

DISA

WHO'S WHO



Updates
on the People
and Programs
of the Defense
Information
Systems Agency

THE SAFETY OF THE NATION RELIES ON YOUR SYSTEM. WHAT DOES YOUR SYSTEM RELY ON?

Whether you need proactive mission-critical support or basic system maintenance, SSTEW is the answer. Sun Support Total Enterprise Warranty (SSTEW) helps keep your critical Sun™ systems up and running perfectly. Always. It reduces your enterprise's back-end costs with volume discounts, contract management and some of the industry's most sophisticated asset tracking tools. So get SSTEW, the ultimate purchasing vehicle for all of your Sun Microsystems support and warranty services. Because a lot is relying on your IT.



Call 877-SSTEW-96 or visit SSTEW.com to learn what SSTEW can do for you.



To *MIT* Readers:

I'm delighted to have this opportunity to introduce some of the people within the Defense Information Systems Agency who are making significant contributions in support of our mission partners. The men and women profiled in "DISA Who's Who" represent the stellar military and civilian work force of our agency and our constant focus on meeting the needs of our customers every day.

DISA supports the warfighter through a variety of activities. While every important mission isn't reflected in these few articles, the words and thoughts of the people in these articles reflect their dedication to mission support, innovative efforts to achieve enterprise solutions, and achieving the appropriate balance between sharing and protecting information.

As you read about the people behind the mission at DISA, I hope you come away with an appreciation for the professionalism, dedication and outstanding quality of our work force. You will also learn a lot about DISA and some of its key initiatives by reading about the contributions these folks are making.

As DISA and its mission partners address the operational and technical challenges inherent in our dynamic global missions, we need people like these more than ever. DISA begins its planned Base Closure and Realignment move to Fort

Meade, Md., early next year, and senior leadership remains committed to solutions that will keep as many of the members of our work force with us as possible. Our telework, transportation, work-life and incentive programs are among the best within the Department of Defense, and we will continue to strive to maintain and create new programs to motivate and empower our invaluable team members.

Paige Atkins
Director,

Strategic Planning and Information
Defense Information Systems Agency



DISA's vision:
"Leaders enabling information
dominance in defense of our nation."

(Editor's Note: *The following profiles of DISA employees are based on interviews with MIT Editor Harrison Donnelly, who wrote the articles appearing in feature format.*)

Publisher's NOTE

KMI Media Group, publisher of *Military Information Technology*, produced the "DISA Who's Who" special section. The magazine, which publishes 11 times each year, reports on a wide range of C4ISR issues. The Rockville, Md., company also publishes *Military Logistics Forum*, *Geospatial Intelligence Forum*, *Military Medical/CBRN Technology*, *Ground Combat Technology*, *Military Training Technology*, *Military Advanced Education*, *U.S. Coast Guard Forum* and *Special Operations Technology*. The content of this special section was compiled by KMI editors in cooperation with DISA Public Affairs. This publication was designed by the KMI Art Department. Copyright 2010.

KMI Media Group
15800 Crabbs Branch Way
Suite 300
Rockville, MD 20855
Telephone: (301) 670-5700
Fax: (301) 670-5701
Website: www.mit-kmi.com

The appearance of advertisements in "DISA Who's Who" does not constitute endorsement by the Defense Information Systems Agency or the United States Department of Defense. DISA does not exercise any editorial control over the advertisements in this publication.

Table of Contents:

| | |
|--|----|
| Colonel Randy S. Taylor | 24 |
| Lieutenant Colonel (P) Michelle Nassar | 25 |
| Kimberly Rice | 26 |
| William Keely | 27 |
| Paul E. Flaherty..... | 28 |
| Chris Paczkowski | 29 |
| Denise C. Gentile | 30 |
| Julia Brown..... | 31 |



Colonel Randy S. Taylor
Commander
DISA CONUS

Colonel Randy S. Taylor is commander of DISA CONUS, where he leads an organization of joint-service military and civilian personnel who provision, engineer, operate and assure DoD's enterprise infrastructure in direct support of joint

warfighters, national-level leaders, and other mission and coalition partners across the full spectrum of global operations. Prior to his current role, he served in the White House Military Office as program manager for presidential contingency communications, and in the Army Special Operations Command as commander of the 112th Signal Battalion (Special Operations) (Airborne) while deployed in Afghanistan, Iraq and the Philippines.

What is the scope of DISA CONUS' responsibilities?

Our scope is as broad as directly managing the majority of the DoD's global capacity on the Defense Information System Network [DISN] and as deep as ensuring a single circuit supporting a warfighter in Afghanistan is always on. I'll give you a chilling example of the criticality of our mission by describing one of over 33,000 circuits DISA CONUS manages across the globe every day.

Early in my command of DISA CONUS, I awoke to a 3:00 a.m. phone call from Special Operations Command. The caller proceeded to describe that weeks of meticulously tracking a person of much interest were likely rendered useless when a DISN circuit, which enabled a CONUS-based pilot to remotely control an unmanned aerial vehicle from over 7,000 miles away, dropped for a matter of seconds. Even though the restoral time was brief, it provided the window of opportunity for the target to blend back into obscurity.

I imagined the impact to the special operators on the ground having to abort their mission and start over from square one. The gravity of this outage framed my perspective of the DISA CONUS mission. I'm happy to say that diversity across the DISN has improved significantly and this incident was a rare exception to the reliable service we're known for providing. In the simplest terms, we enable information dominance on a round-the-clock basis for today's net-dependent warfighters and national-level leaders.

DISA engineers and provides command and control capabilities, from the president to our troops in combat, with its global infrastructure and enterprise services. These capabilities must be reliable and protected against physical and cyber attacks. The bandwidth capacity of this global network has increased twelve-fold in the past five years and will certainly continue to increase. I anticipate that the demand on DoD's networks will expand even as our wars in Iraq and Afghanistan come to an end and we reset our forces for the next engagement. The prevailing view is that by 2011, 80 percent of our armed forces will reside in CONUS and deploy as expeditionary forces when our nation calls.

What do you mean by expeditionary forces and what will they require?

At the end of the day, it's only the soldiers on the ground who can seize and hold terrain. We have to empower them with information dominance—forward at the edge and en route while deploying. To do so, we're transforming the old, clunky way of deploying, where you literally pack up your network and its servers and ship it all off to the combat zone only to learn that you can't use what you've shipped when you hit the ground and that you've got to fight using a different network. I grew up with that approach, and I'm glad that its days are numbered. Expeditionary forces need the ability to deploy rapidly and reach seamlessly into the same networks—in the same way—throughout all six phases of an operation. It doesn't make sense anymore to use one network in CONUS while preventing or preparing for an operation, and then use another network, with new accounts, login credentials, or applications, while you're en route or fighting.

It's a question of balance—a question of how much of the network you turn off, pack up and carry around with you, and how much an always-on enterprise provides you wherever you need to plug into it. When you're out of balance, as we have been, you're slow to deploy and forced to train differently than you fight. The robustness and reliability of the DISN today provide the much-needed capability to reach into the so-called cloud and rebalance what we have to carry to the fight. Until recently, only special operations forces had the luxury of operating this way. The DISN today is such that it can enable all forces to do so. Although we still have some crusty, server-hugging dinosaurs in the ranks, today's warfighters are comfortable with this approach. What we call cloud computing is as natural to this generation as the air they breathe—it just is. It's what they're growing up with. They trust it and it works.

Expeditionary capabilities aren't just for combat. The same capabilities that enable an expeditionary response also enable a homeland security or a continuity of operations [COOP] response, like having to relocate due to a catastrophe, be it manmade such as a terrorist incident or natural such as a hurricane or even a pandemic. It allows for the rapid deployment of agile service delivery in a dynamic or continually developing scenario. At national and state levels, our nation is recognizing the need for viable COOP capabilities in a way that we haven't seen since the height of the Cold War. We're now facing a full spectrum of chemical, biological, radiological, nuclear and explosive threats. My folks are the ones that operate our nation's greatest capability for communicating and sharing information through such contingencies.

What are some of DISA CONUS' other missions?

Let me pause here to focus attention on the highly skilled and dedicated members of DISA CONUS. They do what they do out of love for our country and our way of life. Many of them have recently returned from a combat deployment or are supporting friends and family members who are deployed. Their

professionalism is matched by their extraordinary technical expertise. They have recently been entrusted with transitioning the Missile Defense Agency's Ground-based Mid-course Defense Communications Network onto the DISN. Through this consolidation, we have improved our operational effectiveness, by eliminating many exploitable seams and gaps that existed when these components of the enterprise were managed differently in each region.

They have also assumed the operational lead for implementing DoD's unprecedented initiative to assure the NIPRNet-to-Internet boundary by consolidating the management of all of the Internet access points worldwide and hardening them and all NIPRNet users against malicious Internet activity. Among many other things, they have also successfully consolidated and centrally managed several capabilities across DoD that had previously been managed on a local or regional basis, such as the Defense Switch Network and Defense Red Switch Network. Through this consolidation, we have improved our operational effectiveness by eliminating many exploitable seams and gaps that existed when these components of the enterprise were managed differently in each region.

How will Base Realignment and Closure impact you?

In addition to supporting the DISA Headquarters BRAC move, we at DISA CONUS are directly supporting all of the BRAC moves

across DoD, which are scheduled for completion by September 2011. This effort involves the enterprise infrastructure support for the closure of over 33 major military bases and the realignment or expansion of 29 others, encompassing the movement of over 250,000 military and 150,000 civilian positions. My professionals are the ones that will engineer and provision the many circuits and network equipment involved with each of these extremely complex moves.

When you look back at your time at DISA CONUS what would you like to say you've accomplished?

I want to know that I did my part in keeping my unit and all of DISA focused on supporting those who trust and rely upon our mission-critical services. When I talk about achieving the right balance in our enterprise infrastructure and developing our expeditionary capabilities, I share the view that the strategic world hasn't collapsed on the top of the tactical world, but inside it. This has occurred at a time when we find ourselves operating in the cyber domain where the net-dependent warfighter must dominate as decisively as in the land, sea and air domains. My goal is to see that DISA is prepared for the next engagement, anytime and anywhere, in any domain. I believe we are doing just that. ★



Lieutenant Colonel (P) Michelle Nassar
Program Manager
SATCOM PMO
PEO-STS

What is your current position and what are the major responsibilities required?

I currently serve as program manager for the Satellite Communications Program Management Office (SATCOM PMO). We are responsible for providing life cycle acquisition management of commercial satellite communications capabilities for all Department of Defense agencies. We offer worldwide COMSATCOM support, strategic and acquisition planning, and consolidated COMSATCOM system expertise to the DoD in support of the warfighter.

What do you spend most of your time on?

The current effort that requires the most attention is the Future Commercial SATCOM Acquisition (FCSA) strategy and associated contract mechanisms. FCSA is a joint venture with the General Services Administration (GSA) to provide a common marketplace for all government customers across the DoD, state, local and federal agencies. The goal is to ensure they all receive solutions that consider nationally directed information assurance and protection requirements, have improved access to federal supply schedules, which offers ongoing opportunity to add new competitors, continued competitive approaches to

transponded capacity in any available COMSATCOM frequency band, and continued competitive approaches to subscription services in any available COMSATCOM frequency band at a savings to the government.

The source selection for this effort is ongoing. The SATCOM PMO transition team is in the process of developing future internal business processes for post-award to ensure a smooth transition. Aside from cost-savings and improved contracting response time, we want to ensure that the migration from current expiring contract vehicles to the new FCSA contracts is as painless as possible for the customer, and there is a lot of work taking place to ensure this happens.

Why is this program important, and how does it benefit warfighters?

DISA at large serves as an advocate for the use of COMSATCOM in order to increase or free up the availability and flexibility of military communications. In the current operational environment in theater, the requirements for satellite services and bandwidth far exceed those available via military satellite; therefore, there is a need to fill that capacity gap with available commercial services. That is our mission focus.

A benefit, for example, of providing increased capacity is supporting the use of UAVs, which supplant the need for warfighters to be in harm's way and also provide critical intelligence

information. The volume of data generated and transmitted by UAVs is huge and is growing every day. Our ability to provide the satellite/communications capacity to support the UAV workload is directly tied to the safety and security of the men and women on the ground.

What challenges have you faced in developing this program, and what innovative technologies or approaches are you using to meet them?

If you have ever attended any acquisition-related forum, you will likely have heard the ongoing mantra that the requirement to adhere to rules, regulations and processes as outlined in the Federal Acquisition Regulation can be very frustrating. The processes that must be followed to acquire a capability often do not allow program managers to provide a product as quickly as the customer wants or needs it. There are several constraints, such as funding types for example, that sometimes limit the kinds of acquisition efficiencies we would like to achieve.

How does the program support broader policy and strategic goals of DISA and DoD?

The SATCOM program supports many of DISA's campaign plan initiatives. Through advances in commercial service offerings, the program improves service to the bandwidth disadvantaged user—warfighters in areas that do not have access to a robust network—and provides upgrades that expand the enterprise to integrate SATCOM to improve warfighter capabilities. Commercial satellite communications will also be a key enabler in achieving DISA's long-term vision to include converging services toward Everything over Internet Protocol (EoIP).

Stepping back a bit from your specific program, what do you see as the most important issues facing DoD/DISA in your area of expertise?

One important issue is modifying existing policies and directives in such a way that we as a department can become more flexible, timely and efficient without compromising the legality and prudence of how we do business. Because of the nature of the commercial satellite industry and the savings achieved through long-term leasing, we need to be able to continually anticipate

future satellite needs and technology trends in order to not only contract for what is needed now, but also to be able to tailor our contracts for future scenarios.

What is your career background, and how has it prepared you for your current mission?

I actually enlisted in the Army Reserves for two years prior to my commissioning as second lieutenant. My basic branch is Signal Corps, and I transferred to the Acquisition Corps at the mid-career point. I deployed to Saudi Arabia in support of Desert Storm as a platoon leader, and to Kuwait and Iraq in support of Operations Enduring and Iraqi Freedom as assistant product manager.

Having said that, I believe my enlisted time offers me an understanding of supporting the Army from a soldier's point of view. The deployment experiences provide an appreciation for what the forces are going through today and their needs. I understand what it is like to be in a remote location requiring and providing communications capability. All summed up, my background and experiences add an additional layer of motivation to get the capability into the warfighter's hands as quickly and feasibly as possible. But while my path has prepared me for the job, there are always new nuances to learn and opportunities to grow with any new assignment. Working a program at the defense level will prove to be both challenging and rewarding.

How will BRAC impact you?

On a personal level, BRAC has posed a challenge. My orders have me assigned to Fort Meade, Md., but DISA is still in northern Virginia. Since I am authorized only one move from my prior duty station, I have been living out of a suitcase at a friend's place the last two months or so. I plan to move to the Fort Meade area in November when my household goods must come out of storage.

On a professional level, I am concerned that there will be significant personnel turnover as the BRAC move date approaches, as some turnover has already begun. This could impact our productivity; it takes time to hire against vacant positions and takes additional time to get new personnel spun up. As a leader and manager, I must focus on fostering a cohesive team and get us through any rough patches ahead. ★



Kimberly Rice
Program Manager
Global Command and Control-Joint

Little more than a decade after arriving at DISA with a bachelor's degree in international studies and government and politics from George Mason University, Kimberly Rice is currently managing the worldwide

Department of Defense program of record for joint command and control. A former participant in one of several agency ini-

tiatives over the years to recruit promising college graduates, Rice last year became manager of the Global Command and Control System-Joint (GCCS-J) program.

Incorporating a wide array of hardware, software, procedures, standards and interfaces to provide worldwide connectivity, GCCS-J is designed to enhance information superiority and support the operational concepts of full-dimensional protection and precision engagement. It fuses select capabilities into a comprehensive, interoperable system by exchanging

imagery, intelligence, status of forces and planning information.

The three major baselines of GCCS-J are Global, which provides situational awareness tools and applications, intelligence applications and the infrastructure used by the overall system, the Joint Planning and Execution System (JOPES), and the Status of Resources and Training System (SORTS).

“The program is at an interesting point now, in that we are still the department program of record for joint C2 but officially in sustainment,” Rice said. “We have operational baselines out there, and last year we completed the closeout of the last major acquisition block for the program, which is the last big development effort, and now everything is in sustainment.

“Now that we’re in sustainment and getting Global fielded, most of our focus this year has been on the problems or issues that users have been having with the system—areas where we may have missed things, and where are the critical requirements that are coming in, for example from CENTCOM, that are the things they need us to do right away to support operations,” she continued.

“A big chunk of our time has been focused on getting out specific releases to address those types of issues,” Rice said. “We’ve had seven or eight smaller releases this year already, which has been good news for users and the program, because it’s getting away from taking two or three year cycles to get capability out the door.”

One of the biggest improvements in the program of late, Rice explained, was the expansion of access within Global from 20,000 tracks to 100,000 tracks. “That was a big

requirement for the users, and it has been a huge improvement.”

Rice’s other focus of late has been in response to termination of the Net-Enabled Command and Control program, which was envisioned as the replacement for GCCS-J. As senior leaders explore alternatives, her office is looking at “what are some of the smart things that we need to do to continue the good work that the joint and service programs have done in terms of evolving the whole C2 system into a next generation system. We’re taking some of the original NECC tenets that are still valid requirements, and, as we await department decisions, we’re looking at what we can do in the interim to keep providing enhanced capabilities and better infrastructure.

“The biggest thing for us,” she continued, “is going to be moving things from the local sites up to the enterprise level, keeping up with technology and making sure where possible we can affect the policies and strategy so that we can get things out as quickly as possible. As the users get the requirements in, acquisition-wise we can get it back out to them as soon as possible. We’re going to try to focus on managing that.”

Rice summed up her operating approach this way: “It’s the ability to get things out the door quickly, using the latest technology out there, while still meeting operational security requirements. It’s being able to switch it out as new stuff comes along, while making sure it is secure and has been appropriately tested. That’s the department’s biggest challenge, especially when it comes to software development.” ★



William Keely **Director of Field Security Operations** **Operations Directorate**

When William Keely, director of field security operations (FSO) for DISA’s Operations Directorate, or some of his colleagues show up at military commands these days, they are definitely getting people’s attention. Keely’s

teams expect this year to conduct some 130 Command Cyber Readiness Inspections (CCRIs), which represent rigorous evaluations of all aspects of information security at defense facilities.

The teams in effect have become an “enforcement arm,” Keely suggests, for U.S. CYBERCOM, the new Department of Defense command charged with protecting DoD networks. CYBERCOM has the authority to terminate a site’s access to the Global Information Grid when it is not in compliance with security standards and regulations.

Judging by the way most commands are responding to inspections these days, the prospect of a cut-off appears to

be focusing minds wonderfully, as the saying goes, on the importance of passing the CCRI. The inspection teams are meeting a different reception from similar missions in the past, Keely reports.

“When we used to do these types of things, we’d have the IA manager, or at the most maybe a deputy J-6, taking us around. Now, when we in-brief and out-brief, we often have general officers. They’re taking it very seriously,” he said.

Teams typically consist of a leader, six analysts and frequently a senior military officer, who acts as a liaison while also underscoring the importance of the process by his or her presence. “We have several 0-6s—colonels and Navy captains from around DISA—who take turns going out as the ‘top cover’ for the inspection teams,” said Keely. “When you have an 0-6 come out to a field unit, it gives even more attention to the inspection team.”

The teams are also showing less sympathy to “repeat offenders,” who may have gone through several earlier inspections without evidencing much in the way of actual

progress. “Before, we would go to critical sites multiple years in a row, and they would get ready to receive us a month or two before. Once we were gone, they might fix a few things, but then go back to normal. We were trying to help them ‘learn to fish,’ but now we’re kind of forcing them to learn to fish and keep on fishing,” said Keely, adding that the teams also have begun “no-notice” inspections.

Such efforts are essential, he said. “The DoD has to have greater mission assurance. Much of DoD’s mission assurance is reliant on the readiness of its IT infrastructure. The first step to readiness is compliance with DoD’s standards and operational directives. We can’t afford for billion dollar weapons programs to be compromised due to cybersecurity breaches.”

Still, Keely acknowledges that the inspection process has its own issues. “One of the primary challenges is the establishment of inspection rigor without sacrificing the unique security issues that can be found at each site. No one can really represent the operational risk of a site through the application of multiple checklists, but we do need to increase accountability for applying best practice security methods across multiple sites.

“We are looking at the application of the continuous monitoring approach that is being discussed across the federal government for the improvement of security management. We are looking at reducing our inspection team size while increasing our amount of data analysis to get a better understanding of the posture of a site,” he continued.

In addition to doing the CCRI, FSO is responsible for ensuring that a proper level of risk management is being conducted on every DISA operational system and many of

the COCOM systems; operationalizing information assurance and computer network defense enterprisewide solutions for DoD; general IA training for the department; development and maintenance of Security Technical Implementation Guides (STIGs); and DISA red teaming and penetration testing.

To help improve readiness of DISA network defense capabilities, FSO also has stood up a DISA Red Team, which has been conducting penetration testing of major DISA acquisitions programs. “We are now preparing to do other Red Team operations to improve our net defense readiness and give our net defense teams true cyber-defense practice with feedback,” Keely explained.

While CCRI is the most time-consuming activity within FSO, Keely emphasized that the office’s most important task continues to be the development and maintenance of the STIGs, which play the vital role of providing good security guidance in the field. Given the onrush of technology, it’s a never-ending job.

“We have to write new STIGs all the time,” he said. “Right now, people are requesting that we write them for BlackBerries, iPhones, Droids and other mobile devices, as well as every time a new version of Windows comes out.”

To improve the STIG process, FSO is working with vendors to automate the configuration standards, so they’re downloadable into the machine.

Keely concluded a recent interview with this observation: “We’ve had people thanking us that someone is taking security so seriously. On the other hand, the people thanking us will also say it’s causing more work and making their jobs harder.” ★



Paul E. Flaherty
Program Manager
DoD Gateways

After a decade spent working on and managing DISA’s Teleport program, Paul E. Flaherty this summer became head of a new initiative aimed at creating an environment in which any user has the ability to send or receive

any content, using any SATCOM band, over any satellite, anywhere in the world.

The new initiative, known as DoD SATCOM Gateway and currently in process of getting organized and staffed, seeks to bring greater unity and efficiency to the multiple SATCOM gateways, or access points, maintained by the department around the world.

“One of the things we are looking at as a department is if there is a way to take these disparate gateway systems and architect them such that you don’t have to have separate Army, Navy or joint systems. From a cost perspective, that

would save a lot of money. From a warfighter perspective, it’s easier for them to deploy if we have standardized interfaces,” Flaherty said. “We’re constantly looking at ways to be more efficient in providing information to the warfighter, because SATCOM provides 80 percent of the information going in and out of theater today.”

In addressing the evolution of DoD’s gateways, Flaherty brings a strong background and solid foundation based on his experience managing the Teleport program, which provides the deployed warfighter with pre-positioned satellite telecommunications for multi-SATCOM band and multimedia (voice, video, and data) connectivity from deployed locations throughout the world to online Defense Information System Network (DISN) Service Delivery Nodes and legacy tactical C4I systems. Teleport facilitates the interoperability between multiple SATCOM systems and deployed tactical networks, thus providing the user a seamless interface into the DISN and legacy C4I systems.

A key aspect of the Teleport program, Flaherty emphasized, is that it is a non-developmental program. “The challenge was to design, acquire and field a system that met critical warfighter requirements by the integration of existing COTS/GOTS capabilities and to do it within approved funding and to do it on schedule,” he said.

“Timeliness is key to relevance as well as keeping current with technology advances,” Flaherty continued. “The Teleport program addressed the timeliness challenge through an incremental approach to implementation and the technology currency challenge by using a technology insertion strategy with each increment fielded. As the warfighter changes how he fights and what he brings to the fight, the program needs to stay agile enough to be ready.”

Flaherty explained that the goal is to take existing capability—whether developed commercially or through government programs—and integrate it into a solution designed to expedite

deployment. “If we’re not timely in getting it out there, it doesn’t help the warfighter,” he said.

A major issue in bringing new capabilities to the field, he noted, is that warfighters at the same time are also architecting how they want to fight, and procuring capability. “We have to make sure we stay synchronized with the warfighter, so it’s important that we are able to do that quickly,” he said.

“The challenge of any program is to stay current and relevant,” Flaherty observed. “We need to continually focus on acquisition process improvement to ensure the processes facilitate getting the job done. In addition, we need to take advantage of and leverage the technology advances in the commercial world. There is no need to develop what has already been developed. Lastly, we need to ensure that DoD policies, directives and instructions don’t unnecessarily tie the hands of the implementers causing potentially avoidable delays and costs.” ★



Chris Paczkowski
Chief, Computer Network Defense
Enclave Security Division
PEO Mission Assurance and Network Operations

Chris Paczkowski has spent much of the past four years touching every one of the estimated 5 million or more computers in the Department of Defense.

Not personally, of course, but Paczkowski has been the leader of a team that has done essentially that, in the course of conducting the largest and most complex software implementation that DoD has ever undertaken.

The software, known as the Host Based Security System (HBSS) is a flexible, COTS-based framework of applications that provide DoD leaders, net defense operators, security personnel and local administrators a mechanism to prevent, detect, track, report and counter known cyber-threats to the DoD enterprise computing infrastructure.

The daunting aspect of that, noted Paczkowski, chief of the Computer Network Defense (CND) Enclave Security Division within the Program Executive Office for Mission Assurance and Network Operations (PEO-MA), was that it involved putting software on every single computer system in DoD. “In most offices, people don’t even have a count of the number of systems they have,” he recalled. “So it’s been a unique challenge, in putting something into local environments where every local environment, even within an organization, is different. Trying to work through that and acquiring, engineering and implementing what would work in all those environments has been a unique challenge.”

The installation effort, which required departmentwide cooperation to succeed, also took an innovative approach to working with contractors, Paczkowski explained. “Our implementation strategy was modified with the HBSS program to

directly include the integrator and vendor in the enterprise implementation phase. In the past, third-party contractors supported deployments and the vendor was not directly involved with these efforts. The success of the implemented solution was in the hands of someone other than the integrator and vendor.

“Now the integrator and vendor are working directly with our government team and have firsthand implementation experience,” he continued. “This relationship empowers the integrator/vendor to do what is necessary to successfully operationalize the capability. Also, we have modified our program training strategy from one that was a strict classroom solution to one that embraces multiple training environments.”

With the HBSS installation largely complete, Paczkowski is focused on tuning HBSS’ effectiveness and leveraging the deployed capability for the enhancement of his office’s other portfolio program, Secure Configuration Management (SCM), which has become prominent during the past year and continues to gain momentum across DoD and the federal government. SCM is the integration and optimization of enterprise IA applications and tools to provide an automated capability to inventory assets, produce configuration policy or guidance, assess baseline configuration of assets, report baseline configuration compliance, manage Information Assurance Vulnerability Announcements, distribute patch and remediation guidance, assess patch compliance of assets, and report patch compliance. SCM delivers capabilities to enable dynamic continuous monitoring, enterprise risk measurement and asset situational awareness.

“The strategic goal for SCM is to make the warfighter’s job easier,” Paczkowski said. “Regardless of a person’s role, everyone has multiple reporting requirements as part of their daily

activities—operational orders, federal suspenses, IA vulnerability announcements and so on. The current configuration management and vulnerability management reporting process is predominately manual data entry.

“We’re finding that a net defender has to have multiple spreadsheets and manually correlate information in order to populate different systems. You’re spending top dollars on a trained analyst to do data entry that you could get a summer intern to do. The challenge is to show them that if they have automated information at their fingertips, and you can populate those requests without putting the information manually into different locations, that’s a savings that enables warfighters to focus on their primary jobs,” he said.

Although the two portfolios may look different on the surface, security and asset awareness really are very intertwined and complementary, Paczkowski suggests. “It’s tough to defend what you don’t know. We’re working with the combatant commands, services and agencies on implementing these enterprise acquisitions. One of the biggest challenges has been under-

standing their environments across the entire enterprise.”

Paczowski concluded a recent interview by emphasizing that while implementing a comprehensive project like HBSS isn’t easy, the enterprise approach to IT being advocated by Secretary of Defense Robert Gates and other senior officials is still the right way to go.

“The challenges we are having with enterprise solutions are not the fact that we can’t stand up a centralized system. It’s just that if you’re going to touch every deployed warfighter in Southwest Asia, or even in every office in DoD, that’s the bigger challenge—making sure that we understand each of the local environments and can successfully implement a capability there.

“This is a huge team effort that required the support of all of DISA, the National Security Agency, the combatant commands and other organizations. These projects are not going to be successful without joint buy-in, and it’s even expanding beyond DoD. There’s a lot of work going on in the federal side that we are moving forward with,” he said. ★



Denise C. Gentile
Program Manager
Net Centric Enterprise Services

After spending the past four years overseeing the design, development, testing, fielding and acquisition life-cycle of enterprise services that enable information sharing across the business, intelligence and warfighting mission

areas, Denise C. Gentile is understandably elated that the Net Centric Enterprise Services (NCES) program is on the verge of receiving its full deployment declaration and moving into its sustainment and operations phase.

“It’s the final milestone,” said Gentile, the program manager. “It’s a significant event for the DOD to get the program through its acquisition lifecycle milestones, and so now it will be fully deployed, fully operational and available to the warfighter.”

But there’s some sadness there as well, Gentile acknowledges. “It’s a bittersweet feeling. When you’ve working so intensively on a program, with all its challenges, highs and lows, you’re always working at a fast pace, with 12-hour-plus days. Although it is a feeling of accomplishment to get the program through all its wickets and to be able to provide capability to the warfighter, it’s also sad that you’re leaving something you have put your heart and soul into for the last several years and leaving behind the staff and stakeholders who helped you achieve success.

NCES is a collection of 11 enterprise services designed to enable information sharing by connecting people and systems that have information with those who need it. These services enable secure information sharing and provide users the ability to discover information, expose information, collaborate and incorporate that information into their mission operations.

Gentile explained the benefits of the approach this way: “Because the services are offered at an enterprise level, the warfighter does not have the expense or maintenance of hardware or software—they are readily available to them regardless of the user’s location. But the greatest benefit to the warfighter is that they are able to leverage these services to obtain information to enhance their common operational picture; they don’t have to carry the cost of these core services.

“NCES is the information sharing pioneer in enabling the joint net-centric vision,” she continued. “We are realizing the tenets of DoD’s efficiency initiatives through deploying enterprise services that eliminate redundancy and duplication across the department. As new enterprise services are identified, and as we expand our global presence and extend our services to our coalition partners, federal and local government, we will continue to improve efficiency and effectiveness for national and global security.”

With a 16-year career at DISA so far, working on a wide range of programs, Gentile brought a wealth of acquisition and management experience and expertise to the challenging task of getting enterprise services to the warfighter.

“We were the first to implement the innovative ABC acquisition approach—adopt, buy, create. We looked across the department and intelligence community to adopt operational services that would serve as enterprise solutions for our customers. Our content discovery service was adopted from the intelligence community; our content delivery service was adopted from the Air Force; our user access portal was adopted from the Army; and the metadata registry was an internal DISA capability,” she recalled.

Increment 4
Protected Satellite Communications

Increment 1
Networking At-The-Halt

Increment 3
Full Networking On-The-Move

Increment 2
Initial Networking On-The-Move

WIN-T

WIN-T IS...

BEING FIELDIED TODAY.

A SELF-FORMING AND SELF-HEALING NETWORK.

PROVIDING INTEGRATED NETWORK OPERATIONS.

A MOBILE, AD-HOC NETWORK.

THE U.S. ARMY'S CURRENT AND FUTURE NETWORK.

FOR MORE INFORMATION PLEASE CALL 508-880-1759.

GENERAL DYNAMICS
C4 Systems

“We also partnered with the testing community to streamline our test and evaluation master plan and established reciprocity for certification and accreditation of these adopted services,” Gentile said. “But we did not stop there; for all our services, we were able to perform early user tests and obtain a limited operational availability decision, which enabled us to deliver services to the warfighter early while we continued to enhance and complete the formal acquisition testing process.”

The wars of today and the future will be contingent on tools and information to make agile, timely and accurate decisions, Gentile said. “I believe that we are facing two major challenges. The first is to be able to evolve technology solutions that keep up with commercial technology that is familiar to our warfighters. Today’s warfighters have more available to them on their iPhone or Droid than on our military laptops. The second challenge is information assurance and how we can

continue to provide secure, robust, agile enterprise services for the warfighter.”

Gentile concluded a recent interview with these reflections: “It takes time to evolve legacy systems to new technology, and it takes time to change the culture of people to adopt change and restructure their business and operational processes. It’s the challenge that enterprise services are faced with today, but as the user becomes more comfortable with enterprise services and realizes mission benefit, enterprise services will become part of their day-to-day operations.

“I am sure that these enterprise services will evolve, and new enterprise services will be added. But the underlying message is that enterprise services enable the warfighter to make more informed, accurate and robust and agile decisions. I am proud to have been a part of this program and the joint net-centric vision. I am looking forward to my next challenge.” ★



Julia Brown
Project Manager, Network Services
DISN Video Services

U.S. and Allied commanders in Afghanistan are now able to communicate more effectively and securely, thanks to a video teleconference (VTC) bridging service that Julia Brown spent much of 2010 helping develop.

The Afghanistan Theater Video Bridge, which met final operating capability in August, represented another successful telecommunications initiative worked on by Brown, a project manager for network services in the DISN Video Services division.

With a background in multiple video systems over the past 25 years, Brown is a firm believer in the value of the direct personal contact made possible by video conferencing technology.

“When you communicate, there are multiple layers of communication,” Brown explained. “The vast majority of the communication we do, as human beings, is actually nonverbal. An e-mail could be misinterpreted or not interpreted 100 percent correctly.

“When you have video teleconferencing available, people, especially those who are in a command level position, seem to prefer video teleconferencing for their communication. It’s very important; because they’re not only observing what people are saying, but they’re also observing behavior. With video teleconferencing, they’re better able to determine if everyone is truly onboard with what’s being discussed. As master communicators, they understand that sometimes, objections and reservations are not necessarily communicated with spoken words, but are exhibited with people’s body language,” she continued.

“It’s particularly important when we’re working with our Allies, especially with the multilingual coalition operation in Afghanistan. Language translation might not always be 100 percent accurate and therefore, a communication impediment or barrier; however, body language and facial expressions tend to be universal.”

As might be expected, the Afghan video bridge posed a number of technological challenges, notably involving the linking of networks maintained at varying levels of security by the U.S. and other nations.

“The biggest challenge was establishing a secure cross-domain connecting the U.S. SIPRNet, NATO and ISAF CENTRIX networks,” Brown said. “I was fortunate to have support from the project co-lead, Army Major Richard Abelkis and his technical guidance. We worked in close coordination with the Joint Staff, the National Security Agency, the Joint Interoperability Test Command, CENTCOM and U.S. Forces Afghanistan to develop, test and field a unique approach to secure H.323 communications in this sensitive environment.”

Brown also spends time on the DISN Video Services (DVS) program, which provides a VTC bridging service, enabling communication between U.S. and Allied warfighters and their support components globally. Brown’s office is currently working to converge DVS onto the IP network environment, and is in the process of establishing a classified IP VTC service at the Defense Enterprise Computing Center, Columbus, Ohio.

Looking back, Brown emphasizes the lessons she has learned from various career mentors. “They taught me to believe in the power of teamwork among people. While I understand and truly appreciate the technical element, the human factor is what makes everything work. I am fortunate to work with talented people across the board, who will overcome obstacles and see a project through any and all difficulties. Human beings are the true interface connectors in any successful technical project.”

“I really enjoy my work here at DISA and look forward to bringing newer technologies to the warfighter and helping to innovate ways for more effective telecommunication in the future,” she added. “I believe in what we do!” ★