Deputy N6 and Communications Officer, Cmdr. Pamela Wynfield and Lt. Cmdr. Mike Thrall, respectively, took the lead for West Coast strike groups deployed for OIF and OEF. Aboard the USS Constellation



Front row, left to right: Lt. Cmdr. Laura Yambrick, Cmdr. Diane Webber and Capt. Treci Dimas. Back row, left to right: Lt. Cmdr. (s) Jody Grady, Lt. Cmdr. Murry Carter and Lt. Cmdr. Yvonne Norton.



From left to right: Capt. Skip Hiser, Cmdr. Tina Swallow and Lt. Jon Kaltwasser of Task Force Web.

(CV-64), their C4 responsibilities as Carrier Strike Force and Commander Task Force Five Five (CTF 55) extended from the Red Sea through the Straits of Hormuz up into the northern Arabian Gulf, and eventually into Umm Qasr, the main southern port in Iraq.

The CTF 55 communicators led by Cmdr. Wynfield and Lt. Cmdr. Thrall, along with communicators in three other Carrier Strike Forces in CTF 50 (USS Lincoln, USS Kitty Hawk, and just prior to out-chopping the Gulf, the USS Nimitz) coordinated and executed detailed, in-depth communications plans. These plans included frequency deconfliction for hundreds of coalition aircraft and a C4 architecture for the CTF 55 ships and submarines that ensured sustainable, reliable, secure communications for their varied and complex missions.

Cmdr. Wynfield coordinated iterative development for Collaboration at Sea/Knowledge Web (CAS/KWEB) primarily for knowledge sharing and replication for afloat units. CAS/KWEB is used by hundreds of personnel and particularly operational staffs. CAS/KWEB makes use of an IP-based replication and synchronization method to share Web pages and manage daily operational reports among afloat units with limited and often times discontinuous bandwidth. She promoted the use of collaborative tools such as chat rooms for real-time and emergent battle group awareness, e-mail for one-on-one and small group interaction, and white boards for extensive near-real-time coordination to improve command and control of forces and daily operations.

Several of the IP Officers who played key roles during OIF and OEF were already forward deployed to the “tip of the spear” in Bahrain. These officers work in the Central Command theater (an area normally operating at a high operational tempo even when not at war) and found themselves additionally challenged during the most recent operations.

Capt. Treci Dimas, the Assistant Chief of Staff for Command, Control, Communications and Computers for Commander, U.S. Naval Forces Central Command and Commander U.S. Fifth Fleet, and her staff (Lt. Cmdr. Laura Yambrick, Information Systems Division Officer; Lt. Cmdr. Murry Carter, Director, Bahrain Information Technology Service Center; and Lt. Cmdr. (s) Jody Grady, Automated Information Systems Plans Officer), along with Cmdr. Diane Webber and Lt. Cmdr. Yvonne Norton, Commanding Officer and Executive Officer, respectively, of U.S. Naval Computer and Telecommunications Station Bahrain, were instrumental in delivering the communications services required to sustain both land and sea-based operations for the thousands of deployed Sailors, Soldiers and Marines.

This support included day-to-day C4 services and direction for the forward deployed U.S. Naval forces, along with coordinated C4 support to ground mobile forces, Special Operations Forces and coalition partners from several nations. Again, as with the IP Officers who were afloat, teamwork was the hallmark of their work and the key to their success. They continue to find innovative ways to deliver more capacity to the warfighter and make lasting improvements to the overall C4 architecture in the region.

All of these IP Officers emphasized that the key to communication success in OIF and OEF was due to the superior teamwork between the many afloat and ashore C4 professionals. The leadership and technical proficiency of the IP Officers profiled here, along with the willingness of the commanders who rely on their communications expertise, were instrumental in achieving an unprecedented level of C4 excellence in operations.

IPs at the Forefront of Innovation — Task Force Web

Several IP Officers have had the unique opportunity to be a part of Task Force Web, a Vice Chief of Naval Operations special project, to develop and implement a Web-Services architecture for the Navy. Capt. Skip Hiser, Capt. Maureen Copelof, Cmdr. Tina Swallow, Cmdr. John Hearne and Lt. Jon Kaltwasser have been in the forefront working with industry leaders, the World Wide Web Consortium (W3C), academia, and joint/coalition partners to develop and implement a Web-Services architecture that will revolutionize the way data are used, transferred and shared. For their efforts Task Force Web was named one of the Department of the Navy’s eGov winners for Fall 2003 for “Building the Web Enabled Navy (WEN), an excellent example of a transformational initiative contributing to business and mission improvement and effective information exchange.”

Key components of their architecture rely on the use of data sharing and reuse, open standards and vendor-neutral interfaces. The result will be a shift in focus from providing “systems” to improving functionality, interoperability, data reliability, security and speed to support the warfighter. Lt. Kaltwasser, the newest IP of the group, has been able to parlay his operational experience afloat into providing a technology solution that works across the Navy enterprise, both afloat and ashore. His expertise, coupled

with his extensive computer science and networking background, made him an ideal choice for finding solutions for some of the Navy's toughest technological challenges, and put him at the forefront of IP innovators for the Navy.

IPs Breaking New Ground for Operation Joint Guardian in Kosovo

Lt. Cmdr. Kristine Modlish was recently deployed to Operation Joint Guardian in Kosovo, the Balkans, as the Kosovo Forces (KFOR) Headquarters J6 Communications and Information Systems (CIS) Coordination Center Chief. In this position, she is responsible for all operational and tactical CIS systems within the KFOR area of responsibility, in addition to managing several CIS plans and projects. These systems run the gamut from Very High Frequency and Ultra High Frequency secure voice/data, secure/unsecure mobile and fixed telephone systems, secure/unsecure Local Area and Wide Area Networks, SHF satellite links, video teleconferencing and all terrestrial long haul communications.

Lt. Cmdr. Modlish's experience in working closely with the C4 professionals of other Services and with the North Atlantic Treaty Organization (NATO) and Partnership for Peace (PfP) countries gives her unique insights into ways in which the strengths of each can be leveraged for the benefit of all. Lt. Cmdr. Modlish is another example of how the IP Community is breaking new ground in areas where their skills add value to joint, allied and coalition operations.

IP Officer Provides Communications Support to the President

Lt. Cmdr. Julie La Point is assigned to the White House Communications Agency (WHCA) providing direct C4 support daily to the President and other key members of the Executive Office and First Family. IP Officers are perfect candidates for duty at WHCA where officers are challenged to "think on their feet." They must be problem solvers, negotiators and troubleshooters with expertise in a wide range of digital and analog communications and computer systems.

Assigned to the command as a Battle Captain in WHCA's state-of-the-art operations center, Lt. Cmdr. La Point leads a joint watch team that monitors and supports all Presidential and Vice Presidential communications teams as they deploy worldwide. She also travels as an Event Presidential Communications Officer. Her small team of highly qualified and motivated Soldiers, Sailors and Airmen arrive in advance of the President and set up "Presidential Quality" expeditionary communications at any location, whether it is a convention center, factory or disaster area (such as Richmond, Va., after Hurricane Isabel or San Diego, Calif., during the October 2003 fires).

The IP Community has come a long way since its inception just two short years ago. The vision of the Navy's senior leaders for a cadre of highly skilled and operationally savvy C4 experts is evident in the profiles here and the hundreds of other IP Officers at work in the fleet today. These examples are representative of the strong engagement of IP Officers at work in Navy, joint and coalition environments. The role of the IP Officer will continue to grow and mature as the needs of the Navy for technological innovation, information dominance and network-centric operations

Lt. Cmdr. Kristine Modlish inspects the KFOR VHF Command Net antenna site at Pec, Kosovo.



Lt. Cmdr. Julie La Point.

evolve. The IP Community will be on the forefront of shaping the future and enabling a true warfighting advantage.

For more information about the IP Officer Community, visit <http://www.bupers.navy.mil/pers4420/ipjobsearch.html>.

Lt. Cmdr. Danelle Barrett is an Information Professional Officer assigned to Commander, Cruiser Destroyer Group Eight.

Afloat Information Professional (IP) Officer Knowledge Management Training

As a result of the efforts of several IP Officers who attended the IP Summit 2003 held in Monterey, Calif., a pilot course was held for IP Officers going to Afloat Knowledge Management (KM) billets. This course was held in Norfolk, Va., November 19-21, 2003. Although most of the officers attending the course were en route to KM afloat billets, some were already in the job, and they provided valuable insight to what KM means to the fleet.

The two-day course covered KM theory, best practices and the tools available in the fleet today, such as KWEB and Collaboration at Sea. There were also presentations from representatives from Task Force Web, Fleet Forces Command, Commander Second Fleet, Center for Naval Analysis and the Naval Post Graduate School. A highlight of the course was a half-day ship visit for discussions with recently deployed strike group staff members.

Plans are underway to conduct the course (with modified improvements) again this spring in San Diego, and look at the possibility of adding it to the pipeline for IP Officers going to afloat billets.

Realizing FORCEnet: A Practical Example

By Lt. Cmdr. Edwin L. Armistead, USN (OPNAV 09W), Earle Kirkley (SPAWAR PMW 161), Andrew Mansfield (SSC Charleston), Dave Huff (FNMOC), Ryan Hofschneider (FNMOC) and Ben Holt (FNMOC)

For Sea Power 21, the Chief of Naval Operations (CNO) stated, "FORCEnet will provide the architecture to increase substantially combat capabilities through aligned and integrated systems, functions and missions. It will transform situational awareness, accelerate speed of decision and allow us to greatly distribute combat power. FORCEnet will harness information for knowledge-based combat operations and increase force survivability. It will also provide real-time enhanced collaborative planning among joint and coalition partners."¹ In July 2003, the CNO reiterated the importance of FORCEnet when he stated, "FORCEnet is the centerpiece of our roadmap to the future. Once implemented, FORCEnet will effectively give warfighters the knowledge of the battlefield to 'know first' and 'act first' — taking advantage of knowledge superiority over an adversary to prevail in battle."²

The task at hand is to fortify the warfighters with an underlying information network of superior battlespace knowledge. Both producers and consumers of data must have secure, reliable access to the required services with sufficient bandwidth to perform their required functions. The concept of this Distributed Services Architecture has been a common refrain since the publication of Joint Vision 2010 in 1996. However, the technology to accomplish this seamless transition has not been available until now. The emergence of Web Services has enabled developers to use common communication protocols and data structures to realize this new FORCEnet architecture.

In the notional example depicted in Figure 1, a diverse collection of applications and devices are shown communicating seamlessly. Through common Web-Services interfaces (e.g., SOAP, REST, XML-RPC) and operations-specific Extensible Markup Language (XML) documents and attachments, an unmanned aerial vehicle (UAV) sends its imagery payload (i.e., a possible target) and metadata through a geo-rectification mediation Web Service to the Global Information Grid (GIG). Applications requiring UAV information subscribe to its data feed and the UAV data stream is automatically transmitted to the subscriber clients who have the appropriate permissions to receive it.

Data filtering of the GIG information can be accomplished using a multi-level security Web Service leveraged by other Web Services and client applications. For example, coalition partners would be able to view a subset of the UAV imagery approved for non-U.S. forces.

Warfighters equipped with client software receiving information from the mediation service can identify targets and generate tasking based on the rapidly changing battlespace situation. These taskings are distributed throughout the FORCEnet (i.e., GIG) via the SOAP/XML Web-Services framework, possibly through the various mediation servers, to the net-enabled warfighter on the ground and in the sky. Speed-of-Command in this net-centric battlespace is such that aircraft may be tasked or re-tasked to

strike targets that were acquired by network sensors only moments before the attack.

But questions still remain about the melding of these technologies and whether they can actually deliver on promises of speed-to-capability, deployment flexibility and open standards. Recently, a partnership of development organizations including Task Force Web (TFW); Space and Naval Warfare Systems Command (PMW 161); Space and Naval Warfare Systems Center Charleston³; and Fleet Numerical Meteorology and Oceanography Center (FNMOC) demonstrated some practical examples that they have developed and implemented over the past two years. This partnership can affirm that there really is substance to the lightning bolts and network clouds in the diagrams that often accompany presentations (including this one) depicting the Web-Services concept. By leveraging widely adopted interfaces (SOAP) and a data description language (XML), these organizations have found that the performance of Web Services can far outshine the legacy stove-pipe methodologies of the past.

The Web-Services interfaces mentioned above have been largely successful because their specifications comply with open standards, such as the use of SOAP and XML as defined by the World Wide Web Consortium (www.W3.org). This is an association where everyone is welcome to participate in the development and discussion of standards. In this manner, Common Application Programming Interfaces (APIs) compliant with open specifications can be freely implemented without license fees or reverse engineering. This has led to a huge growth of their use in the popular programming languages of today. Likewise, the widespread availability of development tools that support W3C standards has contributed to the speed with which software developers are able to integrate Web Services into their applications. Instead of writing customized code to support proprietary data formats and protocols, developers can leverage a common code base that supports a common set of standards and protocols. A reduction in programming errors and increased reliability are additional benefits reaped by using a common code base. Program management also benefits because research and development dollars can be redirected to increasing capability and functional richness of existing applications.

Web-Services components are self-identifying technologies, allowing the creation of a modular, distributed architecture. Interfaces like SOAP or REST provide data "envelopes" containing XML and associated binary data attachments. A data envelope describes the nature of its contents and how it should be processed by the recipient application. Likewise, the XML (www.W3.org/TR/REC-xml) contained within the envelope describes the structure of the data payload.

Since Web Services leverage the same transport mechanisms that built the World Wide Web, the location of applications and servers in this distributed environment has become irrelevant to the

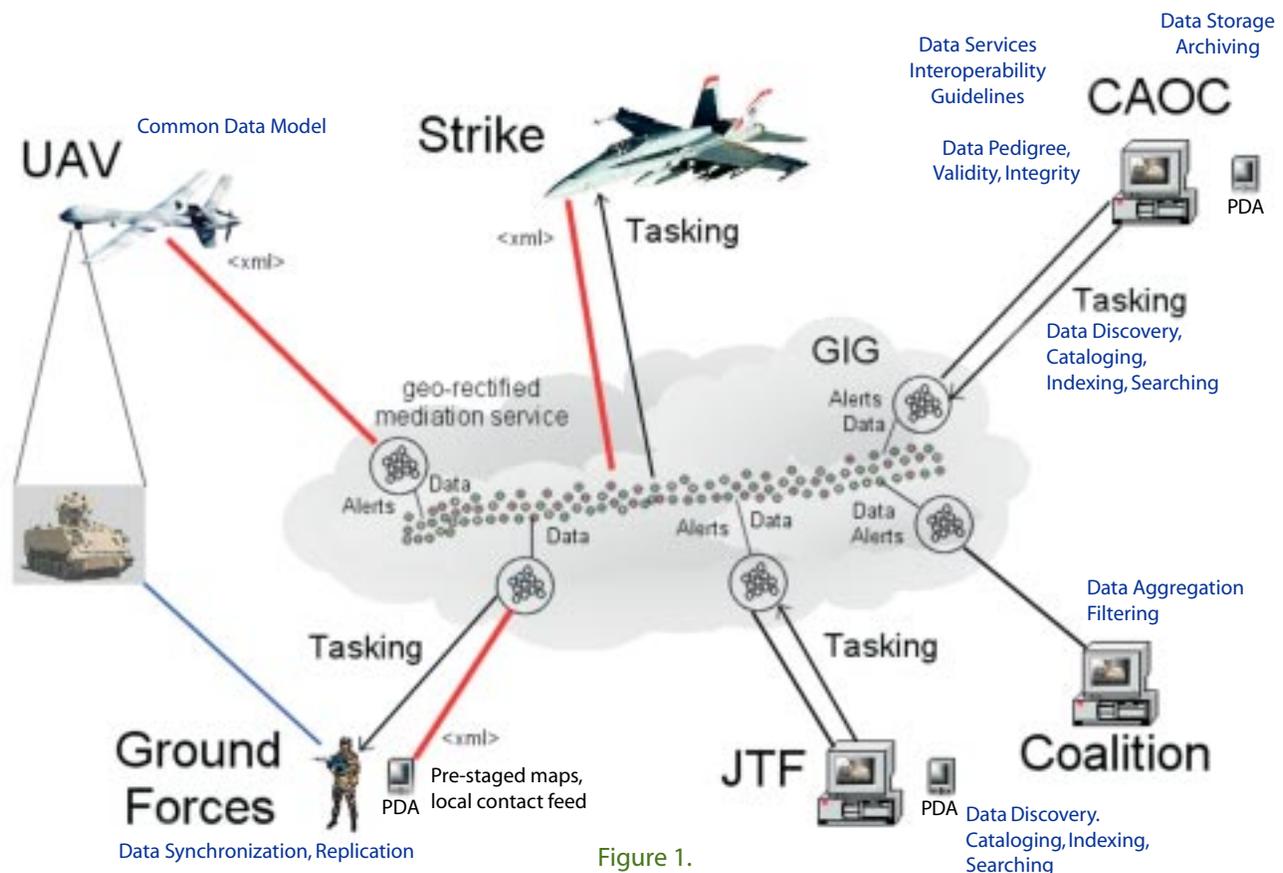


Figure 1.

warfighter. Applications and servers could be in the same room, the same building or halfway around the world. In the past, client software frequently was developed with a small initial scope only to find that a broader need would require scaling of the project. With the tools provided in the Web-Services framework, scaling is no longer a problem. Today, all client-server communication is performed using interfaces that ignore physical location, so a programmer can now change the client-server architecture without having to change the code base. This type of deployment flexibility quickly fosters reuse, as services that are written and deployed at one facility can be leveraged at another, allowing for efficient application development.

A practical example of these melded technologies in action was the recent FORCEnet Integrated Prototype Demonstration (IPD) conducted onboard the USS Essex (LHD-2) from September 25-30, 2003. TFW specific Web-enabled capabilities included:

- ◆ A suite of Navy Enterprise Portal (NEP) Single Sign On (SSO) enabled collaborative tools such as Group Chat, Instant Messaging, Whiteboarding, Discussion Boards and a File Library all based on the Collaboration-at-Sea (CAS) tools.
- ◆ A suite of Command, Control and Intelligence applications, including WebCOP, ITWeb and Intel Shop.
- ◆ A readiness tool based on Type Commander Readiness Management System (TRMS), including a Web Service built specifically to support the Expeditionary Strike Group (ESG) Commander's assets view.
- ◆ A suite of 10 Meteorology and Oceanography (METOC) tools, like Chemical Downwind Report, Ballistic Winds, MyWxmap and Web Search and Rescue, designed specially by FNMOC for FORCEnet support to the ESG.

From a TFW perspective, the Essex crew and the PHIBRON/ESG staffs successfully used all of the Web-Enabled applications during the FORCEnet IPD. One noteworthy achievement was a combination chat and whiteboard collaborative session between the USS Essex and USS Chancellorsville (CG-62) using the NEP with information extracted from the WebCOP and transmitted over the Intra-BattleGroup Wireless Network. Another highlight occurred when embarked staff of the Essex ESG trained members of the U.S. Army 25th Infantry Division based in Hawaii on WebCOP through the NEP, using collaboration tools while underway.

As shown, the particular capabilities of the NEP, and more generally Web Services, have great potential to enhance situational awareness and information sharing. The practical example of the FORCEnet IPD allowed TFW and FNMOC to demonstrate to a large warfighter group the inherent capabilities of these new technologies.

In conclusion, the effectiveness of Web Services, especially in the maritime environment of the Navy, is readily apparent. The ability to provide access to the applications from any enclave, anywhere in the world is truly extraordinary. This new capability is rapidly changing the way the Navy operates in the information battlespace, and lays the foundation for a successful transition to the FORCEnet envisioned by the CNO.

1. Clark, Vern. *Proceedings, "Sea Power 21: Projecting Decisive Joint Capabilities."* October 2002.
2. Donaldson, John. *Navy NewsStand, "NETWARCOM Celebrates First Year In Operation - Hosts CNO Visit."* July 2003. Story Number: NNS030717-16. (http://www.news.navy.mil/search/display.asp?story_id=8529)
3. *Demonstrated during exercise Quantum Leap-1 under the OSD Horizontal Fusion portfolio* (<http://www.defenselink.mil/releases/2003/nr20030828-0413.html>)

Therminator

A transformational enabler for FORCEnet

By John McEachen, John Zachary and David Ford

“Slammer, Blaster, Code Red”—the simple fact that the general public associates these terms with computer network attacks speaks volumes for how far awareness of network security has advanced in the past few years. Unfortunately, the same cannot be said for the technology designed for repelling these attacks. Change has been incremental and, for the most part, we are still conducting business the way we were 20 years ago. Consequently, while the sophistication and virulence of network attacks have increased exponentially, the ability to stop these attacks has advanced only linearly.

For example, in 2001 Code Red infected over 300,000 network hosts in half a day. In 2003, it took under 30 minutes for the Slammer worm to infect over 75,000 hosts, 90 percent of which were infected in under 10 minutes. This escalating rate of propagation highlights the requirement for network detection mechanisms to serve as real-time early warning devices. Clearly, there is a critical need for transformational change in the way the Department of Defense (DoD) performs computer network defense (CND).

Therminator is a new and radical approach to CND on an immediate basis and to systems of exchange on a more abstract level. Consequently, Therminator is well-suited as a transformational enabler for

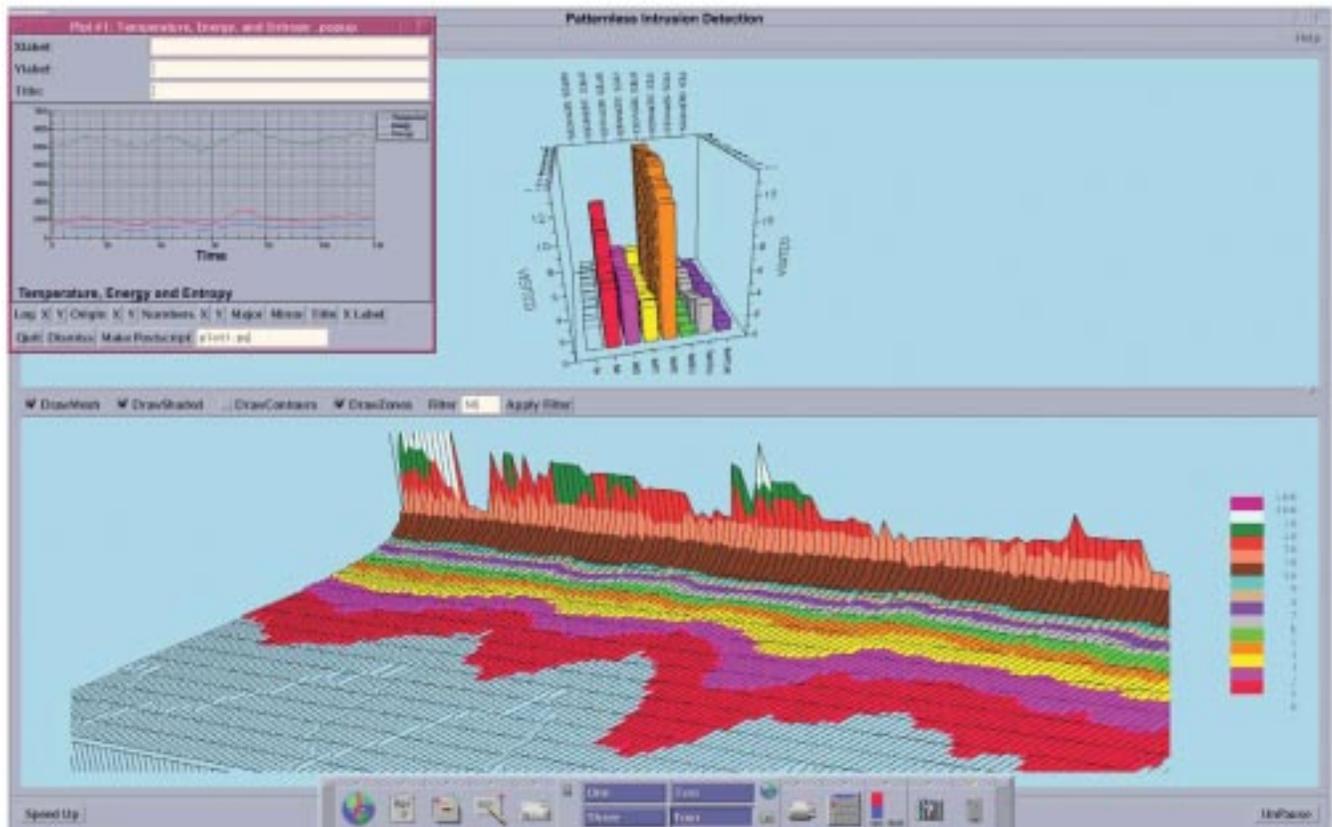
the network-centric vision of FORCEnet. While the specific application of Therminator has been most recently applied to IP networks, the concepts and techniques can be applied to all manner of networks and communications systems.

Therminator is based on proven science from combinatorics, statistics and thermodynamics. The system can be considered a new layer in the “Defense in Depth” approach to network security and provides network administrators with a novel perspective (Figure 1) on how their network is operating. Therminator is highly scalable and its composite approach can even facilitate creation of “Therminators of Therminators.” It has been tested at the U.S. Pacific Command Network Operations Center, Ft. Shafter, Hawaii, U.S. Pacific Command Headquarters, Camp H.M. Smith, Hawaii and the U. S. Army Signal Command, Ft. Huachuca, Ariz. Follow-on installations are being planned.

Background

The development of a dependable and secure networked computing infrastructure depends on real-time monitoring and detection of anomalous events. These events and behaviors typically are sourced at a host and are propagated over a network to a victim

Figure 1. A generic snapshot of the primary Therminator display. The top portion of the graph is a display of average bucket sizes associated with conversation groups. The lower portion of the graph illustrates the “thermal canyon” — the relationship of various network states over time (indicated from left to right).



host or network. The typical approach is to apply intrusion detection principles to a network to capture and classify malicious behavior. The earliest intrusion detection systems (IDS) integrated signature-based analysis for detection with normal network models. Since then, many different systems have been based on the assumption that malicious network activity is inherently different from normal activity. Recent experience, however, suggests that the scope and character of network attacks is such that intrusion detection systems are insufficient network protection mechanisms. This is especially true of signature-based IDS, which compare real events to a set of known malicious or abnormal events. These types of systems are poor at detecting new attacks, variations of known attacks or attacks that can be masked as normal network behavior. The complex, interactive nature of computer networks is subject to the critical mass effect. The spread of worm-like attack is much like the effect observed with a paper napkin when increasing force is applied. The progress of the tear is hardly noticeable at first until, quite suddenly, the napkin is ripped in two. The physical nature of complex, interactive systems such as computer networks highlights the need for rapid, real-time indication of attack propagation.

Thus, there is a real need for a new approach in thinking about CND. Therminator emphasizes active real-time network monitoring and anomaly detection as complementary mechanisms to the traditional network intrusion detection process. The separation of network traffic behavior into normal, anomalous and malicious categories under the umbrella of real-time monitoring and configuration management gives operators a holistic view of network activity.

Motivated by the need for CND transformation, the real-time implementation of Therminator was developed in 2001 at the Fort Shafter NOC by two students of the Naval Postgraduate School, Lt. Stephen Donald, USN, and Capt. Robert McMillen, USMC. Using live operational network traffic and working in tandem with scientists from the National Security Agency, the Institute for Defense Analysis and the SANS (SysAdmin, Audit, Network, Security) Institute, the team produced a working application in 90 days. Testing and analysis have continued over the past two years and in March 2003, software development was picked up by the University of South Carolina Distributed Systems Security and Cryptography Laboratory.

Most recently, Lancope, Inc. of Atlanta, Georgia, released a version of its Stealthwatch Intrusion Detection System that integrates many

of the Therminator concepts. This product, called Stealthwatch + Therminator (SW+T or SWAT), combines the information-dense yield of Stealthwatch with the data reduction features of Therminator to produce a system that provides both macro- and micro-views of an IP network. The ideas behind SW+T are based on a non-exclusive license purchased by Lancope from DoD in November 2002.

Commercial ventures notwithstanding, research in Therminator applications aligned with specific national security interests continues at the Naval Postgraduate School, the University of South Carolina and the Georgia Institute of Technology. Areas of investigation include implementation of Therminator in hardware to operate at gigabit speeds, and analysis of Therminator concepts in nontraditional networks.

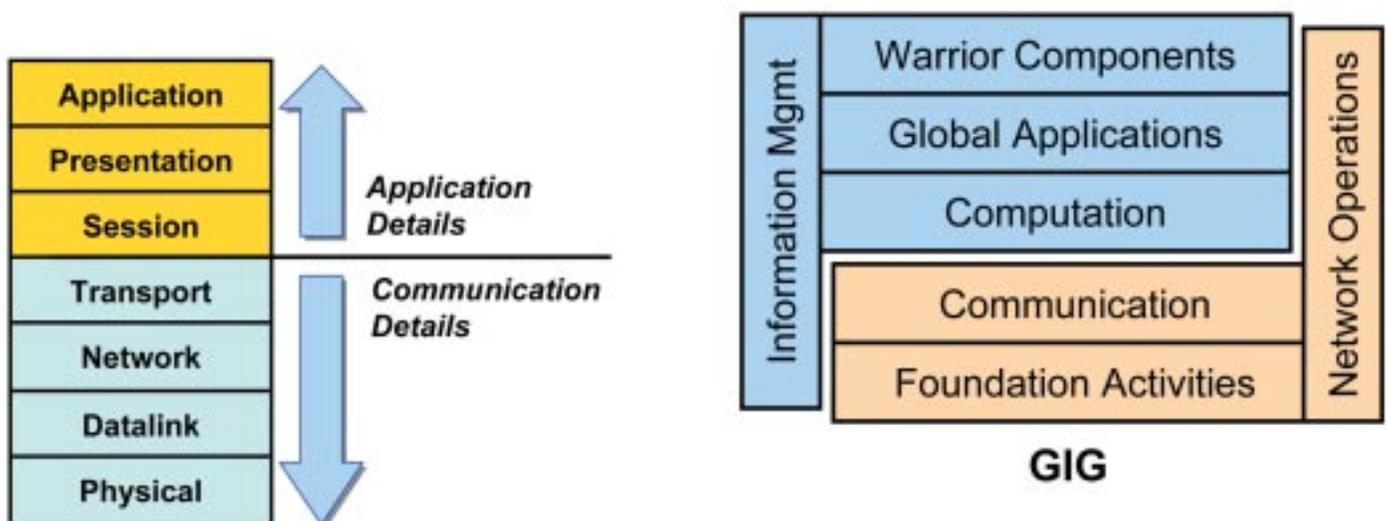
Concept

A computer network is a complex interactive system. The signal it produces is the result of many millions of precise, directed exchanges between thousands of its component parts. To maintain information superiority, survivability (reliability, usability and security) and mission support, it is essential that the state of readiness in this complex machine be timely and understandable to decision makers at several levels in the chain of command. In addition, it is crucial that this trusted state of readiness be defended from those that continually act to undermine both its readiness and integrity. This means that the long and short term actions of those who seek to control our critical infrastructure be transparent to those entrusted with the task of defending and repairing it.

For many researchers the complexity of this problem is an obstacle. The Therminator research initiative uses the complexity of this problem as an advantage. By extending the work and lessons learned by many generations of scientists, Therminator uses the well-founded theories of statistical mechanics and combinatorics as a template and a strategy for dynamic data reduction, visualization, analysis, interpretation and forensics. Thus, it does not rest on the ad hoc opinion of a single researcher or single group of researchers on what seems like a good strategy, it avoids reinventing the wheel by building on well-established scientific and mathematical principles.

Therminator provides a continuous real-time, compact and visual representation of states of exchange between network entities. The basic premise results from modeling the network as a finite number

Figure 2. The division of labor in the Therminator model. Therminator provides a general mapping of the characteristics of communications exchanges, providing a generic metric for warfighters to compare anomalies across applications.



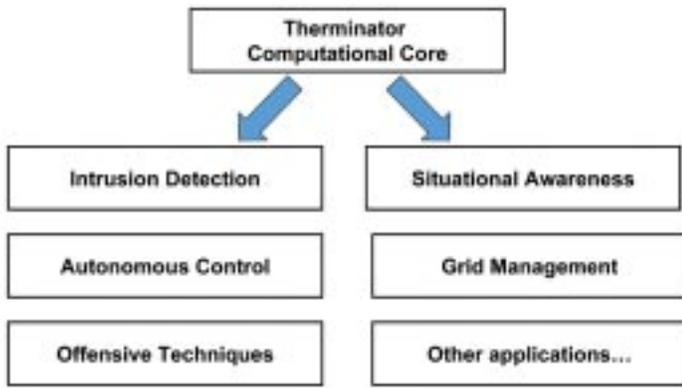


Figure 3. Therminator's approach can be applied across a broad spectrum of FORCEnet applications.

of conversation groups called buckets that pass information, called balls, among themselves. This produces a notion of a network state represented by the aggregate of all the buckets with the balls they contain. The complexity and asynchrony of this exchange among a large set of network nodes creates a high-dimensional combinatorial system to which dimensionality reduction inspired by statistical physics is applied. From this network state and the state transitions that occur during each packet arrival, the thermal properties of entropy, energy, temperature, work and heat can be computed and displayed. Asymmetrical perturbations in these displays have revealed anomalous network activity resulting from malicious activity and misconfigurations, some of which were not detected by standard signature-based intrusion detection systems.

Application to FORCEnet

Computer networks and interacting systems in general, are based on a layered architecture to facilitate systems interoperability and design. The layered design paradigm permeates many modern distributed systems affecting solutions to the association problem.

The inherent elegance in the Therminator approach and the aspect that makes it applicable to FORCEnet, is that it yields a model of conversation exchange dynamics that is consistent across horizontal levels (different applications) and across vertical levels (different architecture layers, shown Figure 2). A consistent model across vertical levels will allow technicians, analysts and decision makers to compare apples to apples because all behavior is cast in the same general model (conversation exchange dynamics). This will reduce the time from data collection to information creation to knowledge understanding and finally decision making.

In other words, using the Therminator approach, anomalous activity in one environment (e.g., satellite control systems) could be reliably correlated with activity in a very different setting (e.g., IP networks). This is made possible because both are considered only in terms of their exchange properties and related dynamics. A subset of these potential applications is shown in Figure 3.

The Therminator architecture as shown in Figure 4 is based on an application-independent central core processing element that is fed by application-dependent sensors. In the case of IP networks these sensors are packet sniffers which perform rudimentary metadata association. External to the core are the graphical user interface (GUI) modules and plug-ins for second-order analysis of the core output.

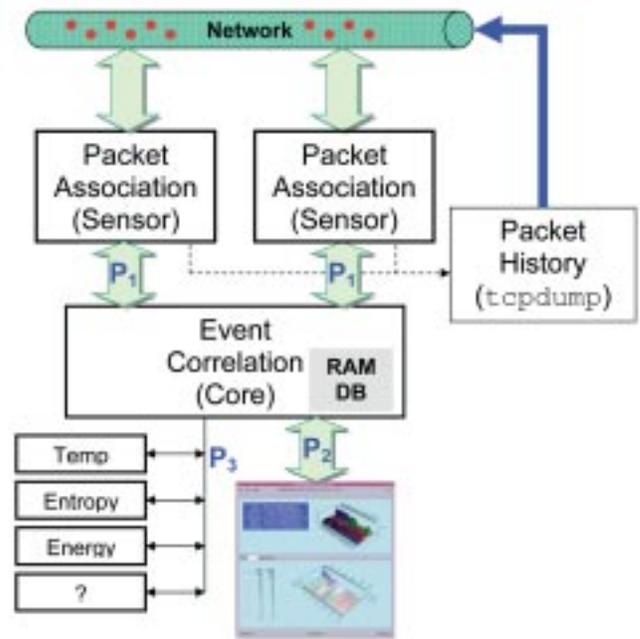


Figure 4. The Therminator architecture is centered upon a core event correlator. Input is received from application-dependent sensors and output is fed to a GUI and second-order plug-ins.

Examples

Therminator has been extensively tested in both controlled laboratory settings and on real-world network traffic. The current software-based implementation handles generated network traffic from 10 Mbps to 100 Mbps without dropping packets. A visualization of the bucket spaces and thermal manifolds provide interactive real-time feedback of the conversations exchange dynamics. Users are able to drill-down to specific packet information simply by clicking anywhere in the GUI.

Figure 5 illustrates the thermal manifold or "thermal canyon" produced from an exchange between 1,000 client machines on an untrusted network with 10 Web servers on a trusted network. Network load was approximately 1,500 packets per second. Figure 6 illustrates the same exchange of traffic with a single UDP (User Datagram Protocol) packet injected. The difference in the thermal canyon between Figures 5 and 6 is evident, keeping in mind that during this two-minute period over 200,000 packets were exchanged.

Figure 7 shows the Therminator response to an actual event on an operational network: a flood of ICMP (Internet Control Message Protocol) packets originating inside a monitored network detected after normal working hours. The packet flood consisted of 6,032 ICMP echo requests/replies within a four-second time period. ICMP echo requests/replies are not anomalous per se. In this event, however, the owner of this particular client machine was logged off and at home, thus prompting a notification to the local CERT (Computer Emergency Response Team) for follow-up. This event was not detected by any other installed network protection system.

The final example of an operational success of this model occurred when Therminator detected a Code Red worm attack during a demonstration. The case study shown is an interesting example of the range of anomalies that Therminator is capable of revealing. Figure 8 shows a small number of packets entering the NPS network that correspond to the Code Red worm. This is in contrast to the result of the swift counteraction of the firewall administrator shutting

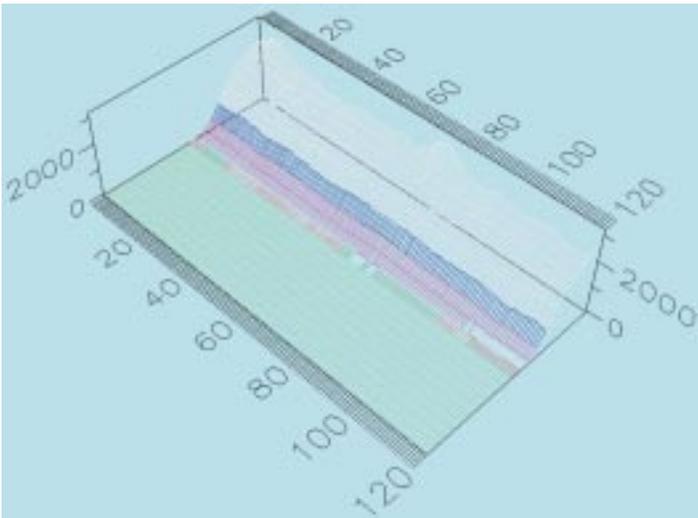


Figure 5. The display associated with synthetic network traffic from 1,000 untrusted clients to 10 trusted Web servers over a period of two minutes. This figure represents over 200,000 packets.

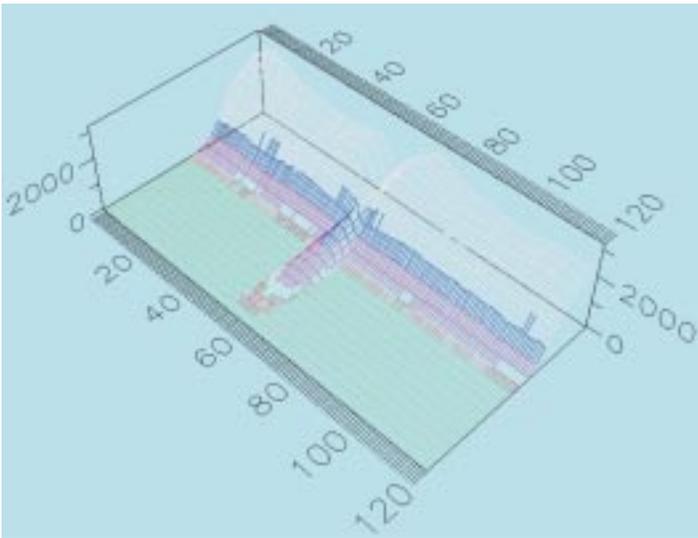


Figure 6. The same 200,000 packets shown in Figure 5 plus a single additional UDP packet. The difference is evident at approximately 60 seconds.

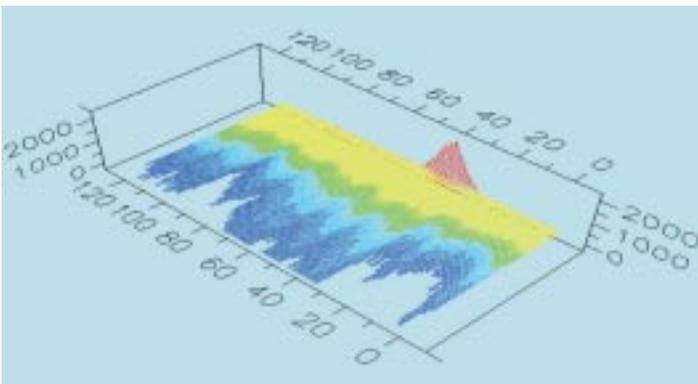


Figure 7. A snapshot of an actual packet flood observed within an operational network. This flood consisted of over 6,000 packets in a four-second period from a single host during off-hours.

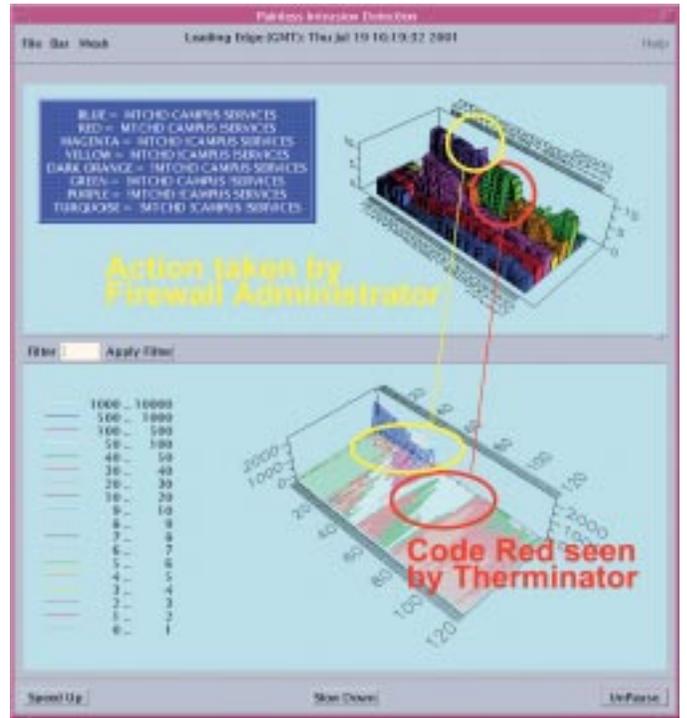


Figure 8. A snapshot of the Code Red attack in progress. The display highlighted by the red circles is associated with the Code Red worm entering the NPS campus. The area highlighted by the yellow circles is associated with the firewall administrator shutting down the firewall in response to notification of the arrival of the worm. Compare the display associated with the intrusion of the Code Red worm with that of the actions taken by the firewall administrator shortly thereafter.

down the firewall highlighted by the yellow circles. This area shows thousands of Web requests heading to the Internet while all the responses are blocked.

Summary

Therminator is a radical attempt at transformation in DoD CND and in FORCENet monitoring in general. Traditional approaches to CND cannot keep up with the rapid changes in network intrusions. By reducing data to an expression of exchange dynamics, Therminator can provide a metric for an apples to apples comparison across communications applications thus allowing for informed and rapid decision making.

John McEachen is an Associate Professor of Electrical and Computer Engineering at the Naval Postgraduate School. Dr. McEachen is the co-director of the ECE Advanced Networking Laboratory and the former director of Reconfigurable Intrusion Detection and Deception Laboratory Research (RIDDLR). In 2003, he was awarded the Richard W. Hamming Award for excellence in interdisciplinary teaching and research.

John Zachary is an Assistant Professor of Computer Science at the University of South Carolina and Director of the Distributed Systems Security and Cryptography Laboratory. Dr. Zachary was formerly employed by the Advanced Research Laboratory of Penn State University.

David Ford is a Research Professor at the Naval Postgraduate School and the DISA chair for Information Assurance. He is formerly of the National Security Agency. □

The Federal Information Security Management Act of 2002

By James E. Collins

What is FISMA?

The Federal Information Security Management Act of 2002 (FISMA) is contained within the E-Government Act of 2002 (Public Law 107-347), replacing the Government Information Security Reform Act (GISRA). FISMA, effective throughout the federal government, places requirements on government agencies and components, with the goal of improving the security of federal information and information systems.

What is the purpose of FISMA?

The purpose of FISMA is as follows:

- ✓ Provide a framework for enhancing the effectiveness of information security in the federal government. This means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction to ensure integrity, confidentiality and availability.
- ✓ Provide effective government-wide management of risks to information security.
- ✓ Provide for the development and maintenance of minimum controls required for protecting federal information and information systems.
- ✓ Provide a mechanism for effective oversight of federal agency information security programs.

What does FISMA require?

FISMA requires the head of each federal agency to provide information security protections commensurate with the risk and magnitude of the harm that may result from unauthorized access, use, disclosure, disruption, modification or destruction of its information and information systems. The protection should apply not only within the agency, but also within contractor or other organizations working on behalf of the agency.

FISMA requires that the agency head delegate to the agency Chief Information Officer (CIO) the authority to ensure compliance with the legislation. Further, the CIO must designate a senior agency information security officer whose primary duty is to carry out the CIO's responsibilities for information security. This information security officer must possess commensurate professional qualifications, training and experience, and head an office with sufficient resources to carry out information security responsibilities. In the case of the Department of the Navy (DON), "agency head" refers to both the Secretary of Defense and the Secretary of the Navy. Within the Department of the Navy, Dave Wennergren, DON CIO, designated Rob Carey, Deputy CIO for Policy and Integration, as the senior DON information security officer.

The FISMA law requires that the CIO carry out the following responsibilities:

- Develop and maintain an agency-wide information assurance (IA) program complete with policies, procedures and control techniques to address information security requirements, including FISMA.
- Ensure that required training is conducted including annual information security training and Internet security training.
- Ensure oversight of personnel with significant responsibilities for information security.
- Assist senior agency officials concerning their awareness and responsibilities for information and information system security.

The law also requires the agency head, in this case the Secretary of the Navy, to:

- Ensure the agency has a sufficient number of trained personnel to ensure agency-wide IA.
- Require annual reports from the CIO regarding the effectiveness of agency IA programs and progress on any required remedial actions.

Specifically, FISMA requires each federal agency to develop, document and implement an agency-wide information security program, which includes the following:

- Periodic risk assessments.
- Risk assessment policies and procedures that cost-effectively reduce the risk to an acceptable level, ensure that information security is addressed throughout the life cycle of each agency information system and ensure compliance with FISMA.
- Subordinate plans for networks, facilities and groups of systems as appropriate.
- Security awareness training for agency personnel, including contractors and system users.
- Periodic (at least annual) testing and evaluation of the effectiveness of information security policies, procedures and practices.
- Processes for planning, implementing, evaluating and documenting remedial action to address deficiencies in agency information security policies, procedures and practices.
- Procedures for detecting, reporting and responding to security incidents.
- Plans and procedures to ensure continuity of operations for information systems that support agency operations and assets.

FISMA requires each federal agency to report to Congress annually by the first of March. The report must address the adequacy and effectiveness of information security policies, procedures and practices. In addition to the annual report, FISMA requires each agency to conduct an annual independent evaluation of the IA program and practices to determine their effectiveness.

The FISMA legislation assigns to the Department of Defense (DoD) the authority to develop and oversee the implementation of IA policies, principles, standards and guidelines. The legislation also requires DoD components to identify and provide information security protective measures commensurate with the risk and magnitude of the harm possibly resulting from unauthorized acts.

What is the impact of FISMA on the DON?

Many of the aspects of FISMA are already in place, such as IA training, incident reporting and testing. DON CIO is preparing policies and plans to carry out the law's requirements, including the basic Secretary of the Navy policy on information assurance, Secretary of the Navy Instruction (SECNAVINST) 5239.3.

The DON CIO has submitted the required annual reports for three years, first for GISRA and this year for FISMA. In practice, DON CIO coordinates with the Navy and the Marine Corps and submits an annual DON FISMA input to DoD. DoD then submits a composite Defense-wide report to the Office of Management and Budget (OMB), which in turn submits the report to Congress as required by the legislation. The relevant Inspectors General and audit services conduct the required annual evaluations, which include site visits, testing and assessments.

FISMA, effective throughout the federal government, places requirements on government agencies and components, with the goal of improving the security of federal information and information systems.

In summary, the overarching goal of the Department of the Navy is to secure the Department's information assets, balancing the need for security with the primary objective of meeting operational requirements. By doing that, we are well along the way to compliance with FISMA.

Mr. Collins is a retired Navy captain providing support to the DON CIO IA Team.

The DON eGov Awards Fall 2003

The Department of the Navy Chief Information Officer (DON CIO) is pleased to announce the winners of the Fall 2003 DON eGov Awards. These awards honor project teams that have successfully reengineered/transformed key DON business and warfighting processes to reduce costs, improve mission performance, and support the effective exchange and sharing of information.

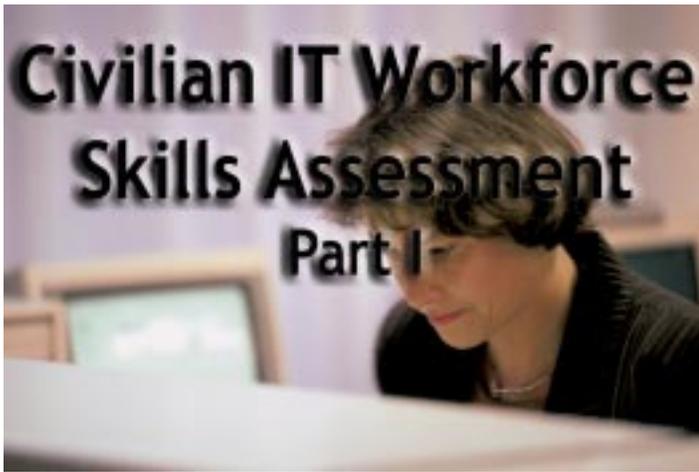
The following teams are honored for their successful initiatives, which are leading the way toward the eGovernment transformation of the DON:

- ◆ Marine Corps Systems Command, HQMC, Manpower & Reserve Affairs & DFAS - Technical Services Organization for Total Force Administration System (TFAS)
- ◆ Commander, Naval Reserve Force, DFAS - Technical Services Organization & SPAWAR Information Technology Center for Naval Reserve Order Writing System (NROWS)
- ◆ NAVAIR Aircraft Wiring Support Equipment Commodity & eBusiness Operations Office for Just-in-Time Wiring Information System (JITWIS) eSuite
- ◆ ASRLW NAVAIR Team & eBusiness Operations Office for Aircraft Shot and Recovery Log - Web (ASRLW)
- ◆ ePMS NAVSEA Team & eBusiness Operations Office for Electronic Planned Maintenance System (ePMS)
- ◆ USS Dwight D. Eisenhower & eBusiness Operations Office for Refueling and Complex Overhaul Integrated Maintenance Package
- ◆ Task Force Web for Building the Web Enabled Navy (WEN)
- ◆ NETC Business Office for NETC Military Awards Processing System (NMAPS)

The eGov awards were presented at the Fall 2003 Naval IT Summit held in Arlington, VA. This first DON IT Summit brought together the DON CIO, DON Deputy CIO (Marine Corps), DON Deputy CIO (Navy) and command information officers from Echelon II and major Marine Corps subordinate commands in a forum to build the Navy-Marine Corps team and advance our strategy for continual transformation.

Look for more information about the IT Summit and the eGov Awards in the next issue of CHIPS.





By Sandra J. Smith

Assessing the IT Civilian Workforce of Today

The first ever federal-wide information technology (IT) workforce skills assessment survey was conducted during September 2003. Sponsored by the Federal Chief Information Officers (CIO) Council, the Office of Management and Budget (OMB) and the Office of Personnel Management (OPM), the Web-based survey was designed to collect information from federal IT employees regarding their current proficiency in a variety of competencies and skills, certifications held, time spent on a variety of specialized job activities and demographic information essential for workforce planning.

Drivers for IT Workforce Planning

The survey fulfills certain legal requirements for workforce assessment and analysis and will assist in the development of Human Capital Plans. It satisfies the E-Government Act (Section 209) requirement to analyze the personnel needs of the federal government relating to information technology and information resources management, and the annual requirement of the Clinger-Cohen Act (CCA) to assess the skills of the federal government IT workforce.

Defining the IT Workforce

The survey was completely anonymous and voluntary, and targeted civilian employees in IT and IT-related positions. Although they are an integral part of the IT workforce, military members and contractor personnel were not surveyed. Civilian occupational series were used to identify the appropriate survey audience including the following traditional and nontraditional IT series:

- GS-0332 Computer Operation
- GS-0334 Computer Specialist
- GS-0335 Computer Clerk & Assistant
- GS-0390 General Telecommunications
- GS-0391 Telecommunications
- GS-0392 Telecommunications Processing
- GS-0854 Computer Engineer
- GS-1550 Computer Scientist
- GS-2210 Information Technology Management

Survey Statistics

The survey took approximately 10 to 20 minutes to complete. The

DON had a 20 percent response rate based on 6,533 respondents. While the survey was self-selecting (not a random sample), the follow-on analysis is statistically valid with a small margin of error and a high confidence level. The 1,333 DON respondents were well-distributed across all major claimants and commands.

Now that the survey data has been collected, the DON Information Management/Information Technology (IM/IT) Workforce Management Team will review and analyze the data as the first step of the DON CIO's workforce analysis approach. This includes identification of potential skill and competency gaps based on forecasted IM/IT workforce requirements. When this is complete, an enterprise IT workforce strategic human capital plan, in line with the President's Management Agenda, will be developed as a guide to fill identified gaps. More information on the workforce planning guide will be forthcoming from the Federal CIO Council and DON CIO.

Survey Demographics

Survey demographics included questions relating to grade, age, retirement, years of government service, years of IT industry experience and other factors. What emerged based on the responses was a profile of the "average IT worker" in the DON, which is shown in Figure 1.

Profile of the DON Average IT Worker
...is between 46 and 50 years of age
...is a GS-12
...has over 20 years of federal government experience
...has little to no private sector experience
...is likely to retire in the next 10 to 20 years
...is fairly mobile (may leave the organization in the next 3 years)
...holds a Bachelor's Degree

Figure 1.

The profile of the average DON IT worker matches the overall federal profile with the exception that federal IT workers are generally GS-13s, and have slightly more graduate degrees but fewer doctorate degrees. Most respondents have a significant amount of federal government service, they are relatively mobile and have little private sector IT experience. Most respondents plan to retire when they are eligible. Approximately 30 percent of respondents indicated that they are eligible to retire within six years; 80 percent are eligible to retire in 20 years.

Initial Top Level Assessment

The survey asked respondents to assess their current proficiency in a set of general (16 total) and technical (53 total) competencies. The competency self-assessment used a five-point scale based on the competencies that make up the GS-2210 occupational series, since they can be mapped back to other job functions and series (e.g., CIO competencies, GS-391s, GS-1550s). Figures 2 and 3 order the highest-rated technical and general competencies based on the number and percentage of respondents who said they were at the "5-Expert" proficiency level. The percentage is based on the total number of DON responses (1,333).

The survey also asked respondents to indicate their IT-related certification areas and estimate the amount of time they spend

Top 10 Technical Competencies (n=1,333)		
Technical Competencies	Responses	%
Configuration Management	205	15.38%
Software Development	201	15.08%
Hardware	196	14.70%
Computer Languages	184	13.80%
Project Management	168	12.60%
Requirements Analysis	154	11.55%
Operating Systems	146	10.95%
Software Engineering	146	10.95%
Systems Life Cycle	142	10.65%
Software Testing and Evaluation	131	9.83%

Figure 2.

Top 10 Certifications Areas			
Certifications Areas	Certified	%	Rank
IT-Related Technical Certificates from accredited Technical Schools (military or commercial)	154	11.55%	1
Microsoft	132	9.90%	2
Comp TIA	50	3.75%	3
Cisco	41	3.08%	4
Information Systems Security	38	2.85%	5
Project Management	38	2.85%	6
Novell	33	2.48%	7
Business Applications	31	2.33%	8
Oracle	29	2.18%	9
Network Support	27	2.03%	10

Figure 4.

Top 10 General Competencies (n=1,333)		
General Competencies	Responses	%
Interpersonal Skills	373	27.98%
Problem Solving	340	25.51%
Customer Service	328	24.61%
Decision Making	251	18.83%
Oral Communication	232	17.40%
Leadership	228	17.10%
Planning and Evaluation	222	16.65%
Organizational Awareness	186	13.95%
Influencing/Negotiating	155	11.63%
Managing Human Resources	145	10.88%

Figure 3.

Top 10 Job Activities		
Activity Name	Responses	%
IT Project Management	292	21.91%
IT Security Information Assurance	194	14.55%
IT Workforce Management Development	172	12.90%
Knowledge Management	116	8.70%
Solutions Architecture	111	8.33%
Records Management	94	7.05%
Privacy	71	5.33%
Enterprise Architecture	70	5.25%
Capital Planning and Investment	50	3.75%
eGovernment	24	1.80%

Figure 5.

(extensive, moderate, minimal or none) on 10 different “specialized job activities.” Figure 4 shows the top certification areas. Figure 5 shows the top activities where employees spend an extensive amount of time.

The Analysis Phase

As noted, the survey collected the respondents’ estimates and/or self-assessment of the amount of time spent on specialized job activities, proficiency in general and technical competencies, proficiency in IT-related skills and certifications held. The analysis of the survey data is a necessary step of workforce assessment that precedes workforce planning. When the data are paired with other indicators such as the Federal Information Security Management Act (FISMA) or the Capital Asset Plan and Business Case (Exhibit 300s), a more comprehensive view of the actual “bench strength” of the workforce is provided. By correlating competencies, skills and certifications to the amount of time individuals spend on specialized job activities, we can make inferences about adequate skills and competencies or the gaps in specific areas.

Sandra J. Smith is the DON CIO IM/IT Workforce Management Team Leader.

Stay tuned...the results of the analysis will be provided as Part II of this article in the next edition of CHIPS.



Editor's Note: Go to page 22 for an article about the Federal Information Security Management Act (FISMA).

First U.S. Navy Installation of DMS Afloat

By SPAWAR PMW 162-2, Tactical Organizational Messaging for Program Executive Office C4I and Space

In a huge step toward implementing a common messaging solution for warfighters afloat and ashore, the Naval Modular Automated Communication Systems (NAVMACS II)/Single Messaging Solution (SMS) Phase II was installed on the USS Belleau Wood (LHA-3) and underwent initial fleet evaluation during October 2003 sea trials. Installation of this tactical command and control system also marks a big step toward realizing the Chief of Naval Operations FORCENet vision of full interoperability between the Navy and Marine Corps — and the rest of the Department of Defense (DoD).

At the same time, it brings Navy one step closer to the DoD vision of a Global Information Grid that links the Navy to U.S. government agencies such as the Department of Homeland Security, the Defense Logistics Agency, the National Imaging and Mapping Agency and the National Security Agency.

SMS II, also called “DMS Afloat,” brings with it the first implementation of the Defense Message System (DMS) in an afloat tactical environment. DMS provides the battle planners on a Combined Joint Task Force (CJTF) staff with a flexible, COTS-based, network-centric, application layer system that bridges communication networks and also provides interoperability with other U.S. and allied forces. Trials with this state-of-the-art advance in communication on an operational Navy ship will provide essential metrics toward increasing communication performance for end-to-end, secure and interoperable organizational messaging.

Capable of delivering data messages with the future enhancements of voice and video attachments, DMS Afloat provides better-protected, faster communications at a measured lower Internet Protocol (IP) overhead than comparable SMTP e-mail. It also provides the capability to interlink existing legacy systems and future DMS architectures. The goal of DMS Afloat is to provide a single point of receipt and transmission for all organizational message traffic. Existing communications architecture reflects legacy, serial protocol tactical communication message processing system technologies (hardware and software) that are, in some cases, over 30 years old. These legacy systems are candidates for planned phase-out, upgrade or replacement using an evolutionary acquisition process as we gradually migrate towards DMS.

“The USS Belleau Wood has a distinguished history of service to the nation and now has the distinction of being the inaugural DMS Afloat ship. I applaud the Navy’s success in this initial shipboard implementation, which expands the messaging envelop to the Navy tactical environment. DMS is now the



Above: IT2(SW) Dawn L. Lee, USN and IT3 Daniel W. Schneider, USN, operating the NAVMACS II/SMS Phase II system onboard the USS Belleau Wood (LHA-3) in October 2003.

system of record for official Department of Defense message communications. This event signifies the Navy’s commitment to transforming their C2 messaging capability throughout the fleet,” said Mr. Verlin Hardin, Defense Information Systems Agency, Defense Message System Program Manager, Washington, D.C.

“DMS Afloat delivers on the fleet requirement for a common, robust, high assurance, organizational messaging solution that supports Navy warfighters and embarked forces from all Services. It is an enabler that allows the Navy to plug into DoD’s emerging Global Information Grid while providing a state-of-the-art, IP-based organizational messaging capability to the fleet,” said Captain Bill Bry, USN, PEO (C4I-Space) PMW 166, Organizational Messaging Program Manager, San Diego, Calif.

As a military communications processor, SMS provides message services to afloat tactical warfighters along with command, control and communication functionalities. It provides a universal messaging process, open-architecture environment and state-of-the-art technology that reduces operator training, technical support, maintenance and overall life cycle system costs.

SMS provides capabilities via high-speed global messaging utilizing IP networks to connect the afloat tactical user with ship-to-shore and inter/intra (ship-to-ship) battle group operational messaging. SMS also supports the existing legacy circuits that are being phased out as all military message traffic transitions to the single transport layer known as the Defense Information System Network (DISN). During this transition period, SMS Phases I and II will connect the various types of organizational message traffic via legacy channels and emerging IP messaging technologies, while migrating to DMS.

The SMS program was structured as an evolutionary acquisition process with phased development that has a scalable system design. As such, the main configuration differences between SMS and the different variants are in the number of extra workstations provided and other specific DMS architecture

components. SMS brings to Navy's afloat tactical environment a high-level, high assurance messaging capability while adapting to Joint and Allied/Coalition Interoperability requirements. The system features for the NAVMACS versions up through SMS Phase II are summarized as follows:

- ◆ NAVMACS (V) is UYK 20, 1970s based H/W and S/W with little memory and little capability. NAVMACS II, the replacement for NAVMACS (V), uses Commercial-Off-the-Shelf (COTS) hardware with Government-off-the-Shelf (GOTS) software that adapts functionality into the Graphical User Interface (GUI) environment.

- ◆ NAVMACS II/SMS Phase I, replacement for NAVMACS (V) and DMS ready, has six variants scalable for all platforms, an upgraded legacy functionality in a Pentium-based system and includes system rack upgrades to allow for DMS insertion. This system's scalable hardware allows for DMS hardware and software upgrades and functionality in the coming years.

- ◆ NAVMACS II/SMS Phase II (DMS) provides DMS to Navy and Coast Guard afloat units and has multiple variants (CJTF, Shooter, Non-Shooter and non-deployer). This configuration brings DMS components into the SMS Phase I infrastructure with no modifications to the system electrical interconnections or footprint.

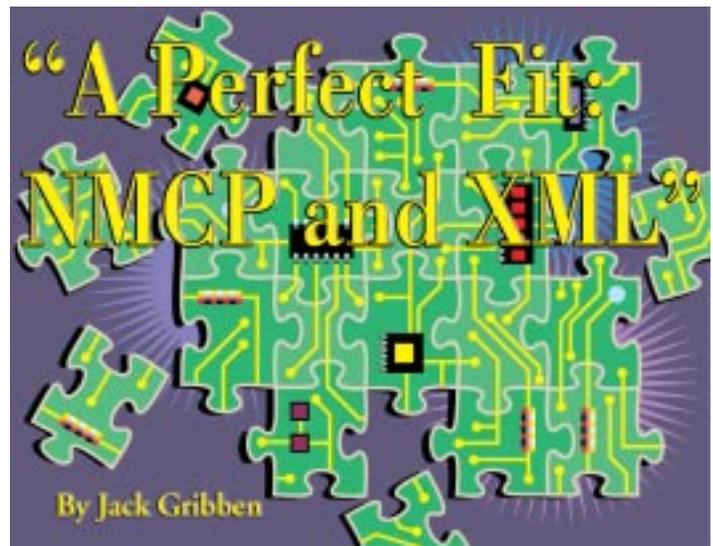
SMS hosts various software applications, such as Microsoft Outlook and Exchange, the Information Screening and Delivery Subsystem (ISDS) used in submarine configurations, TURBOPREP and the Defense Message Dissemination System (DMDS), to ensure maximum space utilization and Pentium processing capability.

NAVMACS II/SMS Phase II will provide a means for transitioning legacy communication systems into more capable, speedier, better integrated and fully joint interoperable capabilities to U.S. Navy ships and their embarked warfighting components.

Additionally, SMS provides a variety of messaging services, security, interoperability, directory services and message access controls, all in an automated, user-friendly package requiring minimal watchstander involvement. It is capable of processing between 8,000 to 15,000 messages a day with an average message size of 4,000 characters (4 kilobytes) and can store messages more than 60 days.

SMS Phase II systems are currently scheduled for delivery to USS Tarawa (LHA-1) and USS Harry S. Truman (CVN-75) with follow-on installations planned for USS Enterprise (CVN-65), USS Nimitz (CVN-68), USS Abraham Lincoln (CVN-72), USS Teddy Roosevelt (CVN-71), USS Blue Ridge (LCC-19) and USS Carl Vinson (CVN-70) in FY04.

NAVMACS II/SMS Phase II represents a unique approach to modernizing the Navy's communications infrastructure. And it will provide a means for transitioning legacy communication systems into more capable, speedier, better integrated and fully joint interoperable capabilities to U.S. Navy ships and their embarked warfighting components. □



When Acting Secretary of the Navy, Hansford T. Johnson, issued the policy guidance memorandum for establishing the Navy Marine Corps Portal (NMCP) last February, he further aligned the Department of the Navy (DON) with the growing number of organizations that, since the mid 1990s, have been building enterprise portals to improve access to cumulative organizational knowledge.

Although the types of enterprise portal-building organizations vary — government versus corporate, military versus civilian agency — the obstacles they face are remarkably similar. Non-integrated legacy systems, existing subordinate portals and countless, different data formats are common challenges.

A high degree of consensus has emerged, however, about a solution to many of these problems. Extensible Markup Language (XML) has largely become the “tool-of-choice” for those who are working to piece together the technical architecture behind these portals and is simultaneously helping to usher in a new wave of knowledge-centric organizations.

But understanding how XML can potentially support NMCP technical needs requires a look at recent history to clarify not only the DON's rationale for establishing this enterprise portal, but its vision for the system's ability to integrate information that its Sailor, Marine and civilian employee users will rely on to carry out mission-related and personal tasks.

Outlining the NMCP Vision

In his February 28, 2003 memorandum, Acting Secretary Johnson wrote, “In order to realize the benefits of our significant information technology (IT) infrastructure investment, a framework for organizing, managing and accessing Department information must be established.” That IT infrastructure investment is comprised of several programs, including the Navy Marine Corps Intranet (NMCI), Task Force Web and Information Technology for the 21st Century (IT-21). Together, they provide a foundation for increased knowledge sharing and seamless access to information across the DON. At the same time, they also present the DON an opportunity to build a framework in the form of NMCP, a single integrated enterprise portal structure for use throughout the Department.

The DON's vision for NMCP is multi-faceted. Most significantly,

“Our goal is a Web-enabled Navy-Marine Corps team, allowing our mobile workforce to have access to self-service transactions, via the Web, around the world. Our movement to Web-Services solutions will provide for the establishment of single authoritative data sources and eliminate ‘stand-alone’ and ‘stove-piped’ legacy systems.”

Dave Wennergren, DON CIO

April 3, 2003

Testimony before the House Armed Services Committee

it is to provide Sailors, Marines and civilian employees a single Web-based entry point for online access to multiple DON information technology systems and applications (including over 350 subordinate or “constituent” Navy portals) that contain a wide range of tactical, training, human resources and other types of information. For example, a Sailor might log on to NMCP to carry out critical warfighter duties, such as tracking fleet positions and conducting key maintenance tasks like ordering spare parts for Naval aircraft. But he could also use the portal to sign up for a training course, check the balance in his retirement savings account or read the latest headlines on Navy NewsStand.

Flexibility is another key part of the NMCP vision. The portal will be flexible to support individual user or command customization. This will allow users, for instance, to personalize the look and feel of their NMCP home page to feature the areas they visit most often. The DON also anticipates NMCP will play an important role in helping it better manage IT resources. Integrating DON systems and applications through NMCP will enable commands and offices operating their own portals to focus more on content delivery and conserve time, effort and funding currently directed toward developing constituent portal features and functions.

Part of NMCP-related improvements to IT resource management will be improving the reliability of Department information and consolidating older, non-integrated systems, a goal DON Chief Information Officer, Dave Wennergren, outlined in the weeks following the NMCP memorandum signing.

“Our goal is a Web-enabled Navy-Marine Corps team, allowing our mobile workforce to have access to self-service transactions, via the Web, around the world,” said Wennergren, in his April 3, 2003, testimony before the House Armed Services Committee. “Our movement to Web-Services solutions will provide for the establishment of single authoritative data sources and eliminate ‘stand-alone’ and ‘stove-piped’ legacy systems.”

XML: Supporting NMCP’s Technical Architecture

The NMCP program is at a relatively early stage in its overall development. But while many important decisions lie ahead, one thing is certain: XML will play a central role in the portal technical architecture. A key reason for XML’s behind-the-scenes prominence with enterprise portal projects such as NMCP is found in the technology’s special ability to extract and integrate data contained in the many different systems and formats that can reside under a portal’s umbrella-like structure.

“XML is the great translator,” says Bob Green, who chairs the DON’s XML Work Group. “In a portal environment, that’s very important. XML gives us the ability to create a common language for achieving the system-to-system interoperability that is necessary for providing information and responding to user queries through a single interface.”

XML tags enable the DON and other portal-building organizations to bridge the gaps that exist among their non-integrated legacy systems, constituent portals and other applications. Organizations can define the tags to clearly identify the content and meaning of both their structured (e.g., text documents, images, spreadsheets, presentation materials) and unstructured (e.g., relational databases, legacy databases or files) data.

The XML catch, to the extent there is one, is that organizations must agree upon standard meanings, or “metadata,” for the information resources (i.e., tags, namespaces, schema) that make up XML vocabularies to effectively transmit data among systems. But here too, the DON is well prepared. As part of the Department’s work to create an overall XML Governance Structure, DON commands have been logging their XML information resources into the Navy section of the Department of Defense Metadata Registry and Clearinghouse. This will further the goal of ensuring consistent applications of XML with NMCP and other programs.

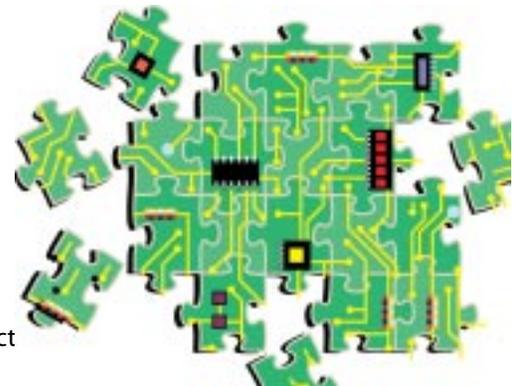
Extensibility is another factor in XML’s popularity with organizations building enterprise portals. In the DON’s case, the NMCP policy guidance memorandum directs that the portal’s technical architecture possesses non-proprietary implementation designed to rapidly respond to technology change. The requirement is tailor-made for XML, according to Green.

“XML’s extensibility allows you to create an infinite number of data types at the programmer level, which is particularly useful for NMCP,” says Green. “It protects portals from becoming snapshots in time and instead enables them to evolve with the organizations they serve. When the goal is to provide the very best and most current information to portal users, that’s a tremendous asset.”

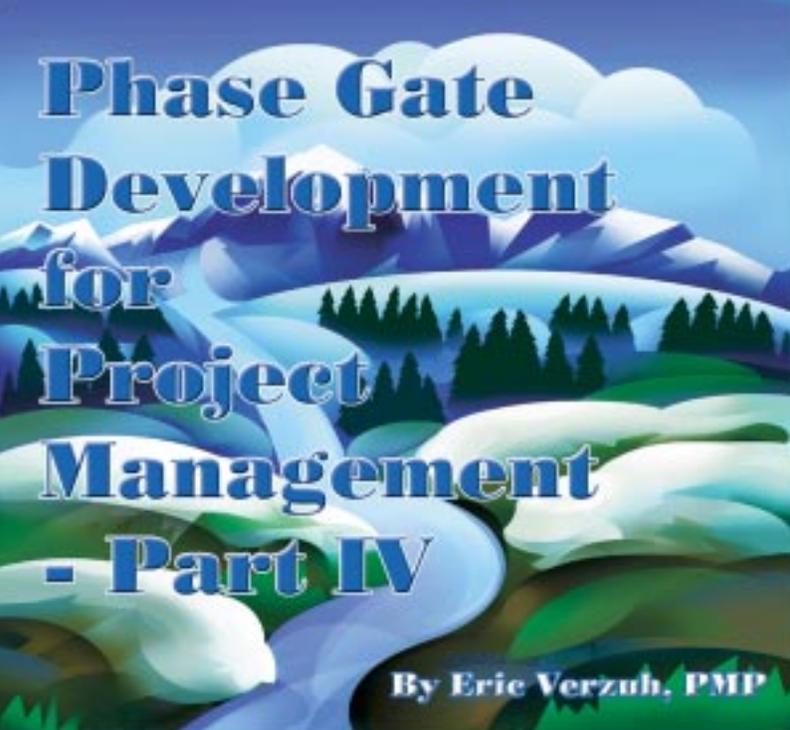
...A portal faced with the challenge of integrating information from multiple sources across a vast and constantly changing enterprise...

...A technology valued for its highly flexible nature and its ability to eliminate barriers to information sharing...

...NMCP and XML. It just might be a perfect fit.



Jack Gribben is a Research Fellow at the Logistics Management Institute (LMI), a nonprofit organization dedicated to improving public-sector management. LMI provides support to the DON XML Work Group. □



This year, 2003, America celebrates the beginning of one of our country's greatest projects, the exploration of the American West by the Corps of Discovery — better known as the Lewis and Clark Expedition. This great journey shares many characteristics with 21st century IT projects: It had a clearly defined beginning and end, required a team of dedicated professionals, confronted previously unimaginable obstacles and finished a year behind schedule! It's true. The original schedule called for the explorers to begin traveling up the Missouri River in the spring of 1804, reach the Pacific Ocean and return to St. Louis before winter 1805. Instead, they completed their journey September 23, 1806, and were instantly hailed as national heroes.¹

When your project finishes 10 months late, chances are there aren't any parades. Worse yet, there is often a sense of frustration and failure. Yet many IT projects face the same dynamic confronted by the Corps of Discovery: They are given a fixed deadline while the actual scope of the project is barely understood.

This is the fourth article in a series profiling project management techniques that apply to the IT environment. If you've read the previous articles, you may already be building detailed action plans, managing risks and developing a more cohesive project team. Those techniques focused on the day-to-day responsibilities of managing a project. This article will take a new perspective, examining an overall strategy for managing the risks of exploring new territory, a strategy called phase gate development.

Lewis and Clark have been described as having "undaunted courage" because of the physical dangers they braved and their willingness to journey into the unknown. They had little choice but to forge ahead with the best information and technology available. Many IT projects must begin the same way: Accepting a challenge with the best information at hand and the need to move forward.

It must be clear that not all IT projects can be characterized this way. IT projects come in many forms, ranging from mostly hardware oriented to mostly software oriented. Within that range some projects begin clearly scoped (extend network to the third floor of the office building because we are adding staff) while others are barely scoped (improve battlefield communication). Which kind is the source of

runaway schedules and budgets? No surprise — it is those that are barely scoped. The answer to improving control over these projects is a phased commitment strategy, more commonly known as phase gate development.

A phase gate development strategy is based on common sense: Don't make a commitment when you don't have enough information to support it. Instead, make a series of decisions to move forward and at each decision point make it legitimate to re-scope or cancel the project.

The Root of the Problem

We can understand the problem better by looking at data developed by Barry Boehm.² Figure 1 is a table that shows the range of accuracy for estimates at each phase of a software development life cycle. Note that the first estimate can be off by as much as 400 percent! Furthermore, the data are for well-run projects. The problem is that this first estimate was prepared when the project was barely scoped. These projects started with a general idea of what was to be accomplished and eventually that functionality was delivered — but along the way the understanding of how it would be accomplished evolved.

That is the nature of IT projects: We begin with a problem to solve and eventually use technology to solve it, but the discovery and creativity required along the way mean estimating will be difficult. Other fields have similar problems. For instance, in the pharmaceutical industry it is commonly accepted that out of 1,000 compounds identified (the chemical foundation for a potential product), only one gets to market as a drug.

This table shows the range of variation from the actual cost and schedule performance for estimates made at different points in the development process. Estimates at each stage of development were recorded and compared to actual performance. For example, Boehm found a project's actual effort and size to range from 4 times the estimate prepared at Initial Concept (pessimistic) to .25 times the Initial Concept estimate (optimistic).

Phase	Effort and Size		Schedule	
	Optimistic	Pessimistic	Optimistic	Pessimistic
Initial Concept	0.25	4.0	0.60	1.60
Approved Concept	0.50	2.0	0.80	1.25
Required Specifications	0.67	1.5	0.85	1.15
Product Specification	0.80	1.25	0.90	1.10
Detailed Specifications	0.90	1.10	0.95	1.05

Figure 1.

Establish Multiple Decision Points

A phase gate development model accepts the reality documented by Boehm and confronts the real risk of over-budget or behind schedule projects: *They are potentially business failures.* Every project is designed to have a return on investment or ROI. Given the uncertainty demonstrated by Boehm, it makes sense that once a project is initiated we revisit the business case periodically to validate the ROI. Figure 2 illustrates how a series of business case reviews relates to standard activities in a development life cycle. (*I fully acknowledge that this life cycle does not represent the complexity that can be found in a systems development methodology. The four phases*

shown here purposely simplify the example.) A curve is included in the figure to indicate the amount of discovery remaining in the project. It should make sense that early in the project there will be much more discovery remaining than at the latter phases.

How many decision points are required depends on the clarity of the project scope. In the earlier example of extending a local area network to another part of an office building, it seems realistic that two gates would be sufficient: The initial go-ahead and a review based on a detailed design and estimate. For the other example — improving battlefield communication — many gates will be required as the team clarifies both the goal (how will we know communication is improved?) and proposes various methods of delivering the capability.

Understanding the Gate

The final, fundamental requirement of using a phase gate strategy is to understand what must occur at each gate and who is responsible for it. A mature gated development model uses consistent gates for similar projects. Each gate consists of three components:³

- ◆ Required deliverables — what the project team will be asked to present at that decision point. These deliverables will change as the project progresses through development.
- ◆ Gate criteria — a known set of questions for judging whether the project should proceed.
- ◆ Specific outputs — what is the purpose of the gate? If it is to approve the next phase of the project, then an outcome should be a formal approval and action plan or budget for the next phase.

Passing a gate is a decision made by the project's owner — the organization that is funding the project and will benefit from its result. The owner weighs the proposed scope and benefits against the estimated project cost, delivery schedule and risks. At each successive gate in the development process there should be more evidence to support each of these elements. On complex IT projects there is seldom a single person who represents all of the owner's interests, so a steering committee performs this function.

The project team and project manager are responsible for supplying the estimates that make up the business case and for providing the evidence of their progress. That evidence takes the form of system development outputs such as documented requirements, system architecture, detailed designs, test results, etc.

At each gate, there are several legitimate outcomes including carrying on with the original project goals; adjusting the triple constraint of cost, schedule and scope; or project cancellation. If the project carries on as originally envisioned that means nearly all previous assumptions are being confirmed as the work progresses.

Managing Risk

Projects that are barely scoped often turn out to be two to four times as expensive as originally estimated because as they progress their scope gradually increases or we find them to be more difficult than initially envisioned. The gate deci-

sions are opportunities to look at the facts gathered so far and determine if the project should be scoped up or down, and to assess the reality of the current budget and schedule. Note that in Figure 2 each gate is described as a business case review, emphasizing that the real decision at each gate is whether the evidence at hand supports the assumptions that make this project a good investment.

Here's an example of how a phase gate strategy keeps projects on time and on schedule: If a project's initial estimate is \$50,000, but its revised estimate at completion of design is \$150,000, the project team and the project owner have choices — if they choose to carry on and the project completes for \$150,000 then it should be considered on budget! In other words, the baseline for measuring performance should not be the initial estimate based more on assumptions than facts. Rather, consider the baseline to be reset at each phase gate. To do it any other way would be like the family that decided to spend \$50,000 on remodeling their house, heard from both the architect and builder that their ideas were easily going to cost \$150,000, yet forged on and complained upon completion that the project was three times their original budget. Performance baselines should not be confused with wishes!

The other legitimate option at a gate is project cancellation. Though most project teams are disappointed when their project is canceled at a phase gate, it is not necessarily a sign of failure. In fact, canceling projects can be a sign of success.

Even in an ideal IT organization — where everyone is smart and knows how to do their job well — we'll still have projects canceled. That's because we must and should take business risks. We can initiate projects with thorough planning, using all our best estimating techniques, yet we lack a crystal ball to clearly forecast the future. Recall the earlier example of the pharmaceutical companies that find only 1 of 1,000 compounds turn into a marketable drug; if they had no canceled projects they would either have 999 unmarketable drugs or no drugs at all. Canceled projects are a sign that an organization is willing to try something new, yet is carefully managing its investments.

Another valid reason to cancel a project in our ideal IT organization is that as we make progress on several projects, a new, more valuable, more urgent project can arise. If all current projects are evaluated at regular gated intervals it will be apparent, which is the best candidate to cancel so resources can be redirected toward an investment with a better return. In reality, we make mistakes due to ignorance and incompetence so it is even more important that we scrutinize every project repeatedly. That is why I originally referred to

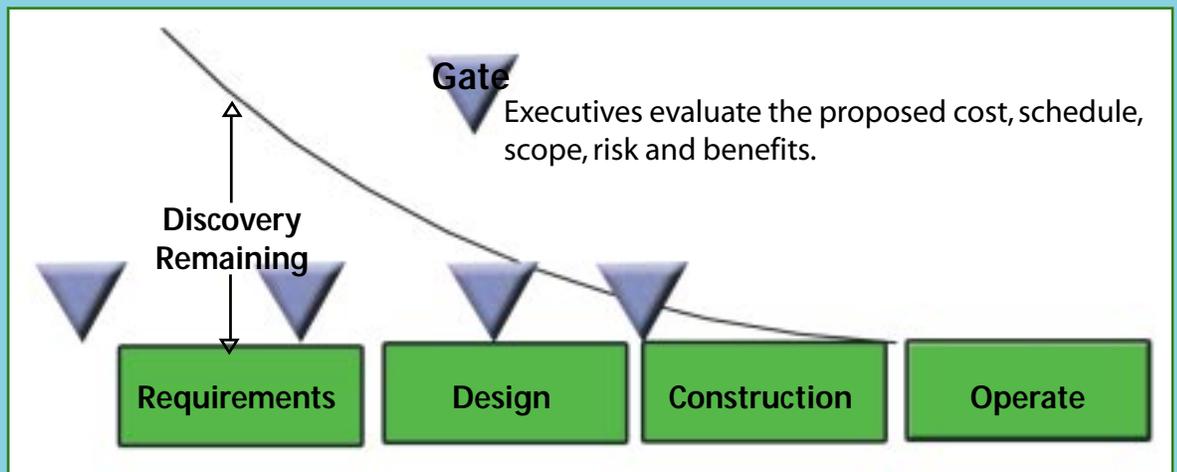


Figure 2. Phase gates in the development cycle

phase gates as a phased commitment strategy — each gate represents a commitment to pursue the next phase of the project.

The Essential Element

A phase gate strategy is unlike risk management and detailed planning, which can be performed by the project manager and team with or without the cooperation of other stakeholders. In contrast, the phase gate strategy only works if it is embraced consistently by those who initiate projects and oversee the project portfolio (the collection of all planned and active projects).

Phase gates must be used at consistent points along the development life cycle so that each project encounters the same gates. Through this common experience all project stakeholders develop a common understanding of the strategy. If only a few projects use gates or each project sets its own gates, the process will never mature and the benefits will never be realized.

The project management office may be given responsibility for establishing and managing phase gates, but the PMO only provides the structure. Those who fund and prioritize projects determine actual use of the process. Fortunately, these are also the people who gain the most from the process, because it allows them to initiate projects that are barely scoped yet retain control of the cost-schedule-scope equilibrium, even as this balance evolves.

Common Criticisms and Obstacles

There are two common objections raised to a phased commitment strategy for IT projects: The first objection is that project teams lose accountability. The second obstacle, strangely enough, is a mistaken belief that an IT organization is already using the strategy. How can we use the example of Lewis and Clark, whose raw determination and perseverance delivered one of our country's greatest accomplishments and at the same time claim canceling a project is legitimate and even a sign of success? Heroes aside, how do we keep a project team accountable for cost and schedule goals if we let them reset the baseline every time they fall too far behind? Excellent questions!

On June 13, 1805, Meriwether Lewis arrived at the foot of the Great Falls of the Missouri River. The expedition was on schedule to reach the Pacific Ocean by the end of summer and make the return trip down the Missouri River before winter. Twenty-nine days later the Corps had traveled only 20 miles; portaging the falls had taken longer than expected. Within days, the expedition leaders faced another unexpected obstacle: the Rocky Mountains. The huge mountain range they confronted was vastly different than the high plateau they expected.⁴

At this point it became clear that their original plan to reach the journey's end by that winter was no longer realistic. Given the reality of their situation, they changed their plans and determined they would winter on the Pacific Coast and return home in summer 1806. Some of their original assumptions proved to be wrong, so they made a new plan based on the best available information — a relevant lesson for any project manager.

Still the objection remains: How will we keep our project team accountable to goals if we allow them to reset baselines? We should also ask whether a team will accept accountability to a goal once it is clearly impossible. The art of setting realistic yet challenging goals combines the ability to estimate with the savvy to distinguish between poor performance and unexpected obstacles. At each gate a team should be asked to justify cost and schedule projections. If these have changed from one gate to the next, they should also be able to produce evidence that the scope or difficulty changed.

The second obstacle to implementing a phase gate approach is mistaking the phases of a development life cycle for phase gates. If you've been thinking, "Yes, we have a phased development methodology, so we are already doing this," you may be guilty of this mistake. Many organizations have multiple phases in their development methodology; yet don't apply the phase gate discipline. The distinction is in execution. If your projects have end-of-phase reviews then see if the following actions really take place: 1) The business case for the project is actually updated with changes noted so the evolution of the business case is apparent; 2) The baseline cost and schedule estimates for measuring project performance are formally changed; 3) The scope of some projects is increased, reduced or redirected based on the work performed in the previous phase; 4) Some projects are canceled as the original assumptions about cost, schedule and scope are proved false; 5) Some projects get higher priority because the underlying business case is stronger than originally anticipated.

If you have phase "reviews" without these results, you don't really have gates you have milestones — and you aren't managing the big picture — only the details.

Summary

The nature of projects is that we must often begin them with a hazy understanding of the actual work required to meet our goals. As a result, projects are initiated with an uncertain relationship between cost, schedule and scope — we have no choice. If final project performance is compared against the initial cost and schedule goals, we should expect to find wide (and wild) variances. A phase gate development strategy recognizes the inherent need to start projects without full information and responds by repeatedly forcing the project team to justify its scope and value at predetermined points in the development process.

Phase gate development does not mean an open checkbook to the project team. It is not a license to "work as long as it takes." Instead, it is a method to manage the business risk of the project, the risk that if the benefits, cost or delivery date changes, the project may no longer be worthwhile. The primary benefits of a phase gate strategy are to the owner, the person who is funding the project and gaining its benefits. It gives the owner greater control over the ultimate duration, cost and deliverables.

Though few IT project teams risk their lives as the members of the Corps of Discovery did, there are useful comparisons to managing projects that begin with uncertain scope. It is unrealistic and ultimately destructive to stick fast to original project goals of cost, schedule and scope when the facts are proving those goals to be a fantasy.

Resources:

1. Fifer, Barbara and Soderberg, Vicky. *Along the Trail with Lewis and Clark*. Helena, MT: Farcountry Press, 1998.
2. Boehm, Barry, et. al. *Cost Models for Future Software Life Cycle Processes: COCOMO 2.0*. Upper Saddle River, New Jersey: Prentice Hall, 1995.
3. Cooper, Robert G. "Stage-Gate New Product Development Processes." Ed. Eric Verzuh. *The Portable MBA in Project Management*. New York: John Wiley & Sons, 2003. (pp. 320-321)
4. Fifer and Soderberg, *Ibid*.

Eric Verzuh is the best selling author of two books on project management. Each year his firm delivers project management training to thousands of IT professionals. Contact him at www.versatilecompany.com.

Are You Ready to PK-Enable?

By Rebecca Nielsen and Kenya Spinks

Wouldn't it be so much simpler if Department of Defense (DoD) personnel had to remember only one simple Personal Identification Number (PIN) to carry out their daily responsibilities, no matter where they worked or traveled in an official capacity? As a result of new technology, this possibility will soon become a reality because all DoD members will rely on digital credentials to authenticate (i.e., verify their identity) to their private Web servers and applications, in lieu of conventional usernames and passwords.

Two memos from the Assistant Secretary of Defense (ASD), dated May 17, 2001¹ and May 21, 2002², set forth the importance of Public Key Infrastructure (PKI) in the DoD Information Assurance (IA) technical strategy. The earlier memo, "Public Key Enabling (PKE) of Applications, Web Servers, and Networks for the DoD," states, "e-mail in all operating environments and Web applications in unclassified environments shall be PK-enabled." The later memo, "Public Key Infrastructure (PKI) Policy Update" provided implementation dates of October 2003. However, the Department of the Navy Chief Information Officer (DON CIO) is aware that not all Navy Marine Corps Intranet (NMCI) eligible sites will have transitioned by the October 2003 deadline, and released a Naval message³ granting the Department a six-month grace period. The Department's new implementation date for meeting the three PKE milestones, identified in the May 21, 2002 memo, is April 1, 2004, as shown in the chart below.

The plan is to meet the milestones via enterprise solutions within the DON. For example, the rollout of the NMCI includes the public key-enabled Microsoft Outlook e-mail client and Microsoft Windows 2000, which are capable of certificate-based logon. Sites that have already transitioned to NMCI should be on their way toward meeting the first two milestones.

Existing October 2002 Requirement	Adjusted Milestone Date
Milestone 1: Ensure all electronic mail (e-mail) sent within DoD is digitally signed	April 2004
Milestone 2: PK-enable DoD unclassified networks for hardware token, certificate-based access control	April 2004
Milestone 3: PK-enable Web applications in unclassified environments	April 2004

The Navy Marine Corps Portal (NMCP) will support applications requiring PK-enabling. If the application requires only authentication, then integrating the application with the NMCP single sign on (SSO) solution meets the PK-enabling requirement. This article focuses on how to meet the third milestone, PK-enabling Web applications in unclassified environments.

What Is PK-Enabling?

PK-enabling is the process of using Public Key Infrastructure to provide solutions for some IA requirements. PKI itself is a framework

established to issue, maintain and revoke public key certificates.⁴ A certificate is a digital representation of information that at least:

- ✓ identifies the certification authority issuing it
- ✓ identifies or names its subscriber
- ✓ contains the subscriber's public key
- ✓ identifies its operational period
- ✓ is digitally signed by the certification authority issuing it⁵

The DoD has established a PKI to issue certificates to all DoD military and civilian employees and to other individuals who work full-time on-site at DoD facilities. DoD PKI certificates are issued primarily on Common Access Cards (CAC). Eligible personnel, known as subscribers to the PKI, who receive their CAC, hold three digital credentials: an identity certificate, an e-mail signing certificate and an e-mail encryption certificate.

PK-enabling provides applications with the capability to rely on digital certificates, either in lieu of existing technologies such as usernames and passwords or to enhance functionality such as incorporating digital signatures. Because PKI is based on cryptography, PK-enabling can also provide encryption services such as creating an encrypted channel through an untrusted network or encrypting a file or message so that only the intended recipient can read it.

PK-enabling not only enhances the overall security of the application, but also provides user and administrator benefits by reducing the requirement for both individual and application password management. Users will no longer be required to remember usernames and passwords for each system they are authorized to access. Instead, users need only remember the single password that unlocks the private key on their CAC. Administrators, while still required to manage who is authorized to access system resources, can map access rights to certificate identities and do not have to develop methods for transmitting initial passwords or managing password reset requests.

How to PK-Enable Web Applications

The primary requirement for PK-enabling Web-based applications is to authenticate users based on their digital certificate and associated private key. Certificate-based authentication consists of three steps: (1) establishing an encrypted communication channel, (2) validating the subscriber's certificate, and (3) performing a challenge-response between the server and the client to ensure that the user is the subscriber named in the certificate.

• Step 1: Establishing an encrypted communication channel. This step uses a protocol known as Secure Sockets Layer (SSL), or its successor, Transport Layer Security (TLS). This protocol requires that the application server send its public key certificate to the client. The client then generates the shared secret that will be used for the encrypted channel, encrypts it with the public key in the server's certificate and sends it to the server. The server's private key is required to decrypt the shared secret, so the client and server have now exchanged a key that is used for all further communications.

• Step 2: Validating the subscriber's certificate. After an encrypted

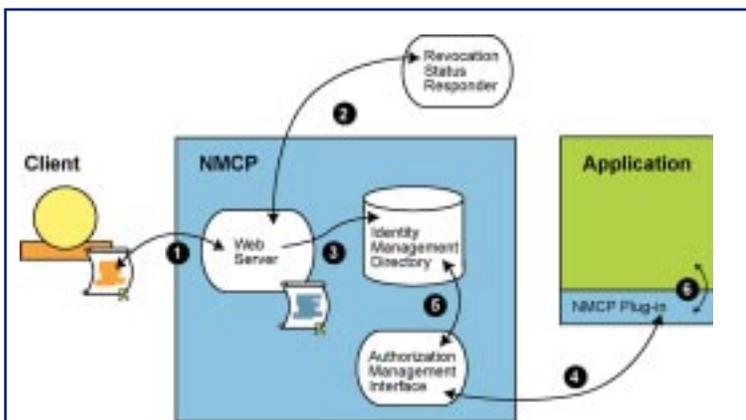


Figure 1.

Integrating an Application with NMCP

- ✓ *NMCP Web server performs certificate-based authentication.*
- ✓ *NMCP communicates with revocation status responder to ensure user's certificate has not been revoked.*
- ✓ *NMCP Web server provides identity of user to NMCP identity management directory.*
- ✓ *After the user has requested access to an application (not shown), the application communicates with the NMCP authorization management interface to determine the user's identity and authorizations.*
- ✓ *NMCP authorization management interface retrieves identity and authorization information from NMCP identity management directory.*
- ✓ *NMCP authorization management interface provides user identity and authorization information to application via the NMCP plug-in.*

channel has been established, the client sends the subscriber's certificate to the server. The server validates that the certificate was issued by a PKI that the server trusts, that the certificate has not expired and that the certificate has not been revoked. To support PK-enabling, the NMCI office is establishing responders at each Network Operations Center that can respond to requests from applications regarding the revocation status of certificates.

- Step 3: Performing a challenge-response between the server and the client. Because certificates are public, the server must now establish that the user attempting access is actually the subscriber named in the certificate. The server then sends a challenge to the client. The client must digitally sign the challenge using the private key that exists only on the CAC issued to the subscriber and return the signed challenge to the server. The server can use the subscriber's certificate to verify the signature on the challenge.

If these three steps are successful, the server can trust that the identity of the user is the same as the identity stated in the certificate and can then map that identity to authorizations.

NMCP — The Pathway to Single Sign On

The Department of the Navy intends to PK-enable at the enterprise portal level rather than requiring every application to be enabled. The DON CIO "NMCP Policy Guidance Memorandum"⁶ conveys the DON's approach to establish a framework for organizing, managing and accessing departmental information through an integrated por-

tal structure. The DON CIO is responsible for establishing a set of standards for the portal that focuses on quality assurance, quality of service, data standardization, metadata management, interoperability and enterprise-level information resource management.

The NMCP is a Web-based, user-customizable service that provides single sign on to all Web services using certificate-based authentication. The NMCP will pass authorization tokens extracting unique identifiers from the identity certificate to various Web Services behind the portal. The Department affirms that enabling at the portal level is not only feasible, but also cost effective. This is a benefit to each application developer and will not require individual applications to be enabled.

Applications that have already been PK-enabled should experience a more effective interface to the NMCP. In the future, these same authorization tokens will contain specific role-based attributes, allowing only those users who have the need-to-know with access to those enabled Web applications. Those Web Services requesting access from the NMCP must have their services registered in the NMCP service registries.

The NMCP will further support functional and organizational collaboration across the DON and promote DON-wide process engineering. The end user and organizational commands will be able to subscribe to desired services, tailor the view provided and have these services provided at each logon to the enterprise portal. Figure 1 illustrates the future NMCP architecture.

Summary

The Department of the Navy is taking aggressive steps to meet DoD PK-enabling requirements primarily through the strategic use of the NMCI and the NMCP. Developers of applications that have been identified by the Functional Area Manager (FAM) as either approved applications or approved with restrictions should coordinate with their Functional Area Manager to integrate their Web-based applications with the NMCP. Some organizations may own applications with constraints that prevent them from fulfilling these requirements. These organizations should contact their appropriate chain of command for guidance. For more information regarding the NMCP, contact David.O.Rose@navy.mil.

References:

1. Assistant Secretary of Defense (ASD) Command, Control, Communications and Intelligence (C3I/CIO) Memorandum, "Public Key Enabling (PKE) of Applications, Web Servers, and Networks for the Department of Defense (DoD)" of May 17, 2001.
2. Assistant Secretary of Defense (ASD) Command, Control, Communications and Intelligence (C3I) Memorandum, "Public Key Infrastructure (PKI) Policy Update" of May 21, 2002.
3. DON CIO Washington 292338Z SEP 03.
4. X.509 Certificate Policy for the U. S. Department of Defense.
5. American Bar Association. Digital Signature Guidelines. August 1, 1996.
6. Department of the Navy Chief Information Office Memorandum, "Navy Marine Corps Portal (NMCP) Policy" of February 28, 2003.

Rebecca Nielsen and Kenya Spinks support the DON CIO Information Assurance Team. □



Can You Hear Me Now?

Managing the Electromagnetic Spectrum

By the DON CIO Spectrum Team

It is clear that spectrum is a key component in achieving information dominance for future U.S. military operations. The DON spectrum management process, if adhered to, will greatly enhance the warfighter's ability to have seamless and transparent access to spectrum's extraordinary capabilities for transmitting information.

The 22-screen multiplex cinema down the street from Ray Willis' office in Alexandria, Va., does a brisk business on most days, but Ray rarely has time to catch Hollywood's hottest new flicks. He and his colleagues are too busy working on a blockbuster of their own that has real-world implications for Department of the Navy (DON) warfighters afloat and ashore.

Ray is part of a team of dedicated professionals at the Navy and Marine Corps Spectrum Center (NMSC), formerly NAVEMSCEN, focused on managing the DON's use of the electromagnetic spectrum — a class of radio waves propagated by a system of electric and magnetic fields that include the full range of radiant energy from radio and light waves to gamma and cosmic rays. Atmospheric interaction with these waves provides characteristics that can be harnessed, using electronic systems and devices, to transmit information.

Supporting the management and use of the radio spectrum from the NMSC perspective means planning and coordinating joint use of required frequencies through operational, engineering and administrative procedures. The objective is to enable DON spectrum-dependent systems and devices, such as radios that support voice communications or digital data links, Global Positioning Systems, and systems for detecting and suppressing enemy radar and communication sites, to perform their functions in the intended environments without causing or suffering, unacceptable interference.

Spectrum management is a high-stakes proposition. DON command and control centers are afloat assets with no direct access to commercial or military communications systems via landline, which puts

commanders in the position of being solely dependent upon wireless technologies that use spectrum to perform mission-essential tasks. Comprehensive spectrum coordination in this environment is more than just good policy — it is crucial to the DON's ability to remain highly maneuverable, flexible and tactically effective.

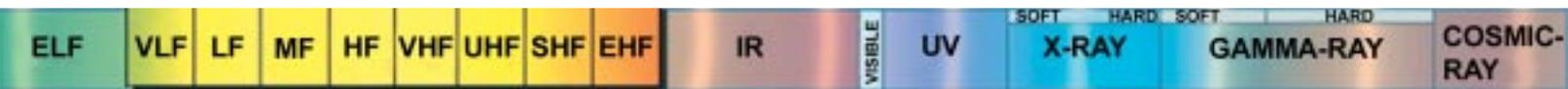
Spectrum's Crowded Neighborhood

An NMSC spectrum certification engineer, Ray Willis has devoted more than 15 years of his career to managing and supporting United States military spectrum activities. In that time, he has seen up-close the extraordinary growth in the number of military and commercial systems and devices using spectrum, from high-powered mobile radar and ship/air early warning systems to cellular telephones and personal communication system (PCS) devices such as Blackberries.

"The biggest change I've seen is that, coincident with the rapid technological advances in spectrum usage, the critical importance of spectrum in mission performance has become more and more evident," said Willis. "You see it talked about everywhere. At congressional levels, at the FCC."

Like rapidly expanding suburbs near large cities, however, the crowded spectrum neighborhood is vulnerable to its own traffic jams. When individuals and organizations forget or ignore the necessary basics for operating a piece of equipment harmoniously in the electromagnetic spectrum with its finite number of frequencies, there can be serious consequences.

"The fact is you want the piece of equipment to successfully operate to achieve the



desired mission. You want to be able to turn it on," said Willis. "But there have been cases where people purchased something and we determined later on it couldn't be used in that [frequency] band. When equipment is acquired without considering the rules and regulations governing its use, or the necessary process for securing the required authorization, then the user has just bought himself a big paperweight because he cannot legally use the equipment."

The NMSC-led "process" is a key part of the DON's approach to managing the electromagnetic spectrum and ensuring its spectrum-dependent equipment can operate successfully and without interference in land, air and sea-based environments. This spectrum management process consists of three basic phases: equipment certification, frequency assignment and host nation approval.

Phase 1: Equipment Certification

Before a unit decides to purchase or develop equipment that requires use of the spectrum, it must obtain an equipment certification, a "permit to operate," from the National Telecommunications and Information Administration (NTIA) — coordinated through NMSC. The Center reviews the equipment application to ensure it is compliant with spectrum management policy, allocations, regulations and technical standards, and determines whether the radio-frequency spectrum it requires is available. When granted, a certification provides a unit the authority to conceptualize, experiment, develop or operate (and then procure) new spectrum-dependent equipment.

Equipment certification is also where a unit gets its first exposure to the DD Form 1494, Application for Equipment Frequency Allocation. The DD 1494 is the vehicle through which units provide specific technical information to NMSC regarding their spectrum-dependent equipment across all three phases of the spectrum management process.

An increasing number of DD 1494s are arriving at NMSC from units seeking certification to operate commercial-off-the-shelf (COTS) equipment, which is not surprising since more units are purchasing ready-to-use COTS products with military capabilities that can be more cost-effective for the DON. This was the case, for example, with

the Naval Oceanographic Office Network's (NAVO Net) Stennis Space Center headquarters in 1999 when it submitted its DD 1494 for the SmartLink C-Band SATCOM Terminal, a system that proposed using spectrum to provide ship-to-shore connectivity in support of oceanographic survey operations for T-AGS 51 and 60 class ships.

Phase 2: Frequency Assignment

Once a system or device has completed the equipment certification process, and a letter is produced confirming that the equipment has been certified, the next phase in the spectrum management process begins: obtaining a frequency assignment. In this phase, a unit must submit a frequency assignment proposal. When NMSC receives a frequency proposal request, it must include the nomenclature of the certified equipment that will be used. The granting of a frequency assignment, a license to operate, gives a unit the authority to operate a piece of equipment on a specified frequency, frequencies or frequency band at a specific location and under a specific set of conditions.

The spectrum management process isn't a one-way street, of course. NMSC engineers and telecommunications specialists who are responsible for shepherding DD 1494s through Phase 1 (equipment certification) and Phase 2 (frequency assignment) often contact manufacturers, in the case of COTS products from outside vendors or the units themselves to clarify outstanding questions and issues.

Ray Willis recalls how a back-and-forth consultation between NMSC and one unit helped to resolve a potential pre-assignment frequency interference issue. The DON wanted to install a Dry Dock Flood Alarm System at the Pearl Harbor Naval Shipyard to guard against floods by measuring the harbor water levels.

"This alarm system had the potential for interfering with some systems already operating at the same location," said Willis. "We suggested the unit do an on-site study to confirm whether the new system would create interference. They determined the power was low enough, so it would not. Sometimes we have to do things like that — to assist frequency managers at units when a new frequency is being introduced and encourage them to ask, 'Have we done everything that is necessary to ensure electromagnetic compatibility?'"

Phase 3: Host Nation Approval

Spectrum management doesn't stop at United States borders. While the DON mission is worldwide, host nations have sovereign rights over the spectrum within their borders. The use of U.S. spectrum-dependent commercial and military systems abroad requires careful coordination and negotiation.

The Host Nation Approval (HNA) phase applies to spectrum-dependent equipment that could be used in a foreign country or its territorial waters. The DD 1494 requires a unit to indicate the geographical area in which a system will operate. This discloses, for example, that systems like NAVO Net's SmartLink C-Band SATCOM Terminal, used in worldwide ocean areas, have the potential for interacting with a foreign government's spectrum policies and regulations. NMSC takes the lead on HNA coordination. Working with the cognizant Combatant Command (COCOM) and/or other U.S. government agencies, it secures approval for the DON to operate its spectrum-dependent equipment outside the United States, which entails obtaining approvals and certifications from host nations.

Coordinating HNA can be time consuming; it can take over a year to receive authorization from a country. Issues that affect the amount of time required include: how the host nation uses the frequencies being requested, equipment certification, output power, and in-country locations and length of time in which equipment will be used.

It is clear that spectrum is a key component in achieving information dominance for future U.S. military operations. The DON spectrum management process, if adhered to, will greatly enhance the warfighter's ability to have seamless and transparent access to spectrum's extraordinary capabilities for transmitting information. For Ray Willis and his NMSC colleagues, that will be better than the best Hollywood ending.

You can contact the DON Spectrum Team at DONSpectrumTeam@navy.mil. □



By Richard B. Waina, P.E., Ph.D.

The title of this article is actually the wrong question to be asking. The CMMI (Capability Maturity Model Integration) is NOT a set of “bolt-on processes” that last only as long as the wheel is squeaking. The CMMI Product Suite, as noted in previous articles in this series, is a process-improvement approach that provides descriptions of best practices (at a very high level — they’re not procedures) that address productivity, performance, cost and stakeholder satisfaction. The CMMI provides a consistent, enduring framework that accommodates new initiatives and focuses on the total-system problem.

Five process areas are related to process management and six are related to management oversight. The information contained in these 11 process areas assists executives in:

- Focusing on long-term organization viability rather than short-term project and contractual issues
- Establishing a strategic business plan
- Providing and protecting resources for long-term improvement of the organization’s processes

As noted in my previous series of articles for CHIPS, “Five Critical Questions in Process Improvement,” any process improvement program should be driven by and related to some set of business or overarching organizational needs. Use the CMMI as a “checklist,” if you will, to see where existing organizational processes might need some “tweaking” to enhance their effectiveness and efficiency.

Leadership

The role of the leader is at the heart of CMMI-based process improvement. Proactive leadership is the most critical element of any implementation. Bottom-up change is too unpredictable. Organizational change must be designed, implemented as a mission-critical project and led from the top for the following reasons:

- Competing alternative solutions result in piecemeal efforts instead of integrated effort.
- Resources must be committed and dedicated to the process-improvement effort.
- Leaders must establish a mentoring environment for process

improvement, reward process improvement efforts and discourage resisters to process improvement.

- Leadership behavior is watched and emulated.

Leaders must establish and maintain the vision for process improvement. They need to be:

- ✓ Able to see the business need for process improvement and express it in a compelling manner.
- ✓ Willing to personally lead the effort.
- ✓ Capable of changing their own behavior to comply with the new processes and to support others as they learn to comply with them.

Beyond that, the primary function of the leadership is to provide an environment in which process improvement can flourish and enable systematic, continuous process evolution. They can do this by:

- Providing a stable environment which enables process maturation (Level 2) including:
 - Promulgating policies which establish clear expectations with regard to process discipline
 - Requiring key processes to be documented
 - Providing appropriate process and domain training
 - Providing resource levels adequate to permit process institutionalization
 - Reviewing process improvement plans, progress and corrective action
- Establishing an organizational process framework which enables organizational learning and leveraging of good practices (Level 3):
 - Establishing a family of standard organization processes designed to be tailored for specific accounts or projects
 - Establishing an organizational product/process/service delivery metrics database
- Establishing a quantitative management environment (Levels 4/5):
 - Requiring regular reports of summary process/product/service delivery metrics appropriate to the delivery domain
 - Reviewing the utilization of product/process/service delivery data

Leaders can delegate authority, but can never delegate away responsibility. The leadership of the organization must make CMMI-based process improvement a priority and provide the visible leadership necessary to keep process improvement a high priority within the organization. Managing change is a difficult and time-consuming task. Without sufficient top management sponsorship and leadership (which means much more than just mandating “get it done”), process improvement will at best flounder and more likely fail. This will engender a climate that will make future improvement initiatives more difficult to achieve.

Two Models

As described in the first article in this series (Summer 2003), CMMI models have two representations, continuous and staged, which provide alternative approaches (see Figure 1) to process improvement. The continuous representation focuses on process capability — the range of expected results that can be achieved by following a process. Process improvement is measured in capability levels that relate to the achievement of specific and generic goals in each process area. The continuous representation provides

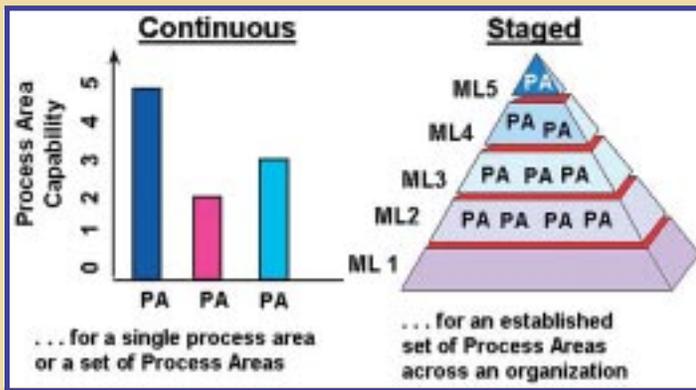


Figure 1.

flexibility for organizations to choose which processes to emphasize for improvement and how much to improve each process. It enables selection of the order of process improvement that best meets the organization's business objectives and mitigates risk.

The staged representation is based on organizational maturity — the combined capabilities of a set of related processes. It focuses on a few key process areas to help an organization prioritize its improvement activities. The CMMI staged model implements this "roadmap" approach to process improvement by selecting a few critical process areas and incorporating the Capability Level 2 generic practices as Institutionalization common features. Note that this view does not imply that a Level 2 organization (or even a Level 1 organization) is not performing some of the practices of the other process areas. In fact, we can assume that it is performing at least some of the engineering practices or it would not be able to produce and sell products.

An organization using the staged representation first focuses on establishing a stable management environment and process discipline so that desirable processes are not abandoned in a crisis. The emphasis is on implementing some basic documented processes so that successful practices can be repeated; some organizational memory is established to reduce the reliance on "heroes" and reduce the risk of unsuccessful organizational performance. At Level 3 the focus shifts from repeatable project performance to an organizational learning mode, so the "good/best" practices can be implemented across the organization, further improving organizational performance by reducing the incidence of "less good" practices.

Which Model?

There has been much debate in the community about the relative merits of the staged and continuous approaches. I believe the debate can be better framed if we look at the differences between process maturity and organizational maturity. Process maturity focuses on the effectiveness/efficiency of specific processes related to various organizational functions. Organizational maturity reflects the underlying management/leadership infrastructure, which supports the ability to make process changes (hopefully improvements) globally and have them "stick" (endure).

The staged and continuous representations of the CMMI are identical at the detailed goal and practice level, except for the base and advanced practices in the continuous representation. Therefore, implementation of the two versions (for the same compo-

nents) will be identical. The only question is the order of component implementation. These priorities will be driven by the needs of the organization, which are a function of the business purposes and current problems.

The continuous architecture has the advantage of providing a fairly well-defined improvement path for a specific Process Area (PA). However, if you have a large number of process areas, it becomes more difficult to provide guidance to an organization that is attempting to rationally allocate limited improvement resources across PAs. Do you focus on a few or try to maintain uniformity of capability levels across PAs or use some hybrid approach? This question needs to be answered in the context of the organization's business goals and objectives.

The advantage of the staged architecture is that the organizational improvement path is well defined in terms of which PAs need attention first. (However, there may be valid business reasons to modify that recommended path.) The Maturity Level 2 PAs focus on getting documented processes in place at the project level. Maturity Level 3 provides a framework of standard processes for leveraging best practices across the organization. Maturity Levels 4 and 5 focus on detailed process and product metrics for control and improvement.

Strategy versus Tactics

The mapping back and forth between continuous and staged CMMIs, while fairly straightforward, can be challenging to inexperienced persons striving to develop reasonable process improvement plans for their organizations. Faced (typically) with limited resources and limited capacity for organizations to embrace and implement changes in behavior, they seek the kind of guidance which is available from staged models. Simultaneously, they are concerned that focusing on only a few process areas may cause them to neglect some other areas whose performance may be critical to organization success.

I suggest that the staged representation be used to develop the process improvement strategy and the continuous representation be used to develop the tactics of process improvement. By this I mean that an organization should, per the staged model, focus on those Level 2 and Level 3 Process Areas that support its business needs (which could include a mandate to become Level 3 for competitive reasons). In general, this will enhance the ability of the organization to establish that environment which will enable lasting process improvement. In developing action plans for specific Process Areas the organization should consider the continuous representation, as this will give it more detailed guidance as to the exact steps that need to be taken to achieve maturity of a given process.

Transitioning from Another Model

Many organizations are concerned with capitalizing on investments they have made using other models. Given that it was derived from existing models which were in widespread use, the CMMI is compatible with a variety of capability and process improvement frameworks as shown in Table 1. Organizations can build on their existing process improvement

Departure Model	CMMI - Compatible	Features Enhanced by CMMI	Additional Features Provided by CMMI
SW-CMM	YES	Core processes are integrated	Systems Engineering and Project Management
EIA-731	YES	Core processes are integrated	Software System Development and Project Management
ISO 9000:2000	YES	Organizational institutionalization	Progressive levels
SE-CMM	YES	Core processes are integrated	Software System Development and Project Management
PMBOK	YES	Core processes are integrated	Systems Engineering, Software System Development and Integrated Project Management
Homemade	Maybe	TBD	TBD
Nothing	YES	Addition of process framework	Provides integrated project processes

Table 1. CMMI Compatibility

infrastructure and use the CMMI as a new set of guiding principles. In particular, organizations transitioning from the Software CMM to the CMMI will need to deal with the following issues:

Level 2:

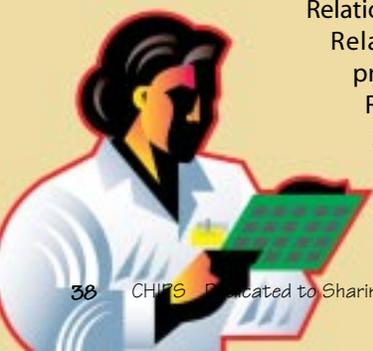
• **Requirements Management** - Traceability, which has always been necessary but not clearly demanded, is now asked for explicitly. Requirements Management is expected to operate in parallel with Requirements Development and offer support as new requirements are discovered and requirements change requests are made.

• **Project Planning** - There is increased emphasis on having a detailed Work Breakdown Structure (WBS). Planning parameters now clearly include:

- Critical competencies and roles needed to perform the work
- Cost of externally acquired work products
- Knowledge and skills training, mentoring and coaching needs
- Capability of tools in the engineering environment
- Level of security required

The identification and involvement of stakeholders is an important evolution of the "all affected groups" statement that appeared frequently in the SW-CMM. The commitment process is now explicitly defined. The required plan for stakeholder interaction includes:

- List of all relevant stakeholders
- Rationale for stakeholder involvement
- Expected roles and responsibilities
- Relationships between stakeholders
- Relative importance of stakeholder to project success by phase
- Resources needed to ensure relevant stakeholder interaction
- Schedule for phasing of stakeholder interaction



Data Management (from EIA/IS-731) is now addressed as part of Project Planning for the planning and maintaining of project data items. Their contents have been added to the list of project management concerns. Data Management requires administrative control of project data, both deliverable and non-deliverable. Some large, critical projects demand that even Engineering Notebooks with daily entries be placed under control for audit purposes.

• **Project Monitoring and Control:** Monitoring Commitments have been elevated to the Specific Practice level. Monitoring Risks and Stakeholder Involvement are also more strongly emphasized in the CMMI compared to the SW-CMM. PMC also includes Monitor Data Management.

• **Process and Product Quality Assurance** stresses the objective evaluation of products as well as processes. Evaluation criteria must be established based on business objectives. What will be evaluated? When or how often will a process be evaluated? How will the evaluation be conducted? Who must be involved in the evaluation?

• **Configuration Management:** The idea of a "Software Library" has been replaced by the more encompassing "Configuration Management System," which includes the storage media, the procedures and the tools for accessing the configuration system.

• **Supplier Agreement Management** evolves the initial ideas found in Subcontract Management and incorporates the original intent of Subcontract Management, as well as, lessons learned over the past seven years. It is unlikely to be declared "Not Applicable" in an appraisal, as it now focuses on all sources of supply for projects.

• **Measurement and Analysis** (new) makes crystal clear the intent of the Measurement and Analysis common feature found in the SW-CMM. An organization that barely passes the Measurement and Analysis Common Feature requirements of the SW-CMM would not pass the measurement requirements of CMMI. Using the guidance in this process area, the organization can evolve its measurement program from basic project management measures to those based on the organization's set of standard processes, and then to statistical control of selected sub-processes according to the organization's business needs.

Level 3:

• **Requirements Development (new)** concepts are consistent with very modern publications on Requirements Engineering. It incorporates and expands on the interface ideas of Systems Engineering and Software Engineering with regard to gathering, analyzing, documenting and maintaining requirements found in the SW-CMM. Requirements Development truly shows the recursive and iterative nature of developing requirements: the Requirements Development process area includes a description of developing an operational concept and operational scenarios to refine and discover new requirements, needs and constraints that include the interaction of the product, the end user and the environment. It also includes a strong focus on interface requirements. It suggests the use of models, simulations and prototyping to perform risk assessments to reduce the cost and risk of product development. It is very tightly coupled to the Technical Solution process area and emphasizes the idea

of starting the process of requirements validation very early in the product life cycle.

• **Technical Solution (new)** practices apply not only to the product and product components but also to services and product-related processes. Technical Solutions are developed interactively with product or product component requirements definition. Technical Solution stresses the need for developing alternative solutions. Once the “best” set of alternative solutions are selected it is then possible to establish the requirements associated with the selected set of alternatives to be allocated to the product components. Technical Solution also stresses:

- Product or product component design
- Documenting the complete design description in a “Technical Data Package”
- Designing interfaces
- Performing make, buy or reuse analysis
- Implementation
- Establishing and maintaining product support documentation

• **Product Integration (new)** presents the concepts to achieve complete product integration through progressive assembly of product components in one stage or in incremental stages according to a defined integration strategy. It stresses the careful analysis and selection of the optimum integration strategy. The basis for effective product integration is an integration strategy that uses combinations of techniques in an incremental manner. It points out the need to establish and maintain the environment required to support the integration of the product components. It also stresses the effective management of interfaces to ensure that all interfaces will be complete and compatible.

• **Verification (new)** captures the ideas of using reviews, loads, stress and performance testing, simulation, observations and demonstrations as applicable to ensure that the requirements are being addressed at each phase of the development life cycle from a systems, hardware and software point of view. Peer Reviews are now a goal within this Process Area.

• **Validation (new)** places a stronger emphasis on ensuring that the system will perform as intended in the operational environment.

• **Risk Management (new):** The concepts inherent in risk management finally made it to Process Area status:

- Risk Identification
- Risk Assessment
- Risk Analysis
- Risk Prioritization
- Risk Mitigation
- Risk Contingency Planning

The ideas behind Risk Contingency Planning and Risk Mitigation have been merged but are now clearer.

• **Decision Analysis and Resolution (new)** presents the concepts of identifying alternatives to issues that have a significant impact on meeting objectives, analyzing the alternatives and selecting one or more that best support prescribed objectives. Decision Analysis and Resolution is a new concept for the software world whose time has certainly come. Understanding decision-making models from Operations Research can help in making full use of this process area.

• **Organizational Process Definition** wording has changed subtly but significantly from that of the SW-CMM. “Establish and maintain a usable set of organizational process assets including the organization’s set of standard processes,” acknowledges that an organization may utilize more than one standard process to handle its product lines and business needs. The Process Database evolved into the Organizational Measurement Repository.

• **Integrated Project Management** includes the aspects of Integrated Software Management and Intergroup Coordination that were found in the SW-CMM. The project is conducted using a defined process that is tailored from the organization’s set of standard processes. It also emphasizes the need to integrate the concepts in the Project Plan and all supporting plans such as:

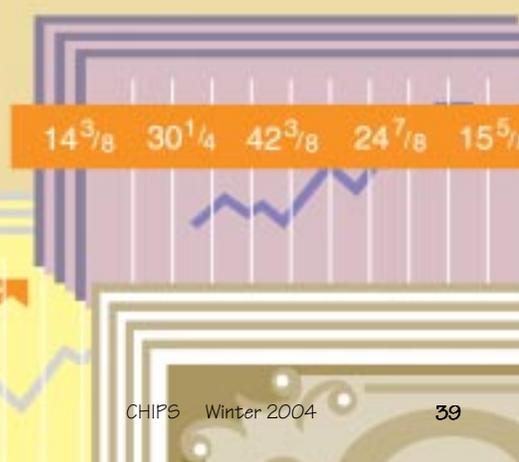
- Quality assurance plans
- Configuration management plans
- Risk management strategy
- Verification strategy
- Validation strategy
- Product integration plans

Levels 4 and 5 Process Areas reorganize and hopefully clarify the Software CMM Levels 4 and 5 practices.

Conclusion

CMMI implementation involves determining an overall process improvement strategy based on business goals and objectives. This article has dealt with a set of fairly high-level strategic issues involved in implementing a process improvement program based on the CMMI. The next article will deal with the tactics of actually developing and implementing specific improvements to processes.

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. Dick can be reached at www.md maturity.com. □



from point a to b or information transport), Network Defense (how we defend the information) and Operations Support (how we provide day-to-day operations warfighter support).

Infostructure Control. We provide our communications professionals with specific guidance for managing Net Operations. The Special Instructions to Communicators (SINC) Manual provides detailed instructions on how we support communications in theater. Each day, the NOSC publishes the Communications Tasking Order (CTO), which delineates how we will “fly the network” for that day. As events occur, we issue communications Notices to Airmen (NOTAMS) to keep senior leaders informed of significant events. We use the tools at our disposal as our single pane of glass to view the state of the enterprise.

Command Network Defense. Our means of network defense employs a “Defense-in-Depth” strategy using a combination of firewalls, intrusion detection systems, relays and anti-virus protection to protect and defend the enterprise.

Operations/Warfighter Support. In PACAF, we’ve worked hard to integrate the services we provide to warfighters. In addition to monitoring computer network status, our NOSC also provides theater-wide Help Desk support which includes Air Traffic Control and Landing systems oversight, In-Transit Visibility and eventual Theater Battle Management Core System Unit Level (TBMCS-UL) Help Desk support. The NOSC is the one-stop shop — and not just for communications.

The Challenges

We have one major issue that encompasses our focus for taking net operations into the future, and we codify that in a concept we call “Operational Rigor and Discipline.”

What do we mean by Operational Rigor and Discipline? Perhaps a good start is to state what it is not. Imagine for a moment that you need a critical operation that will save your life. Now picture yourself with a doctor who decides to “wing it” rather than follow specific and rigorously defined medical procedures. What are the chances that you will survive? Operational Rigor and Discipline is the systematic process of creating clearly defined and documented procedures for a process. By following this process, we eliminate the “magic” that frequently appears to be the way of doing business in some enterprises, and it provides the platform for ensuring success by doing the same correct procedures over and over with positive results.

Two other significant challenges we are working are:

Configuration Control. Like any other large organization, we purchase services from a diverse group of vendors. The challenge, of course, is figuring out how to integrate these disparate services into a framework that provides the right information to warfighters at the right time.

Malicious Code. Another challenge we face comes from viruses and worms. The entire world recently suffered from the “Welchia.Worm” and “Blaster” virus attacks. Welchia, unlike embedded e-mail viruses, added a new twist by exploiting remote procedure call (RPC) vulnerabilities in networks. The result was degradation of services worldwide. In PACAF net operations, we view virus incidents as the equivalent of a Class B Mishap (loss of an aircraft and its associated loss of life). Without Operational



Above: The PACAF NOSC.

Rigor and Discipline, we needlessly increase our risk to the ever increasing spread of malicious code.

The Way Ahead

The NOSC is undergoing a vector change to enable PACAF “Predictive Network Battlespace Situational Awareness” through a detect-in-depth/defense-in-depth strategy. Additionally, we want to facilitate PACAF’s ability to conduct Capabilities-Based Net Operations throughout the theater of operations.

The PACAF NOSC’s way ahead is simple: lockdown the network. This means we need to facilitate enterprise standardization and provide configuration standards down to the desktop and through the NCCs. It also means we must facilitate the methodical, systematic deployment of new technologies in collaboration with our industry partners to assist in automating data gathering, and reporting and tracking of network status while eliminating unit-level “County Options.” Lastly, it means we must: (1) create new Tactics, Techniques, Procedures (TTP) for our people; (2) identify network processes; (3) focus on filling gaps in guidance; (4) identify training deficiencies; and (5) train to the standard. This entails using personnel with the right credentials to fly the network; codifying well-defined processes and procedures; conducting periodic “check rides”; and erecting strong standard/evaluation functions to sustain the effort over the long term.

In addition to the advanced technology we must leverage for success, we need our partners to provide us with the processes that go along with the tools. It does not help us to get the product first, deploy it and then find out that we need to execute within a specific framework after the fact. The process has to come first, so we can more efficiently leverage technology tools to achieve the desired effect on the enterprise.

We need our partners to continue an open dialogue with us and help keep us current on the latest and best technology solutions. Partnerships are one of the things that define us as Americans — our willingness to work together for a common cause. At the end of the day, each of us has a commitment to protect our troops and bring them home safely. The right technology mix helps make that possible.

Reference

1. Network Centric Warfare Department of Defense Report to Congress. Updated January 25, 2002. (<http://www.defenselink.mil/nii/NCW/>).

Portal Technology For Military Supply Chain ERP Solutions

By Robert L. Sullivan and Robert B. Stevens

Today's Army logistics applications and systems are moving across enterprise boundaries on a global scale, which means that business process owners are pivotal in facilitating collaboration within the Army and other enterprise stakeholders. Collaboration requires integration and, integration requires a comprehensive understanding of applicable business processes. The Army Logistics Modernization Program (LMP) will network business process owners across enterprises that provide input to the development of standard work processes and solution sets. This allows innovative thinking and organizational differences to be captured at initial design, rather than implementation.

To capitalize on this innovation the Program Manager for the Army's newest rocket delivery system, the High Mobility Artillery Rocket System (HIMARS), is teaming with the University of Maryland (UMD) Supply Chain Management Center (SCMC) and the Center for Public Policy and Private Enterprise for one year on a Supply Chain Management demonstration project to identify portal technologies for solving supply chain issues. This project will leverage the Supply Chain Portal technology built for the Office of the Secretary of Defense (OSD) that is currently being transitioned into production in the U.S. Air Force.

The project will be developed by proven technologies to establish the foundation of a best practices supply chain and sustainment network to support the Army venture into Life Cycle Contractor Support (LCCS). The Portal initiative is an outgrowth of the HIMARS Milestone C Decision. The Assistant Secretary of the Army for Acquisition, Logistics and Technology (ASA(ALT)), the Honorable Claude Bolton, directed the HIMARS Product Manager to evaluate the benefits and risks associated with Contractor Logistics Support (CLS) and publish the results Army-wide.

Logistics supply chain efficiency comes from making good decisions based on accurate knowledge delivered in near-real time. There is always an inherent tension between the cost of gathering data and the measurable improvement in efficiency, operational needs and readiness goals. The Army is moving toward Performance Based Logistics (PBL) for more accurate predictions of impending failures based on condition data obtained in near-real time. Implementation of PBL will result in dramatic cost savings and improved weapon system availability. PBL focuses on inserting technology into both new and legacy weapon systems that will support increased stock availability, improved maintenance capabilities and business processes. It also involves integrating and changing business processes to improve the responsiveness of the logistics system. The Army's HIMARS weapon system is a PBL initiative, Section 912 Pilot Program, designated by the Department of Defense (DoD).

To support PBL, the HIMARS Program Office is defining capabilities such as enhanced prognosis/diagnosis techniques, failure trend analysis, logistics decision support systems, serial item management, automatic identification technology and data-driven interactive maintenance training. The UMD Portal initiative is designed to support LCCS, but will also enhance the characteristics of PBL. The ultimate intent of the portal initiative is to increase operational availability and readi-



Soldiers from Charlie Company, 3/27 Field Artillery Regiment, Fort Bragg, N.C., get ready to aim their High Mobility Artillery Rocket System (HIMARS) as part of the Rapid Force Projection Initiative field experiment (RFPI). This experiment is being used to test new equipment and its usefulness with light forces in the field. Photo by Spc. Russell J. Good.

ness throughout the weapons system life cycle at a reduced cost without adversely affecting readiness. Data visibility and enhanced data management are key to solving the Army's ability to implement PBL on a grand scale. It must also include data accessibility at the vendor level. After high-level analysis of applying PBL to the HIMARS sustainment strategy it appears that an Access Portal architecture implementation within the electronic Supply Chain Management (eSCM) infrastructure can support these integrated scenarios — with some issues to be worked by the Program Office before implementation.

A crucial goal of the project is to develop best practice supply chain strategies for HIMARS, placing an emphasis on real-time links between key suppliers and end users that will result in a significant reduction in time for supply/resupply and more accurate demand forecasting. The UMD plans to design the enhanced supply chain architecture leveraging OSD and Air Force efforts, to optimize the physical, distributed network of warehouses, distribution centers, stocking points and transport flows. To accomplish this, the UMD technical team in conjunction with software integration companies, will build and test an initial HIMARS Supply Chain Portal capable of executive decision-making support, advanced planning/forecasting and workflow automation. It will serve as a showcase for the Army's LMP effort.

The UMD's HIMARS project will be conducted in five phases beginning with an accelerated research and planning effort taking less than 90 days. The University technical staff has only weeks to fully recognize and adapt military supply procedures and functions into standard commercial practices that can be networked and programmed into COTS applications. The Supply Chain Strategy Development phase will begin even before the research and planning efforts are complete, taking less than five months. Inputs from the initial phase will be used to construct a HIMARS Supply Chain Network Map that defines key actors, supply nodes and interdependencies. This map will be accompanied by a strategy to optimize HIMARS/industry interactions, product/information flows and chain-wide business rules.

Since HIMARS is a highly deployable system mapping supply chain alternatives, it provides a real challenge for software developers to build a network that is constantly moving toward multiple military and political objectives. Unlike commercial enterprises that are built around stable nodes, the HIMARS supply chain is highly mobile.

Business rules are constantly changing due to operational and political diversions, which affect supply flow and distribution points.

Based on the Network Map developed in Phase Two, detailed functional specification of the prototype Supply Chain Portal will be developed as the third phase. The functional specifications will identify the entire portal configuration with linkages to specific data systems and the specific software to be used.

A prototype Supply Chain Portal, employing Collaborative Forecasting, Advanced Planning and Enterprise Resource Planning (ERP) software, will be rapidly designed, stood up in a test environment and delivered to a sample of key HIMARS users. This will mirror Army LMP efforts directed by the Army Material Command (AMC). The HIMARS Program Office is working closely with AMC's LMP vendors and architect designers to insure collaboration. Synchronization between the two efforts is key to completing Phase Four.

Success is achieved when UMD delivers a HIMARS Supply Chain Roadmap Document defining the processes and policies the Army must follow to maximize the investment on a portal strategy. This document is accompanied by a prototype access portal with applications and capabilities to evaluate contractor logistics support benefits and risks. The success of the project is expected to galvanize interest from the U.S. military to portal applications for developing future ERP initiatives.

Total Life Cycle Management (TLCM) is a critical business process to the HIMARS Program Manager and the future of Army acquisition logistics. A current review of commercial supply chain portal architectures reveals that TLCM is an end-to-end business process that flows across all levels of the organization. It also interacts at the vendor and sub-vendor level. In the Army today, the TLCM process is disconnected and incomplete, which is partly due to stovepiping and the lack of cross-functionality among logistics providers. In the UMD portal architecture the TLCM process will be completely integrated with business processes enabled by ERP solutions (such as SAP). Thus, HIMARS TLCM business processes must be managed as part of the overall Army ERP integration effort.

The HIMARS improved SCM efforts will be realigned as an end-to-end business process that is implemented jointly with all other business processes in the Army integration domain. On the management side, eSCM implementation (and all variants) will be managed by the Program Management Office in accordance with the architectural guidance from the LMP working group. Under this architecture the Army can avoid customization of SAP solutions and COTS applications. Instead, the Army can focus on reengineering business processes to align with COTS solutions and industry best practices. This trade-off is cheaper in terms of avoiding the costs of software development, long-term support and upgrades. In addition, it will also enable the Army to drive architectural design toward a single solution and enhance its investment. This recommendation results from the success of the HIMARS eSCM portal application.

Today's eSCM technology can pave the way for rapid logistics automation and true integration of information across multiple military functions, even in a legacy IT environment. Portal technology provides the extended enterprise with a personalized single point of entry to enterprise information via the World Wide Web. But the real potential for the technology goes beyond the portal as just a window to the Web. Behind the HIMARS eSCM portal will reside a set of applications that offer a wide array of technologies developed over the past decade and employed as an integrated suite of COTS mod-

ules. The eSCM suite combines sophisticated integration technology with powerful Web-based search, collaboration and categorization tools to simulate true integration of disparate Army IT systems and databases.

The eSCM modernizes the user's view and information process, while facilitating migration from legacy to modern IT — often transparently to the user. In facilitating modernization, the UMD eSCM technology incorporates modular integration design to enable plug-in replacement of application systems and databases as the system is modernized. Plug-ins use COTS integration modules capable of tying into virtually any database and application — even Army legacy systems, many of which are unstructured textual information sources. Because the technology provides for initial application in a legacy environment, users can anticipate more rapid development of business applications and early access to a fully integrated, commonly shared information warehouse. The HIMARS acquisition program has been a leader within the Army in developing and showcasing technology enablers to support advanced business applications, defining measurable performance metrics and reducing total ownership costs over system life cycle.

Applied globally to the military's expanded supply chain, eSCM technology can facilitate horizontal and vertical integration. Integration would apply to Army retail, wholesale, contracted operations, supply, maintenance, transportation and ultimately procurement (cross-functional integration), with controlled access to various levels of the Internet — corporate, enterprise and public domain. Other benefits to the military logistics enterprise community include enhanced end-to-end visibility of assets throughout the supply chain and concurrent access to federal and commercial supply data, resulting in streamlined requisition and other critical business processes.

Anticipated benefits of the eSCM Portal include increased adaptability to respond quickly in changing operational environments; ability to identify the best alternatives when unplanned events occur; increased customer satisfaction through shorter lead times; improved service; ability to provide customers with accurate updates and commitments; increased responsiveness and operating velocity due to the ability to manage inventory, processes and network design — not just the movement of goods.

Other expected benefits of the eSCM Portal include: enhanced operating efficiency from downtime reduction, workload leveling and proactive response to plan shortfalls, reduced inventory levels due to greater predictability, reduced uncertainty and improved control — all of which stem from being able to see the supply chain network all the way to the final customer — the Soldier.

Robert L. Sullivan is the Precision Fires Rocket and Missile Systems (PFRMS) Project Office Champion for Reducing Total Ownership Costs (RTOC) in Huntsville, Ala. He is a retired U.S. Air Force officer with service in the strategic missile commands. He holds a bachelor of science degree in Industrial Technology and Engineering from the School of Engineering and Technology, Southern Illinois University at Carbondale, Ill.

Robert B. Stevens is a senior consulting logistics analyst for the PFRMS Project Office in Huntsville, Ala. He is a senior Army logistician for the U.S. Army Reserve with 24 years experience and over a dozen overseas deployment tours worldwide. He holds a bachelor of science degree in Resource Management from Faulkner University and a master of science degree in Logistics Management from the Florida Institute of Technology. □

Teamwork Solves NMCI Problem



By Bob Bloudek

When the Navy Marine Corps Intranet first started being discussed, folks in the Naval Air Systems Command Weapons Division Technical Library at China Lake knew they were going to have a problem. The library subscribes to hundreds of electronic resources that are accessible to China Lake and Point Mugu personnel from their workstations via Internet Protocol (IP). Technical Library Director, Sandy Bradley explains, "With the legacy network, we had a firewall at each site we serve, one at China Lake and another at Point Mugu. Our vendors could verify a computer was physically at one of those two sites by checking the IP of the firewall. With the NMCI, we have a number of firewalls and switch points so there isn't any way to predict or specify which firewall our users will be routed through. Asking the vendors to allow NMCI IP recognition wasn't acceptable because it would open access to everyone on the NMCI network — which will eventually include the entire Navy. As NMCI workstations replaced legacy computers, library customers found they could not access all of the electronic resources they had come to rely on. We started hearing from them — and their complaints were legitimate."

A small team consisting of Bob Bloudek from the Technical Library, James Furnish from the NMCI Information Strike Force, and Larry Jenkins and Jeff Thatcher from the Information Technology/Information Management Department, set off seeking solutions. Since NAVAIR was one of the first Navy organizations to implement NMCI, we didn't have anyone else we could ask about how they solved this type of problem. We were able to get a lot of help from the Naval Post Graduate School Library, especially from Lillian Gassie who is the information systems manager. Students at NPS are able to connect to the library's Web sites from home though a proxy server. With that in mind, the team began exploring the possibility of using similar technology to solve the China Lake and Point Mugu access problems. The team was great to work with, Larry and Jeff know computer technology, James is an expert with the NMCI network, and Lillian is willing to share her experiences in setting up a proxy server. Everything just seemed to fall into place.

The team was able to secure storage space on a NAVAIR computer located outside the legacy and NMCI firewalls. A copy of EZ-Proxy, a software program written especially for libraries was evaluated. After a "little blood, sweat and tears" the software was installed and configured specifically to work with NMCI's security requirements. "The first attempts at testing weren't successful — neither were the second, third nor fourth attempts. We just kept working away," said Jenkins. "We would reconfigure the software and then we would test again — finally we were successful!"

Above left to right: Jeff Thatcher, Bob Bloudek and James Furnish check access to the NAVAIR Weapons Division Technical Library resources via an NMCI workstation in the library.

"The first attempts at testing weren't successful — neither were the second, third nor fourth attempts. We just kept working away!"

The proxy server and software now enable NMCI users at China Lake and Point Mugu to access the valuable electronic periodicals and databases available via the library Web site located at <http://www.nawcwpns.navy.mil/~tlibrary/>.

The technology is pretty simple, when an NMCI user clicks on a link; data goes from his workstation to an NMCI switch point (in San Diego, Hawaii or Norfolk) back to the proxy server at China Lake and prompts him for a username and password. When the data are entered, the proxy server directs the user to the proper Web site. Authorization is based on both the IP of the proxy server and the username/password. A legacy user can click on the same link; the proxy server has been programmed to recognize the user is from NAVAIR WD and simply passes him through to the vendor's Web site. Now that we can access these sites from our NMCI workstations, we won't have to maintain as many legacy computers. Many offices kept their legacy computers when NMCI rolled out because they needed access to the library resources. They didn't have that access with NMCI until our proxy server was implemented, but now they do.

This is a temporary fix for what was a serious problem for us. We will continue working related issues as they come up. Meanwhile, we are happy to answer questions and share our lessons learned.

Bob Bloudek is a Technical Information Specialist at the NAVAIR WD Technical Library, China Lake, Calif.

By Retired Major Dale J. Long, USAF

The Lazy Person's Guide to Voice Telephony - Part I

In today's world, most of us have three basic expectations: *Flip a switch and electricity will provide power; turn on a tap and you'll get water — and lift a telephone handset and you'll get a dial tone.*

Electricity, water and communications are the three main “flows” that keep modern society functioning. Over the next couple of issues, we will look at one of the main streams of communications flow: voice telephony. Originally developed in the 19th century, voice telephony became one of the killer applications of the 20th century. During the last 100 years, telephone lines have spanned the globe, linked most of the world, and served as the basis for later systems like the Internet. Its simplicity and effectiveness as a means of communication are the crowning achievements of modern technology.

Ease of use does not mean that it is simple technologically. Today, voice telephony involves a wide variety of technologies and protocols: circuit and packet switching, radiated and guided media, and analog and digital signaling, to name a few. But despite all the variations, vendors and equipment, you can pick up a phone anywhere in the world and call any other phone — if you know the number.

In recent years, telephony has been pushed out of the limelight by data and computer networking. Computer Help Desk technicians are greeted by office staff as saviors when they arrive to unstick a stuck PC. Telephone techs, on the other hand, get barely a nod as people walk past the closet where they are trying to figure out which of the 1,000 pairs of little blue and white wires on those old 66-blocks go to the phone on your desk.

So, this edition of the LPG is dedicated to all those people who make sure we can pick up a phone and talk to anyone, anywhere, in the world. We will start by looking at what it takes to connect the world with voice communications via circuit switching and guided (wired) media, the old traditional basis upon which telephony was founded. Once we have covered the basics, we will move on to wireless services and the latest trend in the voice world, voice over Internet Protocol (VoIP). But for now, and as usual when we examine any technology for the first time, let us wind up the Way Back Machine for a trip to the 19th century to see how it all started.

Telephony 101

Telephony is a system that converts the human voice to electrical impulses, transmits it and converts it to a tone that sounds like the original voice. The discovery that became the basis of the telephone came in 1831 when Englishman Michael Faraday

proved that vibrations in a metal object could be converted to electrical impulses. It took another 30 years until German inventor Johann Philipp Reis built an apparatus that changed simple sounds to electricity and back again in 1861.

As with any new technology there were people willing to tell everyone else that voice telephony was impossible. In 1865, the Boston Post opined: *“Well-informed people know it is impossible to transmit the voice over wires. Even if it were, it would be of no practical value.”* As with things like heavier-than-air flight, heart transplants and reliable overnight delivery, the pessimists were once again proved wrong.

The first practical telephones were invented by Elisha Gray and Alexander Graham Bell. Working independently, Gray and Bell both developed systems based on electromagnetic receivers with steel diaphragms. It was a tight race. Both men filed for patents at the New York patent office on February 14, 1876, but Bell got there first, beating Gray by a mere two hours. Even after the technical concept had been proven, there were still people who believed the telephone was of no practical value. In 1877, an unidentified New York financier allegedly told Bell that, *“The possibility of a private home telephone system throughout the country is out of the question. Almost the entire working population of the United States would be needed to switch [install] cable.”*

And, in what ranks up there with the poorest business assessments ever made, there is this famous quote attributed to an 1877 Western Union memo: *“This ‘telephone’ has too many shortcomings to be seriously considered as a means of communication. The device is inherently of no value to us.”* So, in response to Alexander Graham Bell's offer to sell Western Union the complete rights to the telephone for \$100,000, Western Union President Carl Orton replied: *“What use would this company make of an electric toy?”* Once Bell Telephone negotiated rights of way for its cables and started building its network, Western Union's days as the premier communications company in the United States were numbered.

The House that Bell Built

The fundamental concept of operations for telephone systems has been a dedicated circuit connecting callers. The first phones were primitive devices, little more than a box with a hole where you both talked and listened. In Bell's demonstration model, the two units were directly connected by a single pair of wires. There was no need for a dial, as there was only one other device connected. But for the telephone to become practical commercially, you needed some way to connect callers that didn't involve setting up a different hard-wired phone for everyone you might want to call. What developed in response was the telephone exchange.

The exchange involved one or more operators working at a large switchboard. Callers would signal the operator by tapping on the diaphragm with a pencil. As this didn't turn out to be particularly healthy for the physical condition of the diaphragm, Thomas Watson (Bell's assistant) attached a small hammer to the side of the phone box that callers could use to send the signal. The hammer was soon replaced by a magneto powered with a hand crank. Turning the crank would activate a signal at the exchange and the operator would answer and manually connect the caller to the intended recipient. The establishment of a temporary dedicated circuit for each call (circuit switching) became the primary process of telephony for the first 100 years or so. In the days of operator-assisted calls, this meant you would call an operator who

connected your call to an operator working in the exchange that serviced your party. This sometimes involved going through several different exchanges, so the process of calling got more cumbersome and unreliable as more exchanges participated.

The first telephone exchange was installed in Hartford, Conn., in 1877, and the first exchange linking two major cities was established between New York and Boston in 1883. The first automatic telephone switch that did not require manual operation was patented by Almon Strowger of Kansas City in 1891, but because of the perceived complexity of automatic circuit switching (and in some cases, simple inertia) manual switchboards remained in common use in many places until the middle of the 20th century. In the last 50 years, telephone exchanges have become pretty much completely automated.

Automated switching, which was developed in 1923 by Frenchman Antoine Barnay, allows callers to signal the network by dialing numbers on their phones using pulses generated by a numbered rotary dial. Some of us are old enough to remember sticking our finger in a hole on a wheel, spinning it clockwise until we ran into the little finger stop, and then letting the wheel spin back into place. How far you turned the wheel determined how many clicks the phone made. The clicks we heard on the old mechanical pulse phones were actually momentary disruptions in the current over the telephone circuit. The switch would count each set of current breaks and store each number mechanically until an entire number had been dialed. This required a rigid addressing structure to operate effectively and was the reason for our current system of area codes, local prefixes and the need to dial "1" when calling outside your local dialing area. Many modern tone-based pushbutton phones still have a setting for pulse dialing to accommodate old central office equipment.

In the "plain old telephone system" (POTS), once a dedicated circuit connects the call, your voice is transmitted by a 4 kilohertz analog wave form via a process known as frequency division multiplexing. In a multi-channel analog carrier system, one channel might run at 0-4 kHz, the next at 4-8 kHz, the next at 8-12 kHz and so on, with some of the edge frequencies within each band reserved as guard bands between each channel to keep the signals from interfering with each other. Why use 4 kHz bands? It provides enough bandwidth to reproduce a recognizable human voice. Further, each channel supports a range of signal amplitude (strength) that relates to a volume level. The amplitude level is limited, so no matter how loud you scream over the network it won't exceed a certain volume on the other end of the line. Together, this combination of bandwidth and amplitude is not quite enough for perfect voice transmission, but it's good enough so you can make out the words and recognize familiar voices. This level of service is known as toll quality voice.

Digital Evolution

As manual switchboards were phased out after World War II, we started moving from analog to digital telephony. Digital transmission offers a lot of advantages, including more efficient use of bandwidth, better error handling, enhanced management and control of calls. Virtually all telephone switches today are digital in some way. Most transmission facilities are digital, with the exception of the copper wire local loops serving some residences and small businesses.

Transmitting voice, an analog waveform, over a digital network

requires conversion of the analog signal into a digital format and back to analog on the receiving end. Telephone systems do this through a process known as Pulse Code Modulation (PCM). Harry Nyquist, an engineer at AT&T in 1928, determined that to convert analog voice to a digital format, send it over a digital circuit to reproduce high-quality analog voice at the receiving end, then sample the amplitude of the analog sine wave at twice the highest frequency on the line.

This means that we should sample at twice the highest frequency on our 4kHz toll quality voice channel, a rate of $4,000 \times 2$, or 8,000 times a second. If we do one more bit (or in this case, byte) of math, 8,000 samples per second times 8 bits per byte equals 64,000 bits per second, or 64 Kbps, which is a voice-grade digital channel, the basic building block of our modern digital circuits. Sampling 8,000 times a second means that the sampling process must take place at intervals of 125 microseconds. Each sample is coded into an 8-bit digital value, the resulting 8-bit bytes are woven together (interleaved) by multiplexers, and sent across multi-channel digital circuits (e.g., a T1 circuit with 24- 64 kHz channels). These bytes are directed and redirected by switches across whatever circuits connect the switches in the network and are ultimately decoded back into an analog form on the receiving end. The decoded signal is only an approximation of the original analog signal, but it is close enough to be recognizable and understandable to the human ear.

Precise timing is the critical piece of this puzzle. The phone network must be in a position to accept, switch, transport and deliver every byte of voice precisely every 125 milliseconds (ms). That means that delay (latency) must be minimal and any variation in delay (jitter) must be virtually nil. Unlike the packet-based data sent by computer networks, voice quality will not readily survive latency or jitter.

Phoning Home

Telephones are relatively simple in design, but allow access to one of the most complex networks in the world. They have five main components. Three of the five are easy to pick out because we use and see their functionality every day. The transmitter converts acoustic energy (the sound of your voice vibrating the diaphragm) into electrical energy. The receiver converts electrical energy into acoustical energy (the voice coming out of the phone). The signaling device (key pad, dialing wheel, etc.) is used to get the network's attention and identify the destination. The two less obvious technologies that make this all work are the transformer and the balance circuitry. The transformer electrically separates the receiver from the transmitter. The transformer allows you to talk and listen at the same time. Because of the transformer, telephones operate in full-duplex mode, which means that the circuit is two-way all the time.

The balance circuitry reduces sidetone, which is what you hear when you speak into the microphone and hear yourself through the speaker. This allows the person speaking to get some feedback about what they sound like without drowning out the person on the other end of the line. If you want some idea of what your sidetone would sound like without the balance circuitry, have someone else in your house pick up an extension while you are on the phone. On most home systems, they will sound much louder than the external caller due to proximity.

Modern phones use much more technically sophisticated signaling

and switching systems than the original models, but the basic principles are the same. When you pick up a handset it generates a loop current in the circuit. This current is powered by batteries in the telephone company's central office. That is why even though your power goes out, telephones that don't depend on your home's electrical system for power may still work. (I recommend you always keep at least one wired phone in your house. Cordless phones don't work during blackouts.)

When your phone generates the loop current, it is detected by a line scanner and the central office connects equipment to your line and sends you a dial tone. At the same time, a dual-tone multi-frequency receiver is activated and connected for your line to detect the tones generated by the keypad or interpret the clicks. Once you enter all the numbers, they are entered in the switch's memory. Another central office program reads the numbers, determines the best route for your call and sends a command to the switching matrix to establish a connection. That, in a nutshell, is how a telephone works.

Telephone Services

There are two basic ways to acquire phone service: buy it line by line from a vendor or buy a switch and set it up yourself. The first is what most of us do. The wiring in our house is connected to a local exchange carrier's central office via a twisted pair. Small organizations that need more than one line (small businesses, families with multiple teenagers, etc.) can buy lines individually or in bulk. Larger organizations may buy or lease a phone switch that is dedicated to their organization. Military bases often have telephone exchanges that rival small cities. But the military is not unique in owning and operating phone systems. Most large organizations that occupy any significant amount of facility space buy and run their own switches. There are a few reasons for this.

First, while individual lines may be relatively inexpensive, buying 1,000 lines when only 20 percent of your 1,000 people may be on the phone simultaneously will cost more than leasing trunk lines and sharing them through a private branch exchange (PBX). Second, when you control the switch, you control the services: voice mail, 911 service, caller ID, toll monitoring, auto-attendant features, calling restrictions, etc. You can tailor the services to your organization's business operations, which includes building full-featured call centers.

Third, in many cases it is simply less expensive to set up your own service. For example, any operation that relies on telephone contact with the public to conduct most of their business uses call centers. Having a telecommunications vendor build a call center can cost \$1 million and the recurring charges for even basic call center services start at \$30,000 per month. And you still have to pay for your phone service and provide staff to work the phones. Buying a digital PBX supporting 50 plus employees, that has enough capacity to handle 300 plus calls per hour (at 5 minutes per call), and includes an auto-attendant programmed in seven languages can cost about \$165,000. That price includes the cabling, switch, phones, initial programming and training. You will incur some cost for staff to support the system, but it is unlikely that it will exceed (or approach) what you would pay for commercial call center services. It is convenient to have someone else handle the technical details, but you pay a lot for that convenience. Other advantages of deploying your own systems include having consistent prefixes and number ranges for your organization's

components, managing your phone switches as part of your enterprise architecture, and ability to impose your own security constraints. Even systems for offices as small as six to eight people can be more cost effective over their life cycle. As with anything, look past the capital investment costs and calculate the cost difference over several years. (I use six years because it is just under the average age of the 133 PBXs in my current area of operations. Your mileage may vary.)

Call Me

Not only did the telephone spark a revolution in conducting business, it also contributed to sweeping social and cultural changes. The first telephone exchanges were run by male operators. Allegedly due to the arrogance and impatience of the male operators, telephone exchanges initially got lousy ratings for customer service. Because the work was indoors, had regular hours and didn't require a high degree of physical strength, Bell started hiring women as operators. They proved much more capable at customer service than male operators. Being a telephone operator was one of the first full-time jobs for women in the workplace. In combination with the filing cabinet and typewriter, the telephone was instrumental in the large-scale integration of women into the nation's business environment.

Not everyone was thrilled with the proliferation of telephones. Allowing more people to converse more often and at greater distances may be great for a capitalistic democracy, but if your power depends on absolute control of what information your population receives and exchanges, you might be a little wary. Joseph Stalin, one of the more famous experts in the field of totalitarian control, had this opinion of the telephone: *"It will unmake our work. No greater instrument of counterrevolution and conspiracy can be imagined."* Many countries tightly controlled or monitored access to telephone systems throughout most of the 20th century. Some still do.

Final Words

In considering any two-way connecting technology, the telephone, e-mail or radio, they are swords that cut both ways. You can reach out around the world, but you can also be intruded upon through constant access and accessibility.

Perhaps this is why Mark Twain said in 1890: *"It is my heart-warm and world-embracing Christmas hope and aspiration that all of us — the high, the low, the rich, the poor, the admired, the despised, the loved, the hated, the civilized, the savage — may eventually be gathered together in a heaven of everlasting rest and peace and bliss — except the inventor of the telephone."*

Twain lived at the end of an age where correspondence between great thinkers documented some of the greatest decisions of history. The telephone is an ephemeral medium. How much has been lost because it was spoken over the phone instead of documented in writing? To a writer like Twain, this loss would be a tragedy. As with any technology, its value lies in the use we make of it, and we are better off with it than without it.

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

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; and (N00104-03-A-ZE90) for Adobe products; (800) 295-4239; Also (888) 826-2394

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; and (N00104-03-A-ZE92) for Adobe products; (800) 999-GTSI

HiSoftware, DLT Solutions, Inc. (N00104-01-A-Q570) for HiSoftware (Section 508 Tools); Small Business; (888) 223-7083 or (703) 773-1194

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) 312-6704

Softmart (N00104-02-A-ZE84) for Microsoft products; (610) 518-4000, ext. 6492 or (800) 628-9091 ext. 6928

Software House International (N00104-02-A-ZE86) for Microsoft products; Small Business Disadvantaged; (800) 477-6479 ext. 7130 or (703) 404-0484

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: 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

Adobe Products
<http://www.it-umbrella.navy.mil/contract/enterprise/adobe/adobe-ela.shtml>

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

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

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

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

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

Novell Products
<http://www.it-umbrella.navy.mil/contract/enterprise/novell/novell.shtml>

PeopleSoft USA, Inc
<http://www.it-umbrella.navy.mil/contract/enterprise/peoplesoft/peoplesoft.shtml>

Schlumberger
<http://www.it-umbrella.navy.mil/contract/middleware-esa/schlumberger/index.shtml>

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

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

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: Pending New GSA Schedule

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:

	<u>IBM Global Services</u>	<u>GTSI</u>
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,
	Network Appliances	Network Appliances
Networking	Cisco	Cisco, 3COM, HP, Enterasys, Foundry, Segovia

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 Link

GTSI and IBM: <https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp>

The U.S. Army Enterprise Software Initiative BPA DEAL-S 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

<https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp>

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

<https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp>

The U.S. Army Enterprise Software Initiative BPA AMS-P 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

<https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp>

The U.S. Army Enterprise Software Initiative BPA DEAL-I/D 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

<https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp>

**15 years of Delivering Significant Savings
to DON and DoD customers**



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
SPAWARSSYSCEN 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