



Interview with Diann L. McCoy

DISA Principal Director for Applications Engineering

Diann L. McCoy is the Principal Director for Applications Engineering. She is responsible for engineering information systems to provide command and control, and combat support capabilities to the nation's warfighter. She earned a Bachelor of Science degree in Mathematics from Wright State University in 1974, and a Masters of Science degree in Logistics Management from the Air Force Institute of Technology in 1978. She was selected for her current position in September 2000. Her awards include the Presidential Distinguished Executive Rank Award, the Technology Award for Government Leadership, the DoD Distinguished Civilian Service Award, the Meritorious Civilian Service Award, the Presidential Rank of Meritorious Executive Award, and the Certified Professional Logistician from the Society of Logistics Engineers.

CHIPS: When talking about Defense Transformation in terms of the asymmetric threat spectrum (denial of service, insertion of erroneous information that could cause loss of confidence in official networks/systems, seizure of a network/system for criminal/terrorist purposes, malicious code, etc.) How is DISA responding?

Ms. McCoy: An asymmetrical threat can apply to more than just network attacks; it may apply to more than just the DoD critical infrastructure; the nation as a whole may be impacted, i.e., power plants, critical utilities, etc. While we engage in this type of security, our DISA focus is on the networks for DoD. In a general sense, DISA has the GNOSC, the Global Network Operations and Security Center. It isn't under my direction but their responsibility is to look at the activities that are occurring on the network, assess them and respond appropriately. We do this in conjunction with the JTF-CNO, Joint Task Force-Computer Network Operations, U.S. Strategic Command. The JTF-CNO is led by Maj. Gen. James D. Bryan, U.S. Army, who is dual-hatted as the Vice Director of DISA and Commander of JTF-CNO. In Applications Engineering, we provide many of the capabilities and applications used to analyze the information, to identify trends or activities that could lead to potential denial of service on the network. We are engaged in developing tools and capabilities that will allow us to understand what activity may be occurring and producing methods that will allow us to respond. Everything DISA designs, builds and operates, incorporates required measures to protect against information warfare attacks.

CHIPS: I've read comments from top DoD and DON leadership that there is concern from an information warfare perspective that there is potential for a terrorist/criminal threat that could bring down the whole DoD architecture. With all of DoD and federal agencies on high alert, do you think a threat of that nature is likely to occur — the worst-case scenario?

Ms. McCoy: No, I don't believe so. One of the approaches we use to protect our environment is Defense in Depth, which means you have multiple layers of defense and diverse routing capability so if you lost an application or a communications capability, you still have access to other available capabilities — voice, data, Defense Red Switch Network, VTC, etc. The diversity and robustness in each of these networks or systems comprise the larger Defense Information Systems Network (DISN). You might have an isolated incident, but in terms of vulnerability of the entire system, I think that is highly unlikely. One of the reasons why we

have the DISN is for its positive control and accountability — that's why DISA manages the DISN.

CHIPS: Do you mean if everything else fails we can always rely on the DISN?

Ms. McCoy: The DISN has successfully functioned through several major events that degraded Internet performance. More specifically, what I'm saying is because we have diverse routing and multiple paths, and the means to move information, either voice or data, we have redundancy so we don't have to depend on a single way to communicate. Also the physical and electronic security is more robust than a typical network. In Applications Engineering, we provide some applications that allow us to monitor and analyze what is happening over the network. The Network Services organization actually designs and develops these networks with layers of Defense in Depth protection built in.

CHIPS: Secretary Rumsfeld has stated numerous times that information technology is the enabler behind Defense transformation, but isn't this a natural progression for military operations to rely on IT due to the technology advancements of the last 10 years, especially?

Ms. McCoy: The Secretary is looking not just at the technology per se, but the way it is employed in a joint environment to provide a quantum increase in capability to meet the operational goals of the transformation. What we do is leverage that technology to make it work in a warfighting environment. Given the IT capabilities we have today — we can do things differently; and our methods of operations are tied to the type of IT available. For example, we manage the Global Command and Control System, GCCS, which provides the common operational picture of the battlespace. It gives the warfighter a situational awareness of what is happening and through technology we get better information flow and, more timely information, which gives the decision makers a better opportunity to respond to whatever is happening. Technology enables us to get closer in time to what is happening in the battlespace, as well as having a greater awareness of what is in the battlespace, a greater awareness of what capabilities we might have to bring into that particular environment — and what the status is of those assets.

CHIPS: Is there any one technology or system that is key to linking command and control for joint fighting capability?

Ms. McCoy: I think one of the cornerstone joint applications is

the Global Command and Control System, and we are incorporating multiple technologies and applications in GCCS. The most important feature of these joint capabilities is they have to be secure and interoperable. On the application side, they have to be able to share data in a certain way so that data has the same meaning, and in a secure way so that it cannot be compromised. This is central to Secretary Rumsfeld's joint command and control initiative — the key being joint and interoperable capability. This is what DISA is in the business of providing every day.

CHIPS: One of the things Dr. Myers (Principal Director, Deputy Chief Information Officer, Department of Defense, CHIPS Summer 2002, "Power to the Edge, the Transformation of the Global Information Grid," www.chips.navy.mil/archives/02_Summer/authors/index2_files/power_to_the_edge.htm) stated that is so important to Combatant Commanders is their confidence in the authenticity and timeliness of data.

Ms. McCoy: What you are really talking about is the issue of latency and that is very important. One of the things we are focusing on with the GCCS is providing near real-time data, so decision-makers have the most current information and don't have to gather and synthesize a lot of information. This lets warfighters shorten their decision-making cycle. Some of the tools and capabilities that we have today allow us to overlay information from various sources and fuse it together so the user has the most currently available information to act upon — that is very important. The other thing you asked about is the issue of data authenticity. We view both authenticity and data integrity as essential. We worry about these in every system we build and are also working on the DoD PKI as a key enabler to improve authentication and integrity in all DoD systems.

CHIPS: Is DISA involved in the Homeland Defense Plan?

Ms. McCoy: DISA as an organization is involved in Homeland Defense from several different aspects. Most importantly we support the communications needs of other DoD organizations with a direct Homeland Defense role to include nation-to-nation leadership communications. We also directly provide and support Presidential communications. We do other things in all the different disciplines to include support of whatever type transport mechanisms are required. In particular, in my area of Applications Engineering we are working on an ACTD or Advanced Concept Technology Demonstration, to work with JFCOM initially and then with NORTHCOM — whomever has the Homeland Defense mission. We would take this Homeland Security ACTD and develop a common operational picture and situational awareness for that Combatant Commander. The point is to take some of the things that we have learned under command and control and, see how they can be used to support DoD's role in Homeland Defense.

CHIPS: I spoke with a Congressional Liaison, who has worked on security matters for the House Armed Forces Committee and she said that she is very impressed with the DoD response to Homeland Defense and the Sept. 11 terrorist attacks. She indicated that federal agencies such as the FBI, FEMA, CIA, etc., could use the DoD model and that the national Homeland Defense strategy could also follow the DoD model. Is this feasible?

Ms. McCoy: In prior jobs that I have had I was involved in the larger federal community. I think where possible DoD is sharing its lessons learned from the kind of quick deployments we have

to do. I found that in forums like the National Communications System other folks are willing to listen to our lessons learned. Through the Homeland Defense ACTD we have involvement from several other agencies. As you know there are many political issues in regard to Homeland Defense. In DoD we offer our experience and we found that we may have some things that work, but also we have things that may be different because the whole issue of Homeland Defense is a little bit different. There are different rules of engagement as to who has responsibility. So we can't say these other organizations should just pick up everything we are doing and move with it, but we do offer our experience and capabilities for them to look at — perhaps as a way for them to move forward or begin.

CHIPS: What role is DISA playing in the DoD transformation?

Ms. McCoy: In terms of DISA as an organization, we are playing in multiple forums. One of the biggest efforts we have is the GIG bandwidth expansion (GIG-BE). This will provide a robust network capability throughout the DoD environment. On the applications side, we are looking at the enablers of the "Power to the Edge" vision, the enablers to the transformation. We are involved directly in what we call the "right data strategy," which means that we've changed the way we look at data and the way we provide data. We have begun to employ tools with XML to make it easy to share data across domains and we have designed and built a DoD XML registry to ensure that everyone in DoD who is using XML has access to existing naming standards (metadata tags) and can register new ones. We are also changing or updating our tools and capabilities so they are Web-enabled, making it easier for our customers to access applications and tools that can be used in different environments. A good example is the joint collaboration capability, such as the Defense Collaboration Tool Suite (DCTS) which we are providing to a wide range of users today worldwide, including Combatant Commanders.

We are looking at methodologies and approaches for getting information out and having it available through a process we call content staging. In order to make the vision happen we have to figure out how to manage services in this net-centric environment. We are looking at what types of services are needed and how they should be managed. We call this Net-Centric Enterprise Services (NCES) — critical to the sustainment and technological evolution of the GIG. There are various places where these components are covered in detail as well as how they interact with each other. As an early pilot of these components, DISA will integrate Web-based intelligence services with emerging C3 Enterprise Service to create a baseline C3I "electronic marketplace" on the SIPRNet that will enable mission planners to dynamically collaborate with the intelligence and combat support communities. An example of a managed service would be a Global Directory Service. So we have ongoing efforts to help with the transformational vision. All of these are geared to ensuring that we can provide interoperable capability down to the Joint Task Force Commander level and below — the guy on the battlefield — not just the people at headquarters.

CHIPS: What services would be in Global Directory Services?

Ms. McCoy: A Global Directory Service could contain information as simple as a person's name and e-mail address. As DoD information processing becomes ever more distributed, it could

have information in terms of what types of capabilities, data services or databases are available or where they are staged. Directory Services is one of those capabilities that will increasingly become highly protected and more secure because it will contain information about what is available and perhaps even where it is located.

CHIPS: When you talked about a user getting information and content staging, are you talking about the user's ability to pull data rather than have it pushed at them?

Ms. McCoy: We are looking at the ability to do both because what we find is that in certain cases the user does not have the opportunity to go out and surf. The user needs to have certain pieces of information, which they can predefine, sent to them automatically. But we would have the capability to do either — a smart push or smart pull — or the user could surf the net.

CHIPS: How do Web-enabling databases, information and processes, and process improvement for business and support functions help support the warfighter?

Ms. McCoy: There are a multitude of things that Web services will allow us to do. First it is easier for the user to get to the information. It provides the information to a broader set of users, who are able to get the information whenever they need it and in a faster method of delivery. By using Web technology you have the ability to do more of a real-time collaboration because everyone can pull up tailored information. You can update the information more frequently. It also allows us to take advantage of wireless capability, which is the wave of the future. Another thing that we tend to forget about it is that there can be a very good return on investment. When you go to the Web environment you can carry more of these services in the NCES. So you can reduce the number of servers, which reduces the number of system administrators that may be required to manage those types of services. You also have the ability to do more configuration management to ensure that the same type of capability is being used across the infrastructure. This is key to net-centric warfare.

CHIPS: Do you have security concerns with using wireless technology in the Defense environment where security is our number one priority?

Ms. McCoy: You said it exactly; we do have concerns in how we employ wireless. We are looking at the security and coming up with approaches that will allow us to use wireless in a secure manner. We have turned these approaches into standards for deploying wireless as securely as currently possible. We are also working with industry to improve the security in commercial wireless products and they are responding to that.

CHIPS: In a recent interview I did with Grady Booch, chief scientist for Rational, (CHIPS Magazine Fall 2002; www.chips.navy.mil/archives/02_fall/index2_files/interview_with_grady_booch.htm) he commented that DoD does not fully exercise the influence they have in the marketplace in demanding secure technology products. He said that DoD shouldn't have to spend additional money to build security into commercial products, rather industry should ensure security is built in at the front end.

Ms. McCoy: When we moved to the Internet and the network environment the rules of security became different than when we were operating on a disconnected mainframe. I'm not sure

anyone had a crystal ball on how security should be handled in a networked environment. This has really been a learning experience for industry as to what is needed in terms of security. I think we are demanding more of industry in terms of security. We are beginning to see the big companies, such as Microsoft, incorporate security as one of the key features of their products. We also have the NIAP (National Information Assurance Partnership) process that requires commercial products used in a certain way to be evaluated and certified. So I think we are getting there and vendors are responding.

CHIPS: I was just reading about the DoD debate over open-source software. Many in DoD believe open-source is the wave of the future for many reasons. One of the chief reasons is that the code is visible so it is easier to detect vulnerabilities.

Ms. McCoy: I think in some cases we really need to know the source code because it is the only way to know what is inside that code. There are some applications where that may become very important because of the way those applications are utilized and how they actually fit into the architecture.

CHIPS: There seem to be so many initiatives across Defense, with the Services working toward interoperability for command and control systems. Is there a plan or method of determining which are the most important to integrate first?

Ms. McCoy: That is exactly what the Joint Staff, in conjunction with the OSD principals, are working right now. They have reviewed the interoperability issues and analyzed which ones should be worked first. They are working a plan as to how we are going to get to interoperability faster. We work closely with JFCOM through experimentation and events like Millennium Challenge 2002 to demonstrate interoperability. We are also looking at a process that allows us to demonstrate interoperability through the development phase before we get to the operations phase so that interoperability is built in and then maintained throughout the life cycle. In terms of what capabilities or interoperability problems are worked first, DISA responds to prioritization decisions made by the designated approval authority.

In all these endeavors, we are working hard to provide capabilities that our customers want and use, and we ensure that we always keep in mind the users' experience so we can make our products and services even better.

CHIPS: Are there three top systems or programs that Defense is focusing on first for interoperability?

Ms. McCoy: I believe from a Web capability standpoint, we are looking at the GCCS family of systems — our GCCS program is part of that. They are focusing on what we call the C2 transformation, which looks at getting command and control information down to the JTF Commander and below. Another high priority is to ensure that we have the bandwidth capability down to the tactical level — so bandwidth expansion is high on the list of priorities.

CHIPS: In Dr. Myers' article she talked about the locations (CONUS/OCONUS) for the bandwidth expansion. Will the Fleet be able to share in this bandwidth expansion?

Ms. McCoy: This technology will support all warfighting. What we are talking about is ensuring that, as we transform and move to a net-centric environment, we have sufficient means and bandwidth to move the information wherever it's needed. So it would be applicable to all. What we have to work is how we get that information to the tactical level, to a warfighter on a ship or even one who could potentially be on horseback, so to speak.

CHIPS: Let's talk about the work of Applications Engineering ...

Ms. McCoy: The mission of the Applications Engineering Directorate is to provide responsive, secure and interoperable C2 and combat support capability for decision superiority to the President and Secretary of Defense, Combatant Commanders, Joint/Combined task forces, Services, Department of Defense and non-DoD agencies.

We provide a wide range of products, services and expertise. I already mentioned the Global Command and Control System which is DoD's Joint and interoperable C2 system, and the Defense Collaboration Tool Suite. These are providing situational awareness, readiness, planning, deployment support, collaboration and other capabilities for Combatant Commanders, JTF Commanders and below — today. The Global Combat Support System's (GCSS) Combatant Commander JTF (CC-JTF) capability is using portal technology with links to Service and Agency logistics and sustainment systems, to provide DoD users access to shared data, and applications, regardless of their location.

Over the next few years we are transforming the successful Common Operating Environment (COE) to fit OSD's Net-Centric Enterprise Services (NCES) concept. COE is currently used or planned to be used for/in 125 C2 systems and in support of GCCS, at 650 locations worldwide on 10,000+ joint and coalition workstations. The net-centric capabilities we provide will support the Power to the Edge vision of having tailored, fused information and tools available on the net, effectively supporting users wherever they are and with the means available to them.

In the Information Assurance area we are supporting "Defense-in-Depth" with expertise, products and services such as PKI, network and communications security, plus guards for cross-domain (e.g., Unclassified to Secret) and coalition information exchange. In addition to the Homeland Defense ACTD, we are also involved in Multiple Battlespace Awareness, Active Network Intrusion Defense, Coalition Theater Logistics, and C4I for the Coalition Warrior ACTDs, just to name a few. These are providing adaptive decision support, planning, and execution and collaboration tools through experimentation, demonstrations and spiral development. Our partnering with the Combatant Commanders and the operational community is very important. We are also partnered with the Defense Logistics Agency to provide a variety of eBusiness applications and services for paperless contracting, secure business transactions, wide area work flow, and electronic document access. In all these endeavors, we are working hard to provide capabilities that our customers want and use, and we ensure that we always keep in mind the users' experience so we can make our products and services even better.

Revolution Comes to the Teddy Roosevelt Battle Group

By JO2 Jd Walter, NPDC, Public Affairs Office

The USS Theodore Roosevelt (CVN 71) Battle Group, including the USS Saipan (LHA 2) Amphibious Ready Group, is about to get underway without ever leaving port. Their new mission is to test and evaluate Revolution in Training initiatives designed to enhance the Navy's mission readiness by providing Sailors with new tools and opportunities to develop both professionally and personally. Working with Task Force for Excellence through Commitment to Education and Learning (EXCEL), the battle group will implement and test the Sailor Continuum in an operational environment, as well as test incentives designed to increase performance and productivity. Additionally, the battle group will demonstrate the utility of a new learning management system, Navy Knowledge Online (NKO) that will track each Sailor's accomplishments.

"The innovations being touted by Task Force EXCEL are being driven by the Fleet and are for the Sailors. The acid test has to be at the waterfront. The Navy is bringing the Revolution in Training to Sailors, and it is happening now," said Director of Surface Warfare Rear Adm. Harry Ulrich. "This is the best opportunity to put these ideas and programs to the test." A working group consisting of executive officers (XO), command master chiefs (CMC) and other representatives from the Roosevelt battle group, Saipan ready group, Destroyer Squadron Two, and elements of Carrier Air Wing Eight (CVM 8) recently met in Norfolk, Va., to review and discuss the testing proposal.

"The testing proposals have generated a lot of excitement and enthusiasm," said Capt. Jamie Barnett, project leader for the beta test. "Private industry typically provides incentives for behaviors that enhance performance. That is what we will test within the battle group. We just need to work with the group to precisely define the tasks and how we will measure the outcomes." The goal of this effort is directed at increasing job efficiency and productivity — more time for ship's work by developing each Sailor professionally and personally.



At sea aboard USS Theodore Roosevelt (CVN 71) Oct. 28, 2002, MM3 Ryan Karlin checks the results of the September 2002 advancement exam for division personnel. U.S. Navy photo by PH3 Phillip Nickerson, Jr.