

# Interview with Robert J. Carey

## DON Deputy CIO



**Mr. Robert J. Carey serves as the Department of the Navy Deputy Chief Information Officer for Policy and Integration. Reporting directly to the DON CIO, he is the principal adviser to the CIO. Mr. Carey is responsible for managing and leading the DON CIO staff and developing strategies for achieving information management/information technology (IM/IT) enterprise integration across the DON.**

*CHIPS: What is the DON Information Management/Information Technology (IM/IT) Strategic Plan 2004-2005? Why is it important, and who should read it?*

**Mr. Carey:** The importance of the plan can't be understated because it lays out the high level roadmap as to where the Navy and the Marine Corps will be going in the broad context of information technology.

Navy and Marine Corps Deputy CIOs contributed heavily to the plan, and careful attention was paid to ensure the goals and objectives of the plan support the Department's larger vision for the warfighting capability of the future. So the goals and objectives in the plan are aligned with our warfighting capabilities documents like Naval Power 21, Marine Corps Strategy 21 and Joint Vision 2020.

We linked these documents to the IM/IT Strategic Plan so it is clear that IM/IT is an integral enabler of every Naval program and initiative. So, for example, if you are in logistics, aviation or a Marine on the ground, the DON IM/IT Strategic Plan will help you understand the IM/IT capabilities the Department is building that will help you do your job.

The plan is also aligned with DoD's IT plans and with the suite of legislative statutes and the Office of Management and Budget (OMB) guidance that govern IM/IT. It is not an execution plan; it doesn't go down to the program level. But it is something that everyone in the Department's IT workforce should read to gain a fundamental understanding of the types of things the Department as an Enterprise is trying to accomplish. Because this is where we should be shaping investments tied to corporate management and functional objectives.

The next step is to strengthen the tie between the IT capabilities in the strategic plan, IT programs and investment decision making, and we are working with the Navy and Marine Corps to improve this linkage.

*CHIPS: The list of DON IM/IT initiatives is extensive, how does the DON CIO prioritize these programs in order of importance?*

**Mr. Carey:** Yes, the list is long. Because of the way programs are funded, we are not at a place yet where we can say: 'Let's fund

### **Robert J. Carey**

*Prior to his position as DON Deputy CIO, Mr. Carey served as the DON CIO eBusiness team leader from February 2000 through June 2003 and Director of the DON Smart Card Office from February through September 2001.*

*Carey began his career with the Department of the Army in October 1982 at the Aberdeen Proving Ground, Md., where he was a test director managing developmental and operational testing of small arms and automatic weapons. In February 1985, Carey went to the Naval Sea Systems Command assigned to the Surface Ship Sonar Dome Program Office, managing the Rubber Keel Dome project. Over the next five years he held various positions in the Undersea Warfare Directorate such as the AN/SQS-53C Sonar Project engineer and director of the Surface Ship Sonar Dome Program Office. Following his return from active duty in Operation Desert Shield/Storm, he was a senior systems engineer on the staff of the Program Executive Office for Surface ASW Systems.*

*From January 1995 through August 1998, Carey worked in undersea weapons systems engineering, culminating in a tour as the chief engineer in the new Undersea Weapons Program Office, PMS 404 where he managed systems engineering efforts for all Navy torpedo programs. In August 1998, he served as Deputy Program Manager for PMS 404 where he managed nine ASW weapons programs including Foreign Military Sales.*

*Carey has a Bachelor of Science degree in engineering from the University of South Carolina and a Master of Engineering Management degree from George Washington University. Mr. Carey has been awarded the Navy Civilian Meritorious Service Award and the Navy Superior Civilian Service Award.*

*He is a Commander, Civil Engineer Corps in the U.S. Naval Reserve serving as a Contingency Engineer for the U.S. European Command.*

ATMs-at-Sea but not Enterprise Resource Planning.' Our greatest opportunity to influence IT investment decision making, lies in strengthening the alignment of claimant IT programs with the Department's vision for the Enterprise, and we are making tremendous progress. In the past, our major opportunity to influence the IT budget was just prior to its submission, but we now

can influence the budget throughout the Planning, Programming, Budgeting, and Execution (PPBE) process by releasing policy and guidance documents at strategic points throughout the PPBE cycle.

For instance, during the last budget review cycle we issued DON CIO IT Policy Guidance for FY 2004 Expenditures in coordination with the Assistant Secretary of the Navy (Financial Management and Comptroller (ASN (FM&C))). This guidance tied programs' authorization to expend funds to specific national, DoD and DON IT policies and made every organization's comptroller office responsible for enforcement. Similar guidance for FY 2005 will help make sure that commands are working on things that are aligned with the Department's IM/IT strategy. Another example of progress in this area, is the continuing work by the DON's Functional Area Managers (FAMS) to rationalize and consolidate the DON's software portfolio.

Dave Wennergren, the DON CIO, co-chairs the FAM Council with Vice Admiral Albert Church, Director, Navy Staff. Together they help shape the guidelines about how applications are going to be examined, measured and renewed. Programs that are not meeting the goals and objectives that the Department has laid out can be modified. The Clinger-Cohen Act also helps shape the level of initiatives.

As acquisition programs come up for milestone decisions, Clinger-Cohen requires agency CIOs to review them for security and architectural compliance. As we move into net-centricity all of these programs and their applications and databases must work together. Requirements for security, interoperability, authoritative databases, collaborative environments, and efficient use of limited resources demand that agencies shift away from the traditional paradigm of decentralized IT decision making to Enterprise solutions.

*CHIPS: What are some of the DON IM/IT capabilities that the DON CIO has fostered?*

**Mr. Carey:** There are quite a few; I'll give you a short list, for example, cryptographic logon. We are the champions of smart card technology with Common Access Cards (CAC) in the Department. Since last summer, the DON CIO staff has been logging on to NMCI workstations with the CAC card. This eliminates the need to remember passwords. One of the benefits of the smart card is the ability to log on to the network securely using your PKI (Public Key Infrastructure) credentials contained on your CAC card. Once fielded, the Navy Marine Corps Portal will be your window to the world, and your CAC will be the key that authenticates your identity to the portal, giving you access to all of the applications that you need to do your job.

Another initiative is Internet Protocol version 6. IPv6 is the next state of the Internet Protocol, and it is going to require a fair amount of change. Internet use has exploded, but the number of IP addresses on the current IP is finite. IPv6 will help us deal with the exponential growth of the Internet. As we move to network-centric warfare and Web services, using the current IP, our servers, routers, PCs and Web sites would have addressing issues.

In a policy memorandum, the DoD CIO mandated the transition to IPv6 by FY 2008. Transition is a few years off, but it is a strategic initiative that the DON CIO is working with the DoD CIO and the Defense Information Systems Agency (DISA).

Voice over IP (VoIP) is an exciting technology with huge opportunities to explore. The Naval Sea Systems Command (NAVSEA) has already implemented a VoIP network-based telephone system. This technology has wide application across the Department. We will do a business case analysis to determine the best application for VoIP; and we are championing the examination of VoIP as part of a greater telephony strategy, so that we understand its integration with the "plain old telephone system," commonly known as POTS, and with wireless devices like cell phones and Blackberries. We are examining where it makes sense to distribute converged devices like Blackberries, other PDAs and cell phones for people to do their jobs.

We are working with the Navy and Marine Corps to develop an Enterprise portal capability. This is something we must have to provide a common framework for information sharing across the Department. When you log on to the NMCI and you click on the Internet icon, you will be on the Navy Marine Corps Portal. It will provide access not only to your applications but also options like chat rooms, a global directory and other information that you will need. Underlying this simple concept is a lot of work — singling out databases, applications and access paths — to provide seamless, near real-time access to the authoritative data and intellectual capital of the Department.

Other portals will become aligned with the Navy Marine Corps Portal so we can share content across the Enterprise. Ultimately, we look to commands to stop spending precious resources on the latest greatest portal; and focus instead on delivering the quality, authoritative content, they need to share. We want commands to be spreading knowledge and creating knowledge warriors on the pointy end of the sword — from Iraq to the Naval Medical Center in Bethesda.

We are also working on XML naming conventions. XML is quickly becoming the cornerstone between legacy applications, data and Web services. We have created taxonomies within XML that allow people to identify, tag and create naming conventions so that the word 'ship' means the same thing every time you see it. XML is critical for moving to net-centricity, enterprise-wide services, authoritative data and knowledge on demand.

I have touched on just a few of the Navy's IM/IT transformation initiatives. I encourage all of our readers to go to the DON CIO Web site at <http://www.doncio.navy.mil> and read the Department's IM/IT agenda — the DON IM/IT Strategic Plan.

*CHIPS: Getting back to IPv6, is DoD waiting for industry's lead to make the leap to IPv6?*

**Mr. Carey:** Today, industry and DoD are both moving toward the IPv6 standard. The ideal would be that industry would work the issues, and we would adopt them as soon they were done. Currently, this does not appear to be the case. DoD has made a

serious commitment to transition to IPv6. Our goal, defined by John Stenbit, former ASD (NII)/DoD CIO, is that we will have this capability by 2008. We are working toward this. DISA and the other Services are working on this. We have guidance that says we will buy devices that are IPv6 capable so that when the time comes to make the shift our devices can be used. In some ways DoD is leading industry because we foresee the real need to move to IPv6, and have taken positive steps to get there.

*CHIPS: Do you think commands will need to make a significant investment to transition to IPv6, similar to the Y2K bug issue?*

**Mr. Carey:** No. I foresee, if this is done correctly, that as you normally refresh your technology, hardware and software, whether you upgrade or buy new — you will have a device or application that is IPv6 capable. So you will eliminate the need for a stand-alone investment to bring your technology up to the IPv6 standard. I think some people have fears that there is a huge bill associated with this transition. The cost will be affordable when you consider that you are going to do a tech refresh anyway.

*CHIPS: How does the DON CIO work with the other Service CIOs to ensure that solutions aren't duplicated but interoperable?*

**Mr. Carey:** David Wennergren and I have a very close working relationship with the other military Department CIOs and their staffs. When one of us finds a victory we are very quick to share. We meet with the Deputy Assistant Secretary of Defense (Deputy Chief Information Officer), Priscilla Guthrie, on a biweekly basis.

The purpose of these meetings is to understand from the DoD perspective where we need to be going and what we need to be sharing. One example of an interoperable solution produced by the DON CIO is the OMB Exhibit 300, Capital Asset Plan and Business Case tool. The Exhibit 300 is a lengthy 25 to 50-page report on all major IT systems that everyone in DoD has to complete. The tool we created helps a program manager better understand what OMB is looking for in the content of the various sections of the 300 exhibit and how OMB would score an answer. DON IT programs realized significant improvements in OMB scores since we began using the tool.

The Army was so impressed that it has adopted our work as a best practice and used the tool to prepare its reports for the last two years — a huge payoff in terms of not duplicating something that was already done.

We participate on the DoD Executive Board and other boards in the federal government like the Federal CIO Council. We work to share our best practices not only with the other Services but also throughout government. We all know that we don't have the resources to recreate solutions so that if the Army, Air Force or another government agency has built a best practice on something — we will use it.

*CHIPS: Does the DON CIO have a role to play in Homeland Security?*

**Mr. Carey:** Absolutely. We have a huge role to play. Since before the Department of Homeland Security stand up, we have been

managing the DON Critical Infrastructure Protection program and Dave Wennergren has been the Department's Critical Infrastructure Assurance Officer (CIAO) reporting to OSD. Dave is the link to the DHS CIO in terms of how vulnerable the DON IT infrastructure is in regard to homeland security.

We conduct NIVAs, Naval Integrated Vulnerability Assessments, and look at an integrated view of the parameters of a Naval base, the force protection plan, its dependencies on public utilities that come from outside the fence, network defense and its overall posture to understand where the weaknesses are. We have conducted NIVAs at Navy Region Southwest; Southeast; Oahu, Hawaii ... and we get an understanding of the relationship between the local government services and the Naval installation.

We integrate the cyber view with the force protection view and assess the base's reliance on commercial infrastructures and services outside the fence to get an integrated sense of what local commanders should be concerned about to assure mission readiness. For example, if there were a building that housed the Internet connections for the entire base 50 yards from the fence line, wouldn't you want to know that it wasn't the best location for a building with the vital Internet connection for the whole base?

We have a NIVA team going to Italy this October to look at the support activities in Naples and Gaeta. When we did a NIVA in Hampton Roads, the commonwealth of Virginia engaged the DON CIP team to better understand what it could be doing to improve its security posture.

With this information an organization can decide if it needs to improve so that in the event of a terrorist attack or disaster such as hurricane (because a hurricane can cause as much damage as a terrorist attack), it is prepared. We look at how Navy assets can work with public services to get back in business.

*CHIPS: Would the DON CIO be able to conduct a NIVA for any state?*

**Mr. Carey:** Yes, any state with a significant Navy presence. We have been asked by several members of Congress to work with Naval installations. The Hawaii Congressional delegation wanted us to help them help themselves because they realize how heavily dependent Hawaii is on the Navy. The South Carolina Congressional delegation understood what we had done in Hawaii and other states, and asked us to study the bases and report any of the issues we found so they could prepare in case of an attack or natural disaster.

*CHIPS: Sandra Smith's CHIPS articles on the IM/IT workforce always draw a lot of reader interest. What message do you have for the military and civilian IM/IT workforce?*

**Mr. Carey:** My message is that the world is changing — and that is not news to anyone in the IM/IT workforce — uniform or civilian. The CNO, Admiral Vern Clark is developing a human capital strategy for the entire Department. He is working with Secretary England to determine how we are going to best use the people that we have, and the IM/IT workforce is a component of the strategy.

We examine the skill sets the workforce has, what they are used for, what skills we need, whether there is a path for growth, what career path should be followed — these are things Sandy is working on to ensure that the IT workforce is viable and properly skilled to meet current and future needs. We also look at where technology is going and what training is required to attain the certifications the workforce will need to have a certain level of competency and credibility as technology and job requirements change.

The acquisition community has done a fabulous job of laying out certification levels, training curricula and requirements. To a large extent the IT workforce has done this, but we need to go a bit further in defining accreditations and certifications that allow workers to build a pedigree and compete for different jobs — jobs that will make great use of these skills sets.

*CHIPS: I am still surprised by the number of people who think that the NMCI is just for secure e-mail. What are some of the capabilities that will be populating the NMCI once cutover is completed?*

**Mr. Carey:** Currently, there are about 200,000 users with the authority to deploy up to 360,000. To think that this is only an e-mail system is a misnomer. NMCI is the highway system for information sharing in the Department. It is an enterprise asset spanning the Navy and Marine Corps. NMCI is the fundamental underpinning of how we intend to use IT to execute the Department's mission.

The NMCI is one of the most secure networks in the world. It has dealt with a few viruses recently in as little as a couple hours where industry experienced loss of service. With NMCI we can deal with security in a uniform and consistent manner across the Department. Spending is now controlled. It has also provided a performance measurement mechanism for IT where we didn't have one before. The ASN (FM&C) is very excited about the NMCI because the IT budget is over \$6 billion and prior to NMCI no one could accurately say how much the Department was spending on desktop IT or information services.

The NMCI gives the Department an enterprise portal. We can't have an enterprise portal without an enterprise network. With NMCI we have integrity and consistency of information deployed across the Department. We can have authoritative databases and file sharing access. NMCI provides the ability to have enclaves, for example, the Naval Nuclear Propulsion community of interest. They have information that is not germane to the rest of the Navy. However, it will be on the NMCI on their portion of the network. So they are on the NMCI, but they are able to keep information secure within their community. This is unclassified information, but it is information only they need to know.

Another consideration is that we can control the desktop — we can have the same Gold Disk set of applications running on everyone's desktop, which makes technology updates easier. Completing the NMCI hasn't gone as quickly as we would have liked, but when it is complete it will be the largest intranet in the world.

Looking to emerging technology, NMCI allows us to consider whether we want to leverage this huge network to convert commands to VoIP. So we don't have to pay a public telephone service

or long distance carrier, we can use our own network. I don't know to what extent we will do this, but NMCI gives us the flexibility to consider it. Cisco uses VoIP in all its facilities worldwide, but outside its facilities, Cisco uses another vendor's connections to carry cell phone signals back to the office. Because of the Navy's desire for security, we could use DISA pipes or pipes provided by a vendor with the required security, but if we choose we could use the NMCI.

***We will have to start recognizing and rewarding people for not building their own mousetraps, but for finding the best one already being used and adopting it instead.***

*CHIPS: What does Enterprise IT in the Department really mean?*

**Mr. Carey:** When Dave Wennergren and I talk about the Enterprise we open our presentation with three pictures of an enterprise: the Navy aircraft carrier, the USS Enterprise (CVN 65); the *Star Trek* Starship Enterprise and the Space Shuttle Enterprise. The point is that it really depends on who is the audience, doesn't it? If you are at the Department level like I am, I view the Enterprise as the Navy/Marine Corps team — all 1 million of us. If I am in the Navy, I view it probably as the blue side, and if I am in the Marine Corps, I would probably view it as the green side. None of these are wrong.

In the past, IT in the Department has been very much decentralized in how it is managed. However, we have learned that it makes sense to centralize IT. As we move toward more Enterprise activity, more centralization, we will have more and improved efficiency. Let's talk about the ESI, for example, the Enterprise Software Initiatives licensing agreements. This is where I can best maximize the buying power of the Department by maximizing the customer base at the DON level. My definition of enterprise is looking at the greater good where it is appropriate. You would look at the greatest application or expansion until it doesn't make sense anymore. This is a concept that is foreign to most of us.

That is why Enterprise IT may be hard words to swallow if you were a NAVSEA program manager, which I was, and you were paid to solve a program problem. When you defined the problem within the enterprise of NAVSEA, things got really hard and if you defined the enterprise as the Navy, things got an order of magnitude harder. If you defined it in terms of the Department, your eyes probably crossed — it was just too hard. We need to understand which problems really call for solutions at the DoD or the DON Enterprise level and how to recognize when a federation of multiple solutions might make more sense.

And we need to put reward mechanisms in place that recognize folks who are solving issues on behalf of the Enterprise. There is a fundamental change in culture and mindset that must take place as we move into the work of NCW and Enterprise services. We will have to start recognizing and rewarding people for not building their own mousetraps, but for finding the best one already being used and adopting it instead.

**CHIPS**