The Voice of Military Communications and Computing

Military Information Technology

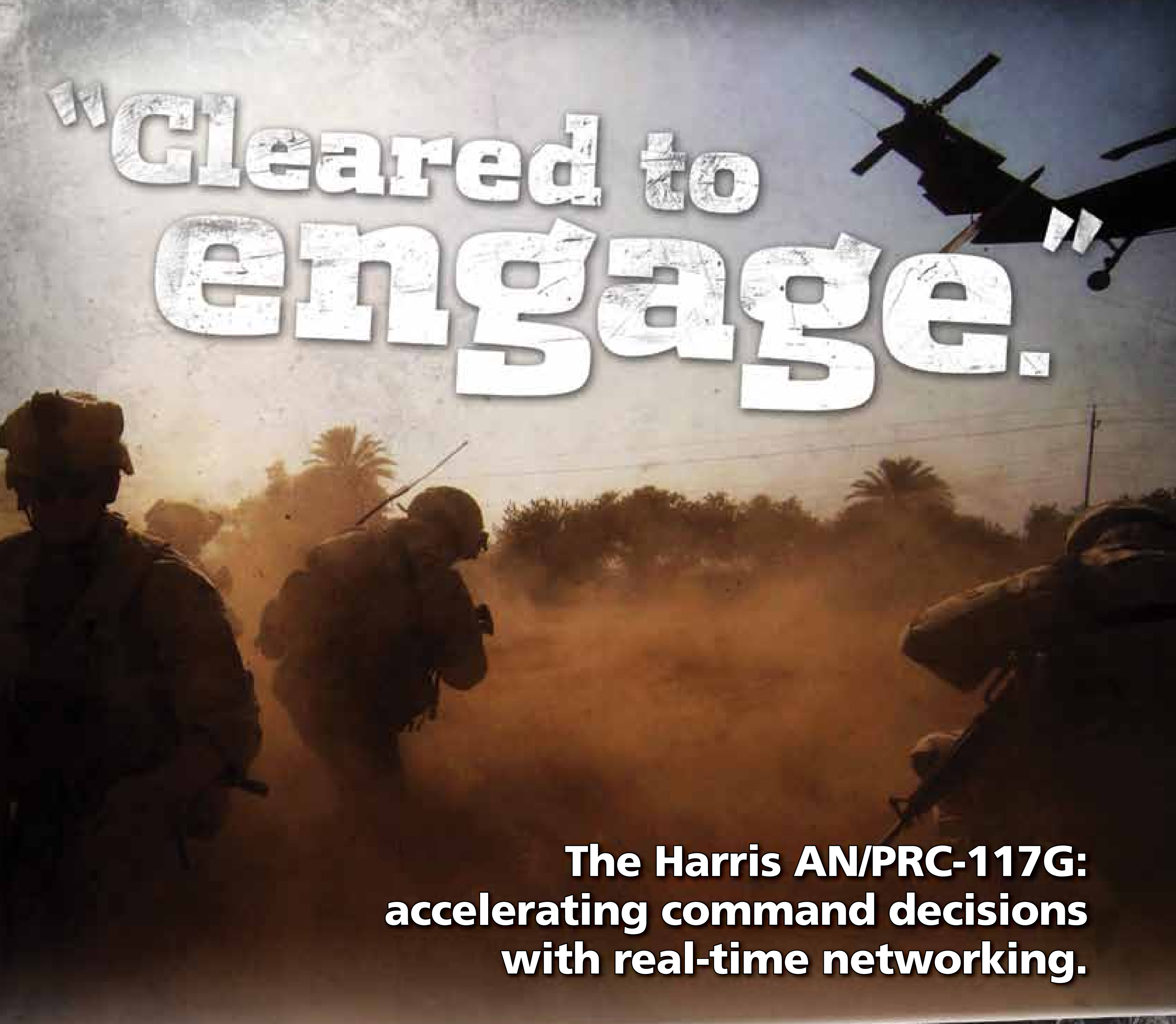
Efficiency Implementer

Gary L. Winkler

PEO EIS
Army

www.MIT-kmi.com
MIT
C4
March 2011
Volume 15, Issue 2

SATCOM ✯ Task Force Interoperability ✯ Data Protection ✯ NGEN Contract


"Cleared to engage."

Military Information Technology

March 2011
Volume 15 • Issue 2

Features

www.MIT-kmi.com

Cover / Q&A

Departments

Industry Interview

MILITARY INFORMATION TECHNOLOGY

VOLUME 15, ISSUE 2 MARCH 2011

The Voice of Military Communications and Computing

EDITORIAL

Managing Editor
Harrison Donnelly harrisond@kmimediagroup.com

Senior Copy Editor
Laura Davis laurad@kmimediagroup.com

Copy Editor
Kat Saunders kats@kmimediagroup.com

Correspondents
Adam Baddeley • Peter Buxbaum • Cheryl Gerber
Scott Gourley • Karen E. Thuermer

ART & DESIGN

Art Director
Anna Druzcz anna@kmimediagroup.com

Senior Graphic Designer
Jittima Saiwongnuan jittimas@kmimediagroup.com

Graphic Designers
Scott Morris scottm@kmimediagroup.com
Jennifer Owers jennifero@kmimediagroup.com
Eden Papineau edenp@kmimediagroup.com
Kailey Waring kaileyw@kmimediagroup.com

ADVERTISING

Account Executives
Cheri Anderson cheria@kmimediagroup.com
Hope Casselman hopec@kmimediagroup.com

KMI MEDIA GROUP

Publisher
Kirk Brown kirkb@kmimediagroup.com

Chief Executive Officer
Jack Kerrigan jack@kmimediagroup.com

Chief Financial Officer
Constance Kerrigan connik@kmimediagroup.com

Executive Vice President
David Leaf davidl@kmimediagroup.com

Editor-In-Chief
Jeff McKaughan jeffm@kmimediagroup.com

Controller
Gigi Castro gcastro@kmimediagroup.com

Office Coordinator
Diamond Mathews diamondm@kmimediagroup.com

OPERATIONS, CIRCULATION & PRODUCTION

Manager, Circulation and Operations
Toye McLean toyem@kmimediagroup.com

Distribution Coordinator
Wayne Brooks wayneb@kmimediagroup.com

Data Specialists
Sharisse Hill sharisseh@kmimediagroup.com
Tuesday Johnson tuesdayj@kmimediagroup.com
Danielle Jones daniellej@kmimediagroup.com
Sasha Scott sashas@kmimediagroup.com

MARKETING & ONLINE

Marketing & Online Director
Amy Stark astark@kmimediagroup.com

Trade Show Coordinator
Holly Foster hollyf@kmimediagroup.com

KMI MEDIAGROUP

A PROUD MEMBER OF

SUBSCRIPTION INFORMATION

Military Information Technology
ISSN 1097-1041
is published 11 times a year by KMI Media Group.

Military Information Technology is free to members of the U.S. military, employees of the U.S. government and non-U.S. foreign service based in the U.S.
All others: $65 per year.
Foreign: $149 per year.

Corporate Offices
KMI Media Group
15800 Crabbs Branch Way, Suite 300
Rockville, MD 20855-2604 USA
Telephone: (301) 670-5700
Fax: (301) 670-5701
Web: www.MIT-kmi.com

EDITOR'S PERSPECTIVE

Harrison Donnelly
EDITOR

If there is one theme running through the comments of senior military and government leaders on the topic of cybersecurity, it's the need for training and development of an expanded cadre of security professionals able to meet the ever-growing cyber-threat.

In response to this pressing imperative, both the public and private sectors are stepping forward with a host of programs, ranging from the National Initiative for Cybersecurity Education to undergraduate and graduate curricula at institutions such as the University of Maryland University College, to cite just one example.

To develop the real pros, though, it's best to start them young. That's why programs such as the Air Force Association's (AFA) CyberPatriot high school cyber-defense competition can represent an important element in the nation's cyber-strategy.

The goal of the national competition is to excite high school students and motivate them toward careers in cyber defense and other science, technology, engineering and mathematics (STEM), while instilling greater national cybersecurity awareness. Math/computer science is the STEM discipline with the greatest projected job growth, but it is also a discipline in which a large percentage of underrepresented persons and women are lost in the leap from high school to college. Moreover, educating a large number of users to the basic elements of computer/network security is certain to increase the security of the national infrastructure.

CyberPatriot III began last spring, with a two-division approach designed to attract both college prep computer science students and the more diverse audience numbering over 500,000 in the nation's JROTC detachments of all services.

The AFA CyberFutures Conference, scheduled for March 31-April 1 in National Harbor, Md., will include the CyberPatriot III finals, presented by Northrop Grumman. The Center for Infrastructure Assurance and Security of the University of Texas at San Antonio, SAIC, General Dynamics Advanced Information Systems, Microsoft and Raytheon are also supporting the project.

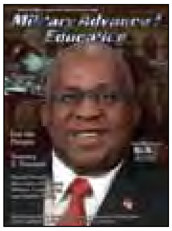
Harrison Donnelly

KMI MEDIA GROUP MAGAZINES AND WEBSITES

Geospatial Intelligence Forum

www.GIF-kmi.com

Military Advanced Education

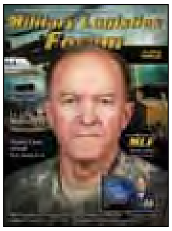


www.MAE-kmi.com

Military Information Technology

www.MIT-kmi.com

Military Logistics Forum

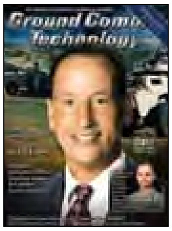


www.MLF-kmi.com

Military Medical/CBRN Technology

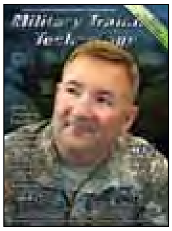
www.MMT-kmi.com

Ground Combat Technology



www.GCT-kmi.com

Military Training Technology

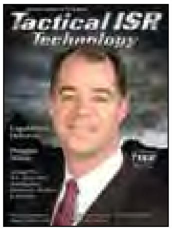


www.MT2-kmi.com

Special Operations Technology

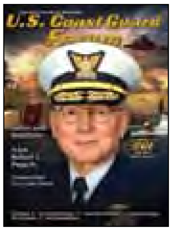
www.SOTECH-kmi.com

Tactical ISR Technology



www.TISR-kmi.com

U.S. Coast Guard Forum



www.USCGF-kmi.com

1010101010101010101010101010101
101010
10101010101010101010101010101010101

Compiled by KMI Media Group staff

PROGRAM NOTES

Army Approves Next Generation Battle Command System

The Army has approved for fielding the next-generation Force XXI Battle Command Brigade and Below (FBCB2) system, called Joint Capabilities Release (JCR). FBCB2 JCR, developed by Northrop Grumman, will give warfighters significantly enhanced capabilities for battle command.

FBCB2 is the key situational awareness and command and control system used by U.S. and coalition forces. More than 95,000 FBCB2 systems have been deployed worldwide, forming the world's largest tactical network. The system has been successfully fielded for 16 years.

JCR will be incorporated into the LandWarNet/Battle Command Baseline for fielding to deploying units scheduled to receive software block 2.

JCR upgrades include an increase in network bandwidth that allows the system to move more information to more users within seconds rather than in minutes. JCR also provides a common FBCB2 platform solution for both the Army and Marine Corps.

"The ability to receive and share battlefield data through a broad-based, reliable network is increasingly important and critical to the mission. JCR provides new collaboration tools and other enhancements that are orders of magnitude more capable than what is available to soldiers and Marines today," said Joe G. Taylor Jr., vice president of the Ground Combat Systems business unit within Northrop Grumman's Information Systems sector.

The system includes Blue Force Tracking 2 (BFT 2), a high-tech, high-speed force-tracking satellite communications network. The Army says BFT 2 will be roughly 10 times faster than the existing BFT system. When JCR is fielded with the new BFT 2 transceiver and network upgrade, friendly positions will be updated in seconds.

With JCR, warfighters will also be able to share more broadly critical, sensitive information. The BFT 2 will include a new programmable in-line encryption device that is fully compatible with JCR.

Other new JCR capabilities include the Commercial Joint Mapping Tool Kit and an over-the-air self-descriptive situational awareness (SDSA) capability. SDSA will eliminate inflexible fixed databases and allow FBCB2-equipped units to change task organizations in the field to meet new mission requirements.

JCR represents a major departure from the original FBCB2 architecture. The new JCR approach is called the Battle Command Product Line (BCPL) and is designed to correct the stovepipe development approach taken by earlier command and control systems. Properly executed, BCPL will enable the Army to develop, test, certify and deploy software capabilities more quickly and at a lower cost.

The version that will be fielded is JCR-Vehicle L-Band (v) 1.1.1.4 V-4. The Army and Marine Corps are currently testing JCR V1.3.1 and considering it for a fielding upgrade this year.

FBCB2 links communication devices, sensors, vehicles, rotary-wing aircraft and weapons platforms in a seamless digital network to provide a clear, continuous and common picture of the battlefield. Most FBCB2 systems communicate via a satellite-based network, while about 30 percent use the Enhanced Position Location Reporting System tactical radio network. (See *MIT*, February 2011, page 6.)

PEOPLE

Army Reserve **Colonel Kaffia Jones** has been nominated for appointment to the grade of brigadier general and assignment as commander (troop program unit), 359th Signal Brigade, Fort Gordon, Ga.

Army **Brigadier General Jeffrey G. Smith Jr.**, commanding general, 5th Signal Command/deputy chief of staff, G-6, U.S. Army Europe and Seventh Army, has been assigned as deputy commanding general for proponency, Army Cyber Command, Fort Belvoir, Va.

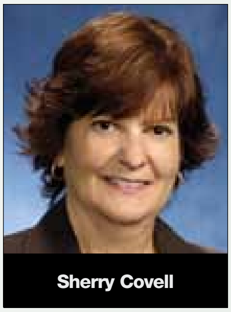
Air Force **Brigadier General David D. Thompson**, who has been serving as vice commander, U.S. Air Force Warfare Center, Air Combat Command, Nellis Air Force Base, Nev., has been assigned as director of air, space and cyberspace operations, Headquarters Air Force Space Command, Peterson Air Force Base, Colo.

Dennis L. Via

Army **Lieutenant General Dennis L. Via** has been nominated for appointment to the rank of lieutenant general and assignment as deputy commanding general/chief of staff, U.S. Army Materiel Command, Redstone Arsenal, Ala. Via is currently serving as director for command, control, communications and computer (C4) systems, J-6, Joint Staff.

Sumit Agarwal has been assigned as senior adviser, Principal Office of the Under Secretary of Defense (Policy), Cyber Engagement and Innovation. Agarwal previously served as deputy assistant secretary of defense (public affairs outreach and social media).

Robert Butler has been assigned as deputy assistant secretary of defense (cyber policy), after previously serving as deputy assistant secretary of defense (cyber and space policy).



Sherry Covell

Harris Corp. has named **Sherry Covell** vice president of intel programs for its IT services business. In her new role, Covell is responsible for client satisfaction, service delivery and growth for IT services across the intelligence community.

Task Force Interoperability

MILITARY, INDUSTRY WORK TO IMPROVE COMMUNICATIONS COMPATIBILITY AMONG THE MANY AND DIVERSE ORGANIZATIONS PARTICIPATING IN A JOINT TASK FORCE.

By Peter Buxbaum
MIT Correspondent
buxbaump@kmimediagroup.com

As joint task forces increasingly become the organizational format of choice for missions ranging from responding to the earthquake in Haiti to improving the Afghan system of justice, the military is working hard to improve communications interoperability among the many and diverse organizations participating in a JTF.

Joint Task Force-Haiti, for example, was a six-month enterprise, at its height comprising over 22,000 personnel, that was tasked with saving lives, alleviating suffering and coordinating humanitarian missions to Haiti in the aftermath of last year's earthquake.

Combined Joint Interagency Task Force-435 is a partnership among U.S. military and civilian agencies, their international counterparts and the government of Afghanistan that conducts detention, corrections, judicial sector and biometrics operations. JTF Guantanamo is in charge of the detention center at that location and of its inmates. JTF North, based at Fort Bliss, Texas, supports federal law enforcement agencies in protecting U.S. borders. Combined Joint Task Force-Horn of Africa partners with coalition forces and host nations to promote regional security and stability.

The makeup of these joint task forces suggests a number of challenges associated with the necessary communications and information sharing that must take place among their various constituent parts. If their communications equipment and networks are not interoperable, it will be difficult if not impossible to coordinate the activities of the JTF partners, particularly in emergency situations. The interoperability issue was first brought to public notice during 1983 operations in Grenada by U.S. forces, which were marked by serious inter-service communications problems.

For this reason, the U.S. military conducts exercises throughout the year to test the interoperability of systems and to work on ways to make systems interoperable which were not designed for that purpose.

Much of the ongoing DoD Interoperability Communications Exercise (DICE), for example, is focusing on the transition to Internet Protocol version 6 (IPv6), the next-generation standard for routing data packets over networks, as well as testing smartphone-like devices for the battlefield.

"We are testing how tactical systems are integrating with big networks with IPv6," said Bradley Clark, chief of the Joint Interoperability Test Command (JITC) Transport Systems Branch, "and how information is being pushed out protocols to certified products. We also expect to see more tactical cell system requirements. People want to use smartphones to see what is going on on the battlefield and to connect to their home bases."

System-Level Assessments

These tests are important in facing the interoperability challenges faced by joint task forces. DICE's principal purpose is to generate system-level interoperability assessments and certifications to support the fielding of interoperable systems to warfighters. Participants include communications equipment and personnel from each of the armed services, combatant commands, Joint Communications Support Element (JCSE), National Guard and Department of Homeland Security, as well as private companies whose technologies are being tested or which are offering interoperability solutions.

"There are a number of issues associated with joint task forces that have come about due to unintended consequences," said Colonel Joseph Puett, commander of JITC, a Defense Information Systems Agency (DISA) unit that conducts the DICE on behalf of the Department of Defense. "JTFs are stood up for a particular reason, and no one necessarily expects that certain partners would be associated with a JTF. Yet they all need to interconnect in one way, shape or form. Just about every JTF that we have fielded in recent history has had some kind of interoperability issue. Providing a mechanism for establishing interoperability across domains once a JTF is stood up is one of the key missions of JITC."

JTFs in Haiti and Afghanistan, among others, comprise diverse groups of military, government and private organizations. "They each operate their own system," said Puett. "Each was designed with one set of requirements in mind, but in a JTF, they must be made interoperable with other systems designed for separate set of requirements."

Col.
Joseph Puett

Karl Fuchs

Interoperability issues often arise when different JTF partners use equipment provided by different vendors, noted Karl Fuchs, vice president of engineering at iDirect Government Technologies, a provider of satellite communications to the military and government. "Some of this equipment was not designed to be interoperable," he explained. "But even when it is, issues have arisen when different vendors are running different versions of the software code and they turn out not be compatible."

Activities like DICE come to test the compatibility of new technologies with existing systems, said Clark. "Tactical users want to integrate new technologies that are coming up, like handheld radios that transmit voice, data and video," he explained. "When these things come out, we do the interoperability assessment to see how these work within the existing environments."

The migration of communications equipment and networks to commercial standards, such as IPv6, has helped promote interoperability, but even then kinks in the systems must be smoothed out. "There are still differences in how people set up networks," said Bill Berger, director of sales and sales engineering at Ultra Electronics DNE Technologies. "Different networks treat IP packets in different ways. These need to be standardized in order, for example, for video to be streamed across networks in real time."

TOTAL COMMUNICATIONS

Connections that Matter®

The **TCS SNAP (SIPR/NIPR Access Point) VSAT** solution is the most versatile deployable communications solution available today. Noted for optimum performance in the harshest of operating environments, this diverse system has a proven design validated in Operation Iraqi Freedom, Operation Enduring Freedom and Operation New Dawn, yet flexible enough to meet future requirements using multiple band and modems options. The TCS SNAP is the No.1 fielded terminal for the US Army in Iraq and Afghanistan.

The TCS SNAP system:

- Offers unique operating flexibility with multi-band, field interchangeable feeds
- 2.0 M quad-band (Ku, Ka, X and C-band)
- Plug-and-play L-band modem support
- JITC tested interoperable NIPR/SIPR baseband options
- Citrix IP Acceleration
- Lightweight, quickly deployable
- Operational in minutes with one-button satellite acquisition
- Cisco Solution Technology Integrator (STI) and Certified Premier Partner

Contact TCS: 1.800.307.9489 | swiftlink@telecomsys.com

www.telecomsys.com

CITRIX

TCS TeleCommunication Systems
Enabling Convergent Technologies®

JITC routinely tests communications systems before they are fielded to warfighters to make sure they comply with DoD interoperability standards and to otherwise integrate systems from JTF partners that do not interoperate. JITC labs simulate large, complex networks and are designed to test the incoming software, systems, and equipment for interoperability.

Bill Berger

bill.berger@ultra-dne.com

"We also emulate the network usage of particular users and virtualize machines," said Puett. "DoD is also investing in federating testing infrastructures so that we can leverage the testing facilities of each of the armed services together with JITC's. We can leverage the best each of these facilities has to offer and that way we do not have to repeat the standardized testing for information assurance and security."

Compatibility Issues

Increasingly, the leveraging of the various labs' capabilities involves linking these various labs over network infrastructures. There are several DoD and service networks specifically designed for this type of activity.

"These new technologies are helping us assure that interoperability requirements are actually satisfied by systems designed to meet those particular requirements," said Puett. Systems designed to be interoperable "are pretty much ready to go. They function as advertised."

JITC's chief challenge is how to make systems that are not designed as such to be interoperable, or at least compatible with DoD systems, according to Puett. This issue almost always arises when older, legacy equipment is being brought to the table.

The diversity of equipment brought to the joint task force by coalition armed services, civilian government agencies and non-governmental organizations represents one issue. "Another issue is that these entities typically come to the mission with commercial off-the-shelf products," he explained. "Quite frequently, those COTS products are not designed with same set of security parameters that we require in the Department of Defense."

Systems not designed to be interoperable take follow-on work in order to create some level of compatibility or interoperability with other systems. "Sometimes it is as simple as a procedure that operators need to undertake," said Puett. "Sometimes it takes a workaround, like 'swivel chair' integration, in which users hand-code information from one system to another. It could also be hardware or software configuration items, turning switches on or off or using a particular port. In the worst case scenario, it requires significant hardware or software changes to the systems."

The kinds of workarounds JITF recommends depend on what systems are involved in any particular situation, the mission at hand and what level of interoperability the participants are willing to live with. "Can you live with the swivel chair or do you require an application to pull data directly from another," said Puett. "Do you require one application to understand the metadata associated with other application?"

Some coalition countries that sought to join the Afghan Mission Network, for example, brought COTS equipment that did not meet DoD security requirements. "In the first instance we told them to use the swivel chair," said Puett. "Meanwhile, we worked with those nations' acquisition directorates to update their systems so that can later achieve a better level of automated interoperability. This often takes the form of a software patch that can be pushed to a particular system and can take anywhere from six months to two years to be put in place."

Humanitarian missions are often of short duration, "but they are critical operations," said Puett, noting that sometimes a decision is made to push everything to the NIPRNet, which handles sensitive but unclassified traffic, rather than the SIPRNet, which carries classified communications. "If we've got to be able to talk to the Red Cross, we might be willing to make the operational decision to operate on the NIPRNet and accept some of the vulnerabilities associated with the Red Cross system. It all depends on the individual situation, the operational need, and how much time we have to deal with it."

The DICE exercises are designed to demonstrate the interoperability capabilities of new technologies as they approach the marketplace. "Much of the emphasis has been on devices that are pushing information to the edge of the network, to the warfighter," said Clark. "DICE provides our industry partners with the operational environment they would be expected to work including a simulated system complete with a mix of network traffic. We run testing scenarios appropriate for a given system and work with the companies to improve their systems."

The 2010 DICE saw the introduction of a number of handheld devices seeking entry to DoD's approved product list. In addition to the emphasis on IPv6, the 2011 tests are expected to focus on testing of requirements for tactical cellular systems that would allow the eventual introduction of smartphone-like devices to warfighters.

"Industry is pushing the leading edge of technology," said Clark. "We hope to provide the latest products and technologies to warfighters while making sure they provide the required level of information assurance and security."

Network standards and protocols, usually developed by industry, also promote a certain level of interoperability, added Puett. "Industry standards form the backbone of interoperability," he said. "If you can identify ahead of time the standards that the technology needs to conform to and industry builds to those established standards, interoperability becomes relatively easy. It is not easy when you are not able to anticipate the interoperability requirements and specify the standards beforehand. Most of the standards we rely on are commercial standards specified by commercial industry through organizations like the National Institute of Standards and Technology and the IEEE.

"The Internet Protocol requires everybody who wants to operate on the Internet to meet those standards," Puett added. "We are finding that things are becoming more interoperable on the data level and that our efforts are focused more on the application and messaging layers of the architecture."

Packet Priority

But conformity with standards like IP does not eliminate all interoperability issues, according to Berger. One interoperability challenge that remains, even among IP networks, involves the configuration that controls how packets are routed and with what level of priority.

"Voice and video must get priority in networks, in order to avoid latency and jitter," Berger explained. "E-mails can bounce around 15 times and still be delivered in a timely fashion. Commanders in the field need to be able to knock everyone else off a busy network if need be. Command and control communications have to get through as a top priority."

The problem is that different networks may assign different priority values to different types of traffic, and this compromises the transmission of data as they cross from one network to another. "One network might assign video a priority value of 50 while it might be 55 on another network," said Berger.

DISA has issued standards for the Differentiated Service Code Point (DSCP) on military networks, but they have not received universal acceptance, according to Berger. The DSCP is the value attached to each IP packet on a network that specifies the service level assigned to it.

Ultra Electronics DNE has a gateway product that has been demonstrated at both DICE and the Joint User Interoperability Communications Exercise (JUICE), which is able to reconcile the data priority configurations among networks based on DISA's DSCP standards.

The Ultra Electronics DNE gateway is a piece of hardware that sits at the connection point between networks. "The gateway looks at each packet and assigns it priority based on established policy," said Berger. "Eventually the DISA standards will be controlling on military networks. But even then, DoD may require the use of commercial networks and those networks might not comply with the DISA standard."

IDirect Government Technologies has also participated and continues to participate in JUICE, which will be taking place this year during June across dozens of locations worldwide. The objective is to evaluate emerging technologies in a joint task force environment.

"Some interoperability issues that we have seen have been relatively mundane," said Fuchs, "such as the interoperability between a particular modem solution and an antenna. Where things get tricky is at the network management level. Can device A talk to device B? How do you intelligently manage all of the devices that are now connected to the network?"

To answer those challenges, iDirect has introduced a product called SatManage, a suite of web-based software tools for automation, monitoring and integration of hybrid networks and networks-on-chip-based applications. "SatManage allows the network operator to understand more graphically what is happening on a satellite network," said Fuchs." "The biggest sticking point for network management has to do with companies changing their codes. As they improve their products and add new features, the code changes, and that has an impact on interoperability."

The approach iDirect is taking to tackle this problem focuses on cooperative and collaborative engineering with other hardware vendors. "The ultimate goal of any network management system would be to develop a capability to click on one end-device, and then click on a second end-device, and then have the system automatically and intelligently build the equivalent of a switch virtual circuit through which all network elements, from quality of service to per-hop behaviors, would be matched," said Fuchs. "This would encompass satellites, routers and terrestrial components of the network end to end. It is a daunting goal, but we are making great strides in that direction." ✩

Contact Editor Harrison Donnelly at harrisond@kmimediagroup.com. For more information related to this subject, search our archives at www.MIT-kmi.com.

Teaming for the Navy Network

Contractors lay strategy and look for allies in competition for Next Generation Enterprise Network business.

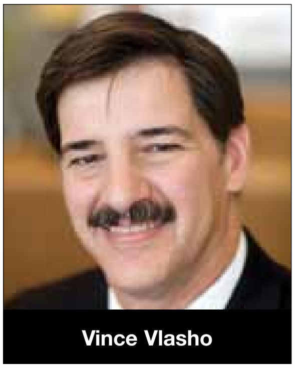
By Karen E. Thuermer
MIT Correspondent
thuermerk@kmimediagroup.com

As the Navy moves toward awarding the first segment of its massive Next Generation Enterprise Network (NGEN) contract this spring, contractors are also working hard to put together their competitive teams and proposals for what is expected to be one of the largest federal acquisition programs of fiscal years 2011-2012.

With a potential value of $14.5 billion and opportunities for both large and small businesses, NGEN also represents the first step towards achieving the Department of the Navy's future vision of a fully integrated Naval Networking Environment (NNE). NGEN will dovetail with development of the Consolidated Afloat Network Enterprise Services (CANES) program, the service's planned network for ships at sea.

Somewhat later than originally planned, NGEN will replace the Navy Marine Corps Intranet (NMCI), the decade-old program under which system operations and security were managed by Electronic Data Systems (EDS), which was later acquired by Hewlett-Packard (HP). Although differing from NMCI in key respects—notably, by providing the Navy and Marine Corps more direct command and control of the network and opening it to multiple contractors and their subs—NGEN will still be one of the largest systems in the world, serving more than 700,000 sailors, Marines and civilians and comprising up to 70 percent of the Navy's total IT footprint.

Patricia Tracey



Vince Vlasho

Because of the acquisition policy taken by the DoN, as well as the sheer size and complexity of the system, NGEN bidders will have to put together large teams of partners and subcontractors to compete for the five program segments. HP's NMCI team, for example, has included more than 200 subcontractors.

To help put together the comprehensive teams of companies needed to handle all aspects of the program, some companies have adopted an innovative "speed dating" approach to finding and evaluating potential teammates able to help them meet technical, small business and other requirements.

Five Segments

The five segments planned for NGEN are enterprise services, transport services, independent security operations oversight and assurance (ISOAA), software and hardware. A separate competition will be held for each segment, with the software and hardware components coming up through various task order competitions. By segmenting the contract, the Navy anticipates that NGEN will have improved capabilities implemented through a block approach that will enhance the NNE network.

ISOAA is its first stage for requests for proposals, followed by transport services and enterprise services.

The Navy hopes that with more competition, it can drive more favorable pricing and direct the integration of the various segments. More competition should also bring more innovation.

"It is important that the Navy be in a more direct operational control mode—not just a contractual mode as it was in the early days," remarked Patricia Tracey, HP vice president for industry and development, defense.

To introduce the most competition to the contract, contractors that win the transport services segment cannot win the enterprise segment. Consequently, companies that are direct competitors will find they also must introduce a cooperative environment in which they can operate together in a way that enables a seamless experience for the Navy.

"The Navy is not naïve in knowing that this is a more complicated approach than awarding the contract to a single supplier," Tracey said.

While NGEN has come under some criticism from industry for its different acquisition approach, Navy officials are ensuring that the contract applies best practices from industry and government, as well as lessons learned from working on other contracts. The overarching focus of senior leadership is to ensure a seamless transition from NMCI to NGEN, while improving reliability, adaptability, security, governance and support to the warfighter.

"The Navy is procuring NGEN services in a set of segmented services in an effort to increase the number of competitors who have an opportunity to deliver service to the Navy and to be able to gain some additional control of network environment by integrating some of the work themselves in the NGEN environment," explained Tracey.

Speed Dating

Understanding the NGEN contract and its timing, however, is not easy for companies. To get a clearer understanding of the contract, potential prime contractors and subcontractors have attended events such as the NGEN Teaming Seminar organized by Input last summer.

During the seminar, a "speed-dating round" was hosted by Accenture, CSC, General Dynamics, Harris, Lockheed Martin and Raytheon to help potential prime contractors and subcontractors find a better way to engage with each other and assess proposal needs in a personable and efficient manner.

"The INPUT event helped us learn which companies were interested in the transport or enterprise services segments of NGEN," revealed Vince Vlasho, Accenture Navy client account lead. "It also provided us the opportunity to meet several small and specialized services companies with valuable offerings that could augment our own."

Given the pace at which the various segments of the NGEN contract are being rolled out, however, many defense integrators feel that it is still too soon to reveal much about their intentions for NGEN. A spokesperson for Lockheed Martin IS&GS-Defense, for example, stated simply that the company is aware of NGEN and is evaluating the opportunity.

Input did indicate, however, that Lockheed Martin is looking for potential teammates, both large and small, with current understanding of the NMCI environment both CONUS and OCONUS and with contract or work experience relevant to the various segments of the NGEN opportunity set, and within both the Navy and the Marine Corps.

Accenture told Input that it is looking for "teaming partners who share our passion for helping clients become high-performance businesses and government."

Vlasho emphasized that Accenture has dedicated infrastructure operations and data center and technology operations groups that deliver enterprise services to Department of Defense, federal government and commercial clients today.

"Additionally, we have a unique blend of DoD technology experience combined with a leading technology position in the commercial sector," he said. "NGEN would benefit from the latest commercial practices packaged and implemented in a manner that facilitates government control."

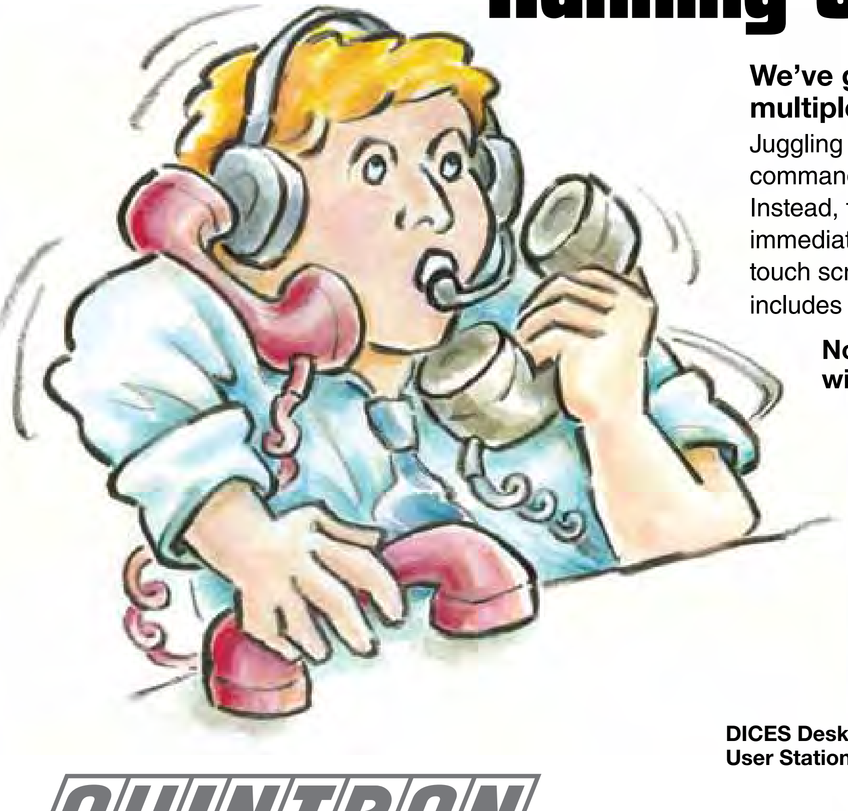
Overall, Accenture hopes to provide the NGEN program transition and risk management services, ITIL-based operational excellence, information assurance, program controls, and transformation initiatives that result in cost savings.

"Accenture presently provides these services to DoD and looks forward to expanding the value its team provides to warfighters, analysts, administrators and other DoD stakeholders," Vlasho said.

"Much of the industry is exploring teaming relationships, with some teams already formed," he added. "Many companies interested in NGEN await additional key acquisition information before making final teaming decisions. We are forging relationships with other large and small companies that have excellent reputations for service delivery for the Navy or Marine Corps and continue to evaluate potential teaming partners."

Given the complexity of the NGEN contract, however, contractors believe DoN will face several challenges as it moves forward with NGEN.

"Some of these challenges are derived from the new operating model that the DoN is putting into effect for NGEN—government ownership of the assets, a larger government role in NGEN operations, and a segmented acquisition strategy," Vlasho said. "This new operating model will require the government to instantiate a work force that is ready to execute its expanded role, and will require both management



and governance structures that enable it to integrate the efforts of the segment service providers."

Accenture offers numerous strengths where the NGEN contract is concerned, he said. "We are more than just a high-performing technology company; we have worked with DoD and commercial customers in a wide variety of engagements to help them overcome similar challenges."

Vlasho regards this important because NGEN provides a path to expanded and improved services for more than 700,000 network users.

"It is an important foundational step in achieving the DoN's vision of a fully integrated and secure naval networking environment that seamlessly connects users, regardless of location," he said. "Points of integration and transitioning to a new environment typically are two of the most challenging aspects of programs such as NGEN, and we see them as vital elements that must be managed and executed flawlessly to avoid disruptions in service to our nation's warfighters."

Austin Yerks, president of CSC's North American Public Sector Defense Group, agrees. "As a go-to partner for critical national programs, CSC brings experience and world-class capabilities in large-scale transformations and mission-critical solutions. This complex integration and transition experience is particularly important on contracts such as NGEN, where any disruptions can ultimately cost lives."

It was recently announced that CSC, General Dynamics Information Technology, Harris Corp. and Cisco would team to pursue the enterprise services segment of NGEN. In addition, CSC is participating in the transport services segment as a subcontractor to Harris, with GDIT and Cisco. "This team's combined strengths offer the best possible team to provide a highly secure, integrated solution that is specifically tailored to the Navy's needs and will ensure availability and reliability," said Yerks.

Security Veteran

Raytheon is no newcomer where the NMCI contract is concerned. The company operated as a sub on EDS's team and remained involved in NMCI until 2007. At that time, Raytheon was largely responsible for security engineering.

Raytheon has pursued onboard and offboard ship networking activities over the last 10 years with the Navy. As a result, Raytheon is experienced with security requirements in the Navy networking environment.

"We have reached out to the Navy to give our view on how on how they should structure the contract going forward," commented Helen Schlientz, manager of business development, Raytheon.

To date, Raytheon has responded to the request for information for NGEN.

"We've talked to a lot of Navy senior officials and believe they are taking the correct steps to move themselves towards their next naval environment," Schlientz said.

"The Navy is heading in the correct direction by taking control of the network operations itself. That is definitely an area they need to protect," she continued, adding that it is also an area in which the Navy needs to have partners that will work towards their future goal.

Regarding prime contractors, Schlientz made the point that companies need to be concerned about their investment exposure. Given the size of the NGEN contract, the investment can be considerable for a company to participate. Teaming and diversifying helps them find a niche category. The duration of time between requests for proposals (RFPs) and the size of larger RFPs also can make for a lengthy timeline. Obviously, companies must consider how much effort or energy they can make towards the contract over the next eight to nine months and where their strengths lie.

Primes also need solid teams that offer diversity in order to be able to give the Navy what it is seeking. In Schlientz's view, this effort is not one-sided, but all encompassing. "If you look at it from an IT services and command and control aspect, that is a lot to offer," she commented. "There are a lot of teams out there that can provide encompassing skills."

Raytheon has an advantage, however, since it comes from a position of knowing the information assurance portion of MNCI. "Our strength is in securing the network," Schlientz said.

The benefit of teaming with subs plays a particular role in the fact the total contract is being broken into different segments. "That offers a lot of possibilities for companies not wanting to make the complete investment," she said.

Service Continuity

The end-point year for implementing all segments of NGEN has been set at 2016, although that schedule could slip.

Meanwhile, HP Enterprise Services remains involved in NMCI though the continuity of services contract (CoSC) it signed with DoN in July. That contract is valued in excess of $3 billion, if all options are exercised.

Overall, the CoSC enables the Navy to transition the comprehensive, end-to-end IT services presently provided under the NMCI contract to the NGEN contract in a manner that minimizes the possible risks to the Navy's IT operations and security.

Going forward, Tracey contends that given HP's experience, the company would offer the Navy the lowest risk alternative in the two major service segments—enterprise and transport. "We believe HP can add value in the two segments that they are planning to award," she said.

That's because the Navy is not looking to rip out and replace its current network with a new one. With NGEN, what's being replaced is the contract (and contractors). In essence, the Navy is changing how it does its IT services rather than replacing its IT. Consequently, HP plans to pursue work in all of the segments and take a teaming and partnering approach.

"We expect to be able to present a fairly compelling case for the significant award for that work," she said. "We would also play to the strengths of more than one company."

The reason, she pointed out, HP has the largest purpose-built network in DoD and has, in that process, pioneered some efforts around applications.

"The company is uniquely responsive to the military requirements," she said. "As a result, the Navy and the Marine Corps has achieved a level of control over that part of their IT environment that no one else has. That is a remarkable accomplishment and HP is proud to have been a part of that." ★

Contact Editor Harrison Donnelly at harrisond@kmimediagroup.com.
For more information related to this subject, search our archives at www.MIT-kmi.com.

PELICAN™

> DIGITAL PROTECTION

LAPTOP AND PORTABLE ELECTRONIC PROTECTION SOLUTIONS

> TACTICAL LIGHTS

LED TECHNOLOGY • WEAPON MOUNTS

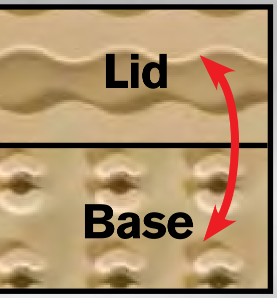
> SPECIALTY PRODUCTS

RACKMOUNT SERVER CASES • FIELD DESKS

> NIGHT VISION AND IR TOOLS

NIGHT VISION TOOLS FOR STEALTH OPERATIONS

STACK WITH AUTHORITY



The new ISP Case from Pelican-Hardigg virtually eliminates load movement with its patent pending Inter Stacking Pattern **(ISP)**.

The system is designed to cube out perfectly across standard logistics platforms for speed and load efficiency. Cross-stacking builds incredibly tight loads that can save time while strapping and netting.

FEATURES

- *6 sizes from 4 to 25 cf*
- *Watertight with pressure purge valves*
- *Lightweight with load bearing rib design*
- *Casters on select cases*
- *Optimized for:*
  - *JMIC container*
  - *463L pallet*
  - *40 x 48 pallet*
  - *1000 x 1200 euro pallet*

PELICAN™

www.pelican.com\mit

Pelican Products, Inc. 23215 Early Avenue, Torrance, CA 90505
877.619.0288 (TOLL FREE) Tel 310.326.4700 • Fax 310.326.3311

Stop That Leak!

As the military responds to the fallout from the WikiLeaks case, message classification and data leak prevention tools are drawing increased attention.

By Karen E. Thuermer
MIT Correspondent
thuermerk@kmimediagroup.com

Amid the ongoing investigation into the WikiLeaks incidents and the massive release of U.S. government secrets, security experts are taking a hard look at how the military and intelligence communities use and share information. At the same time, technology companies are stepping forward with systems designed to prevent repeats of the alleged theft and dissemination of SIPRNet documents by Private First Class Bradley Manning while serving as an Army intelligence analyst.

Not only did the incident signal how easy it could be for a disgruntled or malicious individual to achieve a high security breach, experts warn, but it also served as a wakeup call on how simple it can be for someone to extract classified information from any organization—whether intentionally or by accident.

For all the current focus on protecting networks from outside attacks from cyberspace, analysts say, the WikiLeaks case underscores that more needs to be done to counter the insider threat posed by malicious or poorly-trained personnel.

"Traditionally, secret service communities test employee fitness for service before recruitment," commented Martin Sugden, chief executive officer of Boldon James, an information security company that is a wholly owned subsidiary of QinetiQ. "But once recruited, the individual is entrusted with the management of information. A disaffected employee, therefore, is dangerous."

"There weren't sufficient procedures and technology in place to prevent this largely because government, and the Department of Defense in particular, were focused on potential attacks coming from the outside," explained Gigi Schumm, vice president and general manager, public sector, for the Washington, D.C. office of Symantec. "That is the culture of DoD, where the enemy is typically on the outside."

This real-life example demonstrates why access is a major issue facing many organizations today, particularly DoD and its agencies.

"The first challenge is whether he should have or should not have had that access," said Tim Upton, founder and chief executive officer of Titus Labs, a provider of e-mail, document and SharePoint classification software solutions.

Tim Upton

tim.upton@titus.com

"To combat this type of release, the agencies will need to change their business processes so that information can only be accessed in approved manners," Sugden added.

Schools of thought regarding access have changed in the last decade, starting with the environment before the September 11, 2001, terror attacks, where each government agency regarded information proprietary to their agency. Basically, agencies did not share information with other agencies. Subsequently, however, the Department of Homeland Security was created, some policies were changed, and alterations were made under the interest of national security.

"In the post-9/11 environment, the government felt it had no choice but to look seriously at information sharing that was accessible between agencies and private sectors," said Sandy Holland, senior director of federal sales for Websense, a provider of unified web, data and e-mail content security solutions.

Now in a post-WikiLeaks world, there is a new awareness of the potential risks as well as the benefits of information sharing.

Getting back to Manning and the SIPRNet leaks, however, the issue is first and foremost whether or not this individual should have had or should not have had access.

"This was a casualty of information sharing," Upton commented. "And there will be incidents when access is abused. The fundamental problem is there so much information everywhere."

Gatekeeper Tools

A number of companies offer technologies, such as message classification and data leak prevention (DLP) technologies, to help prevent computer leaks, although it is important to note that no system can be 100 percent safe proof.

Message classification essentially helps an organization understand who owns the data so that it can go back and address whether or not data has been accessed, and by whom or what group. DLP works as a gatekeeper by determining when a document, message, photograph, PDF file or other format can be transferred and when it cannot.

"DLP technology encompasses different kinds of technologies, some of which have to do with encryption," pointed out Symantec's Schumm.

Some DLP technology involves everything from tracking data, monitoring it, setting alerts and preventing it from going where it should not go—whether it be to outside an organization, a CD, DVD or thumb drive, or even sent internally within the organization.

Unlike some civilian agencies, DoD has not yet deployed much in the way of DLP, Schumm suggested, while adding that this changed significantly with WikiLeaks. “After WikiLeaks we have seen an increased awareness and interest in our DLP technologies. DoD and its agencies are looking at them and trying to understand how they can best be put to use within the military.”

Websense, meanwhile, has built enterprise DLP technology into its web and e-mail security technologies with its Trinton solution.

“This runs the gamut across protecting organizations’ networks and end points, providing data discovery and classification, understanding what the risk is in the enterprise, as well as enforcing policies to ensure that confidential data is not lost or stolen,” outlined Dave Meizlik, Websense director of product marketing and communications.

While most organizations have an idea of what data or information is confidential, they do not necessarily know where it is stored and how it is being used, or if they have a set of technologies and policies in place to protect it. For government and military applications, in particular, data loss can be of global consequences.

At the same time, both public and private enterprises need to be able to employ networking services such as cloud and social networking for multiple communications purposes to keep their work force mobile in today’s world.

“They need to be able to do this safely and not expose their organization to risk, especially when we are talking about national security and the lives of service men and women,” Meizlik said.

To do this, entities are using proven methodology to identify that which is confidential.

“This does not mean boiling the ocean. Many organizations have lots of confidential data,” Meizlik said. “You target specifically the data that is most valuable and at greatest risk.”

Essentially, the effort falls into one of three tasks. First, identify where data is stored, including copies or duplicates that are stored in unsecured locations; second, monitor to where data or information is being transmitted, including data that is at risk, but also data that can be lost; and third, protect the information and data with DLP technology at network and endpoint.

“By doing this you are using DLP technology both as an enablement tool and a security tool,” Meizlik said.

That aside, it’s worth noting that data is typically lost because of a broken communication channel or process within the organization.

“This could lead to good people making bad decisions, not knowing they are creating risk or a security event,” Meizlik mentioned. “By monitoring the direction in which information is being transmitted, you can get better feel for what is going on in the organization, what the challenges are, and define an action plan so you can protect that information.”

And because DLP technology is data-smart, it knows the difference between, say, a grocery list and an employee roster.

“With DLP tech, you can enable an organization to use removal media and to copy over that grocery list but prohibit people from copying over sensitive information,” he explained. “Or it can be used to allow them to encrypt that sensitive information so that it cannot be misused or lost.”

This enables the modern enterprise to operate in a very social, mobile, global cloud-based world while reducing risk. “You can set it to prohibit employees from posting, transmitting or duplicating, or you can transparently monitor and issue alerts, so that other people within the government who are monitoring for this behavior can find a maliciously intended folks.”

The key is the content and how DLP is applied within an organization.

“There are lots of DLP technologies out there,” Meizlik warned. “The difference that makes or breaks DLP is the methodology you employ—the simplicity of the solution.”

Classification Tools

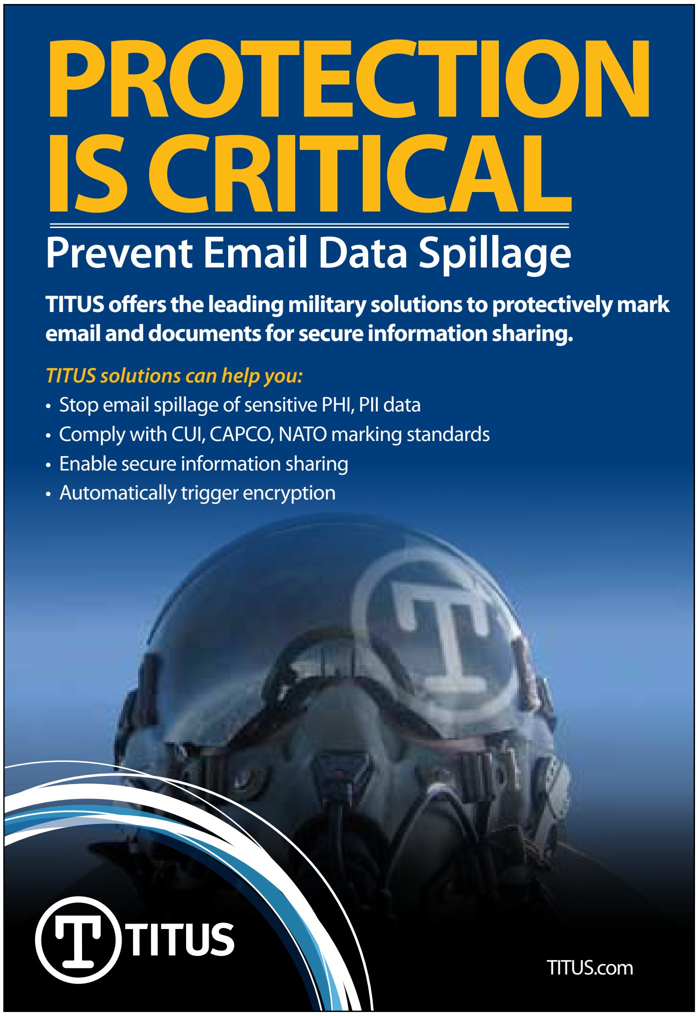
The task of sorting out good DLP tools from bad ones, however, can be just as difficult as sorting and classifying sensitive information from non-sensitive, and vital secrets from those that are less important.

“But I think that is where the weakness is in the system,” Titus’s Upton said.

Even before the utilization of computers, individuals were assigned the task of stamping certain papers “Top Secret” and “For Eyes Only” based on set policies that determined information sharing.

“We still do that today,” Upton said. “But what it is not being done well is translating that classification skill into computerese.”

In fact, in the WikiLeaks example, the information had been marked visually. “But this is not enough and probably only served to help identify the information of interest to the individual,” stated Sugden.



To combat this problem, agencies need to change their business process so that information can only be accessed in approved manners.

"Had the documents been protectively marked using a tool that also added metadata marketing and DoD had been using, for example, an enterprise rights management solution with protection levels being assigned appropriate to the classification of the data, then it would not have mattered that the information had left the organization on a thumb drive, CD or hard drive, as only the device and user with clearance to read and use the documents would have been able to enable and read them," commented Sugden.

To do this, he suggested, the visual markers that are added to documents, such as top secret, need to be added to the metadata attached to the document so that the system can then apply control mechanisms. Those mechanisms can include removing the ability to e-mail, copy or print information; ensuring that data is encrypted in transit so it cannot be read by unauthorized people; allowing access to data from specific locations only (not on mobile devices); and keeping audit trails of who accesses data and what they do with it.

"The overriding principle is that the system must be designed to combat the disaffected employee and not assume that all staff are good," Sugden said.

Message Classification

Firms like Titus are devising message classification tools that offer organizations a solution to enforcing classification policies and preventing inadvertent disclosure of information.

While systems that operate like gatekeepers in opening and closing the door to allow or disallow the movement of data, e-mail, even photographs from flowing may seem like a basic principle, the process becomes much more complicated when systems are asked to tell the data apart.

"If systems cannot distinguish between good and bad data, they cannot know when to lift the drawbridge or put it down," Upton said.

Consequently, how can a computer know which 10,000 documents might be moving to a USB stick? The difficult question is determining if they are top secret, secret or not secret at all.

"Although systems are available that look at data, that kind of determination is not automated," he said. "There needs to be help for the machines."

In other words, if systems are able to identify the data, then the "doors" would be able to open or close appropriately. According to Upton, there are two ways to accomplish this: by message classification and data leak prevention.

"DLP can be the drawbridge to a USB or CD," he said. "The problem is the rules that they set do not let data go to the USB drive. That is a big stick and kills information sharing."

According to Titus, the most important step in securing information is to understand what information is truly sensitive and what information can be freely shared. Information classification can be used to accomplish this objective. But as Upton emphasized, "Simple sells."

Titus Message Classification is a product designed to ensure that all Microsoft Outlook and Outlook Web Access messages are classified before they can be sent, helping to prevent inadvertent disclosure, comply with marking standards and enhance other solutions used by the organization such as DLP and encryption.

New features in the latest version of Titus Message Classification include a "one-click classification" feature, which enables users to classify, market and protect their e-mail with one click of the mouse, as well as "content review and redaction," which allows users to see the exact areas in the e-mail where the problem exists. Content review highlights the sensitive information and enables the user to either edit the content themselves, or automatically black out the sensitive or confidential content using the redaction feature.

"When you combine these with DLP software, users can be more certain which documents can go and which cannot," Upton said. "Or if there are more than 10 sets of rules, or more than 10 documents that are top secret, a user can flag an alert or get an override."

Of course, it is not always possible to identify every e-mail or piece of data when thousands, even millions are involved. "A malicious user is difficult to stop," he said.

But there are other safeguards, such as looking for patterns. "If you see a pattern where there is 500 top secret documents moving to a removable drive, one knows that is a strange occurrence," Upton remarked.

To tag this activity, advance rules can be set. "An organization can set a threshold that allows only a certain number of messages or data to go. After that it triggers the need for extra authorization," he said.

Titus sees the military as the largest market for its software and is working on various capabilities that have been requested. Already the company is working with DoD and the Air Force on secret networks for their e-mails and documents.

"We are doing initiatives with Microsoft, Cisco, Symantec and McAfee, as well as other companies worldwide, whereby their systems can read our metadata and stop data from flowing," Upton added.

Virtualization Solutions

Tom Simmons, area vice president-U.S. Public Sector, for Citrix Systems, has another alternative for combating the WikiLeaks problem. He proposes virtual desktops and other virtualization technologies that can address concerns raised by WikiLeaks. Loosely defined, this involves turning one physical computer or server into multiple virtual machines.

Information can be hosted in the data center. Users can access, manipulate and analyze that information via their virtually connected machines with that data never leaving the data center. Consequently, access is controlled, and users and what they are doing can be audited.

"One will also be able to tell if the data is then pulled across the wire and sent to a thumb drive, printer, or other device," Simmons said. "If we have the ability to audit those different things, we also have the ability to control access to those different things. So I can turn off the capability to do local print or local copy. With the technology in the virtual desktop or virtual application, security officers and IT managers now have the flexibility to provide access to those who need access, audit what they do with it, and dynamically change the access based on need."

While virtual computing and desktop virtualization has been around for several years, the technology continues to mature and morph as the number of types of devices proliferates.

Contact Editor Harrison Donnelly at harrisond@kmimediagroup.com.
For more information related to this subject, search our archives at
www.MIT-kmi.com.

Network Manager, Multifunction Terminal Advance

Completion of software test underscores value of government/industry partnership.

Editor's Note: *This is another in a regular series of updates on the Joint Tactical Radio System (JTRS), as provided by the program's Joint Program Executive Office (JPEO).*

The JPEO JTRS Network Enterprise Domain (NED) has announced successful completion of the formal qualification test (FQT) of the Soldier Radio Waveform Network Manager (SRWNM) with multiple JTRS radios. Completion of the SRWNM FQT is a significant milestone in delivering an enterprisewide network planning and management capability for JTRS radios.

SRWNM enables planning of heterogeneous SRW networks consisting of SRW-capable radios from multiple vendors, generating the presets for the radios in the plan, downloading the presets to the planned radio nodes, and then monitoring the planned operational SRW network. SRWNM is a key component of the JTRS Enterprise Network Manager (JENM), which provides tactical network management product for all JTRS radios.

JENM enables planning, instantiation, management and over-the-air reconfiguration of tactical networks comprising software-defined radios from multiple vendors. That greatly simplifies network planning and operations as compared to using separate management products provided by each qualified radio vendor.

In addition to providing SRW planning and management for JTRS radios being developed on government contracts such as the Ground Mobile Radios (GMR) and Handheld/Manpack/Small Form Fit (HMS) programs, the SRWNM development and FQT included robust planning and management capabilities for the Harris AN/PRC-117G and ITT Soldier-Rifleman Radio.

Both of these radio products are being developed leveraging the JTRS Enterprise Business Model, which allows radio developers access to JTRS software capabilities for integration into their products without government contracts and funding.

The JTRS Enterprise Business Model is designed to stimulate competition, increase innovation and reduce government costs through software reuse while simultaneously speeding development and fielding of tactical networking capabilities. Inclusion of radio products developed under the JTRS Enterprise Business Model in the SRWNM FQT represents a unique government and industry partnership to aggressively deliver advanced tactical networking capabilities to joint warfighters.

Successful completion of the SRWNM FQT with these products included validates the JTRS Enterprise Business Model effectiveness and illustrates its ability to foster a competitive environment in the defense communications and networking industry. All SRWNM and JENM releases are also made available on the JTRS Information Repository to other authorized users within the Department of Defense and commercial industry.

Multifunction Terminals

In other news, the Multifunctional Information Distribution System Joint Tactical Radio System (MIDS JTRS) terminal has been cleared for limited production 2 procurement, following approval of an acquisition decision memorandum by Undersecretary of Defense for Acquisition, Technology and Logistics Ashton B. Carter.

"The MIDS JTRS limited production 2 decision is another major accomplishment for the MIDS program and the JTRS enterprise and advances the program one step closer to full production and the initial operational capability (IOC) milestone," stated Navy Captain Scott Krambeck, the MIDS program manager.

The MIDS program is one of five major ACAT 1D programs within the JTRS Enterprise. MIDS provides interoperable, affordable and secure tactical data link and programmable networking technologies and capabilities for the joint, coalition and international warfighter. MIDS JTRS is a software-defined networking terminal that is not only NSA certified with the Link-16 waveform, but is also equipped with Link-16 Enhanced Throughput and Link-16 Frequency Remapping.

The MIDS JTRS terminal has demonstrated continued maturity over the past year, and with the successful completion of this Limited Production 2 decision, the MIDS JTRS program has reached another significant objective on its path to delivering the advanced networking capabilities into the hands of the warfighter.

The MIDS Program Office is now authorized to allow MIDS JTRS to enter into a second limited production of 42 terminals for the Navy's F/A-18E/F Super Hornet, as well as the Air Force's EC-130H Compass Call and RC-135 Rivet Joint.

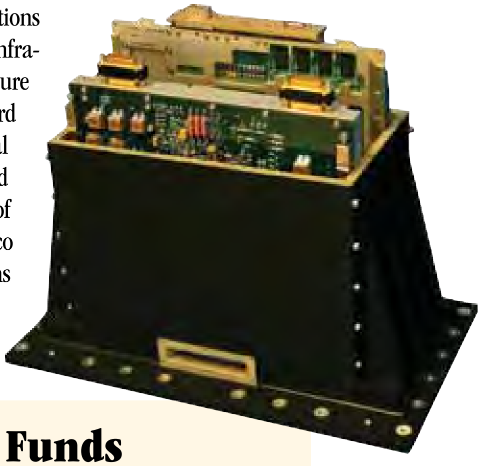
"While we still have some additional MIDS JTRS testing to conduct prior to full production and IOC, I am extremely pleased with the progress the team is making, the new trails we are blazing, and the lessons learned that we are sharing with our JTRS teammates. The outstanding government and industry MIDS JTRS team continues to advance and demonstrate JTRS technology, and soon the warfighter will benefit. I am anxious to get MIDS JTRS operating in the fleet." ✯

DATA

Compiled by KMI Media Group staff

Internet Space Router Solution Offers Bandwidth Optimization

TeleCommunication Systems (TCS), a provider of highly reliable and secure mobile communication technology, has entered an exclusive arrangement to be the operator of the Cisco Internet Routing in Space (IRIS) solution using the Cisco 18400 Space Router on INTELSAT IS-14, the most advanced commercial satellite platform available today. This industry-first solution enables the convergence of satellite communications and existing information technology infrastructure. By utilizing the benefits of secure Layer 3 Internet Protocol routing onboard the spacecraft, end-to-end IP virtual private network services can be offered directly from space with new levels of flexibility and network control. The Cisco 18400 Space Router allows organizations to reach multiple continents from a single connection to TCS' network infrastructure. The converged Cisco IRIS solution enables voice, data and video traffic over a single IP network to increase efficiency and flexibility compared to more fragmented satellite communication networks. Customers benefit from increased bandwidth optimization and application flexibility delivered by TCS through an end-to-end Cisco IP network.



Three Marine Bases Set for New Backbone Transport Network

General Dynamics Information Technology has been awarded a $9.3 million, eight-month task order to perform network systems integration for Marine Corps Systems Command under the U.S. Air Force Network-Centric Solutions contract. Under this contract, General Dynamics will engineer, design, install and test a new dense wavelength division multiplexing backbone transport network at three Marine Corps bases. This project will modernize the base networks and enhance communications technology. The work will be performed at Camp Pendleton, Calif.; Marine Corps Recruit Depot, San Diego, Calif.; and Camp Lejeune, N.C. Dense wavelength division multiplexing is a technology that combines multiple communications signals and sends them simultaneously along a single fiber. The communications signals may include data, voice, video, Internet Protocol ATM and SONET. This technology enables increased capacity, faster transmission times and easy expansion of capacity.

Contract Funds Communications Support for NATO in Afghanistan

Segovia, a wholly owned subsidiary of INMARSAT plc and a provider of secure, global telecommunications to the public and private sectors, has been awarded NATO's Communication Information Services (CIS) Consultant Support Services indefinite delivery/indefinite quantity contract (IDIQ) to provide professional and technical services support to the International Security Assistance Force in Afghanistan. The IDIQ has a four-year period of performance if all option years are exercised. Segovia was also awarded the first task order under the IDIQ—a multi-million dollar contract to deploy full-time communication and information services support to Kandahar, Afghanistan. Under the contract, Segovia's expert consultants will provide CIS support to NATO operations. The communications support meets a critical need for NATO units operating in Afghanistan. The IDIQ and task order awards follow the recent expansion of Segovia's engineering and professional services to include a new Technical Services division, which provides Segovia customers with a host of full-time consultants specializing in LAN/WAN management, functional services, training, systems administration, repair/exchange, configuration management and other key services.

Configuration Software Supports Dismounted Comms System

PacStar, a technology-based provider of communications solutions to the military and government, has reconfigured its IQ-Core Software product for use in General Dynamics C4 Systems' Dismounted Company Command Post (DCCP) communications system. The IQ-Core-based software enables users to train and operate the DCCP faster and more efficiently. DCCP is an expeditionary communications system intended for the Department of Defense. IQ-Core Software automates routine, difficult, or error-prone setup, configuration and management tasks. The software also reduces setup time and improves system uptime by reducing mis-configuration errors. IQ-Core Software is especially valuable in reducing the complexity of tasks related to the deployment of unified capabilities that provide voice, data, video and application services in the field. IQ-Core Software has been proven in the field and has been Joint Interoperability Test Command-certified on five different platforms. IQ-Core Software is embedded in PacStar's broad product family of software-managed deployable communications solutions, including the PacStar 6000 and PacStar 4000-series solutions, which deliver IP and TDM connectivity to defense networks including NIPRNet, SIPRNet, JWICS and CENTRIX-ISAF as well as DoD Defense Switched Network voice and data services and VoSIP.

Marines Buy More Tactical Collaborative Systems

The Marine Corps has awarded iGov, prime contractor for TACLAN and provider of evolutionary tactical network systems and support programs, a firm fixed-price modification to the Tactical Collaborative Work Suite (TCWS) contract. A previous contract worth $25 million for similar work was awarded to iGov in June 2010. The modification, worth a maximum value of $12.3 million, is for the production of an additional 60 TCWS systems. The primary purpose of the contract modification is to begin full-rate production of the TCWS 2.0 hardware platforms. TCWS is a man-portable tactical collaborative system comprising a virtualized hosting platform, segmented physical hardware and virtualized software platforms that provide portal, synchronous and asynchronous collaboration capabilities to support Marine Air Ground Task Force Operations. The initial contract called for iGov to design, develop, build, test and deliver two low rate initial production systems. IGov's ability to quickly design, test and produce reliable, modular virtual hosting platforms that support information sharing services and applications, has resulted in a smaller, lighter weight, ruggedized, modular and scalable standardized capability set that allows for Marines to deploy, manage, and maintain tactical and collaborative services.

SPAWAR Orders More Multifunctional JTRS Terminals

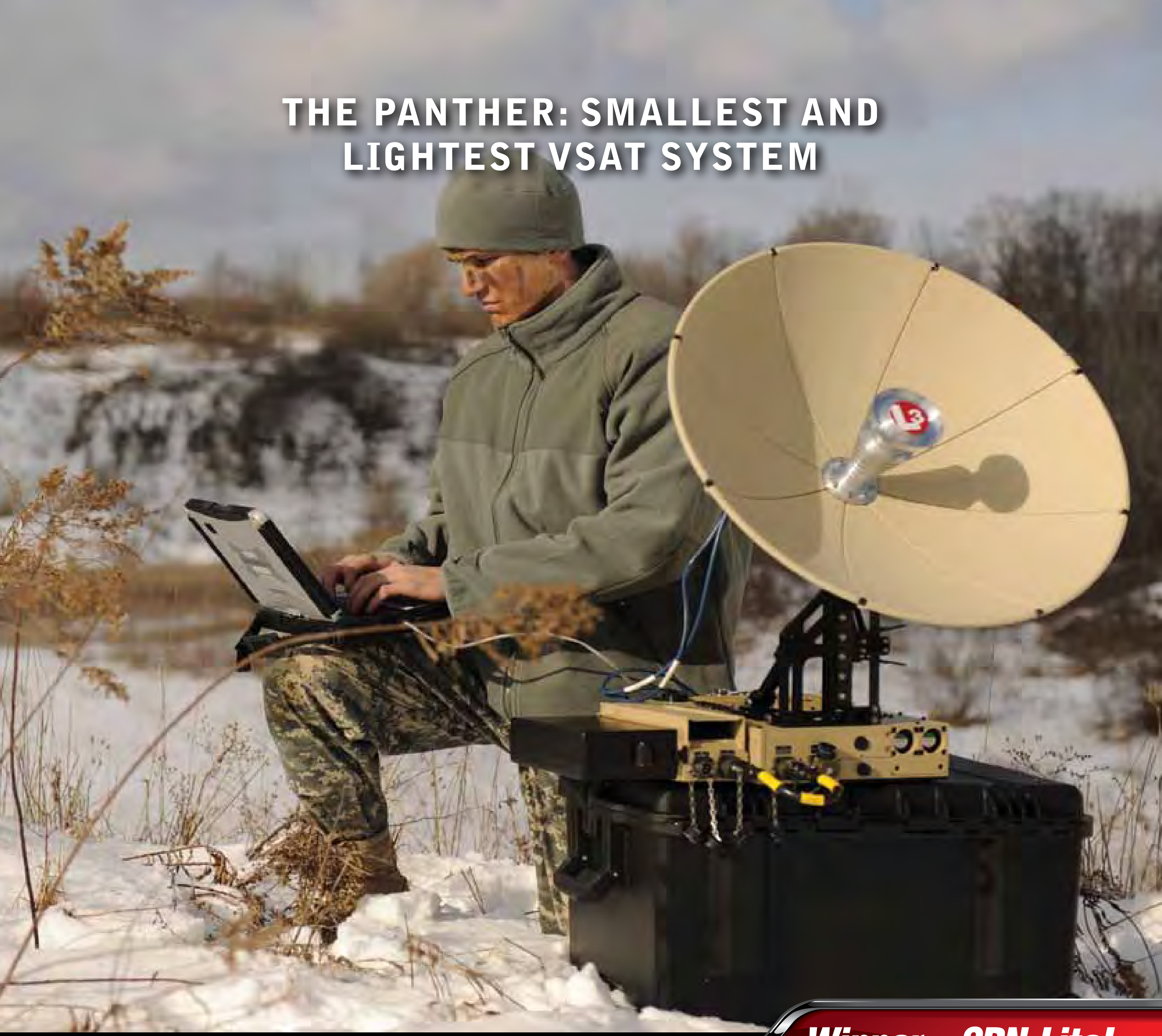
ViaSat has been awarded a limited production order valued at $6.8 million for Multifunctional Information Distribution System Joint Tactical Radio System (MIDS JTRS) terminals for the U.S. government. The award resulted from a competitive procurement through the Space and Naval Warfare Systems Command (SPAWAR). The order was awarded under the MIDS indefinite delivery/indefinite quantity contract initially executed in March 2010. The MIDS JTRS terminals are for F/A-18E/F, RC-135 Rivet Joint, and EC-130H Compass Call aircraft. MIDS JTRS is a joint development of ViaSat and Data Link Solutions and provides a migration path from the MIDS-Low Volume Terminal (LVT) to a certified, reprogrammable, software-defined radio architecture for tactical data links. The terminal has completed contractor and government qualification testing, and received the following certifications: Software Communications Architecture compliance, electromagnetic compatibility certification, Joint Interoperability Test Command interoperability and NSA security certification. ViaSat expects to enter full production and fielding in 2011. The MIDS JTRS adds three programmable channels to the legacy Link-16 and TACAN capabilities of the MIDS-LVT. The three new channels are designed to host future advanced airborne networking waveforms. MIDS JTRS is "plug and play" backward compatible with MIDS-LVT so it can easily replace the MIDS-LVT, but remain interoperable.

DIA Seeks Revamp of IT Infrastructure Services Delivery

The Defense Intelligence Agency (DIA) has announced the award to BAE Systems of two competitive, five-year task orders under the Solutions for the Information Technology Enterprise contract totaling approximately $350 million. BAE Systems will implement its enterprise services delivery model to significantly improve the effectiveness and quality of IT services delivery across the full spectrum of back office, field services, customer care, close support services, network services and missions applications operations for DIA's support of the warfighter. The Customer Engagement and Field Support Services Task Order and the Enterprise Operations Services Task Order both address the DIA's transformational program to re-invent the agency's IT infrastructure services delivery at all unified combatant commands. BAE Systems is teaming with a number of partners and suppliers in this effort. They are Accenture, L3 Stratis, SAIC, Vykin, Cyberspace Solutions, DSA, ISYS Technologies, Mainstreet Technologies, NES, Nova Datacom and Primescape.

Carrier's New Mast Offers Latest in Communications Technology

Northrop Grumman recently completed a significant work performance milestone on the Nimitz-class aircraft carrier USS *Theodore Roosevelt* with the installation of the final section of the ship's main mast. The carrier is undergoing a refueling and complex overhaul at the company's shipbuilding sector in Newport News, Va. An important aspect of this availability includes modernizing the ship's island with the latest technology and installing a new main mast. The 70-ton structure provides a platform for radar and communication systems high above the ship for maximum coverage. During refurbishment, the original round mast pole was removed and replaced with a modified, tapered square pole to increase strength and keep electrical and piping systems enclosed for survivability purposes. It is also larger, which allows for waist-high safety rails and easier access to all areas by internal ladders.



Efficiency Implementer

Q&A

Meeting Demands Within Stringent Budgets

Gary L. Winkler
Program Executive Officer
Enterprise Information Systems
Army

Q: In light of the stringent budget outlook, how would you describe your overall strategy for increasing efficiency at PEO EIS?

A: With the financial situation our country has been in for the past several years, we've been expecting significant budget cuts and preparing for reductions for the past two years. First, we established portfolio integration officers [PIOs] over subsets of the PEO EIS portfolio. The PIOs are really using simple knowledge management techniques to optimize our project managers' [PM] efforts. They identify and communicate among our PMs where we can leverage common technology and products, share lessons-learned and implement similar cost-reducing and streamlining processes, and utilize pre-existing contracts. Our PIOs are senior leaders who have previously been accomplished PMs themselves, so they speak with experience and authority when trying to assist our PMs. Our PIOs helped us increase our output from the previous year in several areas, as we: reduced our contract cycle time by 11 percent for 4,900 contract actions; achieved a cost avoidance or savings of $800 million; took on a new service contracting mission [human resources solutions]; and delivered 235 new major capabilities to over 2 million joint users at 500 locations worldwide.

We also conducted a Lean Six Sigma Black Belt project to look at program overhead rates throughout the PEO and challenged our PMs to decrease the proportion of their program's funds that are spent on program office operations versus product development and fielding. We believe that decreasing this type of "overhead" associated with our program offices is an acceptable risk to ensure that we continue providing timely capabilities and high-quality support to warfighters. We've instituted an ongoing review and analysis of overhead within the PEO and PMs, directing PMs and internal staff to make organizational, staff and contractor support realignments and reductions to meet a goal of reducing overhead to 5 percent.

Lastly, we are working closely with the functional proponents [the customer of the systems we develop] to ensure that documented system requirements accurately articulate the customer requirements—nothing more and nothing less. Our current funding posture does not allow us to implement "nice to have" capabilities, but rather dictates that we design, develop and field critically needed capabilities that can be enhanced in the future, if required and if funding is prioritized accordingly. The bottom line is that we are being as creative and disciplined as possible to ensure we can continue to meet the demands placed upon us even with stringent budget outlook ahead.

Q: What steps have you taken to follow the efficiency guidance issued last summer by Under Secretary of Defense for Acquisition, Technology and Logistics Ashton B. Carter?

A: It's very helpful to have DoD's most senior leaders driving the ideas and processes to help us "do more without more." Not only has Dr. Carter said we must be more efficient and cost-effective, but he also has outlined the areas and methods where our efforts can reap the most benefits. In the area of "mandating affordability as a requirement," we have: developed acquisition strategies that fit funding profiles and budgets; pushed back on requirements creep; used firm fixed price contracts where appropriate; and created multiple strategic sourcing contract vehicles for both equipment and services. To "incentivize productivity and innovation in industry," we have: structured our contracts to use "option years" as incentive for continued support; sponsored five phase I and phase 2 Small Business Innovative Research; and used the Contractor's Performance Assessment Reporting System to capture past performance.

To "promote real competition," we: ensured that the government has the rights to source code, intellectual property and data rights; are using ISO and similar standards; are reviewing each program's competitive procurement strategies at quarterly program reviews; and are working extensively to support small business development by participating in small business forums. In fact, in 2011, we expect small business opportunities to be close to $7 billion, or 26 percent of all PEO EIS contract awards.

In the area of "improving the tradecraft in services acquisition," we have been a key participant in working groups to shape the Army's new position for the deputy assistant secretary of the Army for services. We have taken over the mission for the human resources [HR] solutions service contracting program, and are still doing our information technology services mission we have been doing well for years. Lastly, we are making sure that contracts accurately reflect the right product service code. Services represent a great opportunity for small businesses, and we have ensured that small business participation is a significant percentage of all service contract tasks, such as with HR solutions, where 61 percent of the $4.2 billion contract portfolio is reserved for small businesses.

Q: What results have you achieved from deployment of the Lean Six Sigma [LSS] approach to project management?

A: This is related to another one of Dr. Carter's efficiency initiatives, "reducing non-productive processes and bureaucracy." Our LSS deployment has made great progress over the past year in deploying a culture of learning and change throughout the organization. Ninety percent of our active work force has received LSS awareness training and it has really paid off, as folks are actively identifying areas that can benefit from projects. To date, we have 31 certified green belts and nine certified black belts on our staff. Since 2007, we've achieved more than $278 million in documented cost avoidance or savings. We completed 31 LSS projects this past year, which is more than double the number of projects in 2009. In addition, we achieved a level 4 maturity rating from the Army's Office of Business Transformation, moving two levels higher than a year ago and only one level away from full maturity. We've also enjoyed Army headquarters-level success as one of our green belts, Regina Bumper's team, won the Army's prestigious 2010 LSS Excellence Award Program [LEAP] for their green belt project, "improve PEO EIS in- and out-processing." We were quite honored with the LEAP Award given all of the successful LSS projects submitted throughout the Army.

But I believe that one of the best benefits of LSS that is never captured in all of the metrics noted above is the very real benefit that LSS has on developing our work force. LSS is a forcing function to get folks knowledgeable in tasks and functions outside of their area of expertise. All of the tough, hard work in any business lies between the seams of functions and organizations, and LSS looks at processes that cross those boundaries. Over the past three years, I have seen significant growth in our people's multi-functional knowledge and competencies—it is very satisfying. In fact, one of our LSS black belt projects spawned the development of a PEO EIS human capital strategic plan. If we are going to "do more, without more," then our people must possess multi-functional skills and experience to tackle our tough challenges. I personally have committed to sponsor two LSS enterprise-level projects each year. Our LSS "optimize PEO EIS overhead" black belt project was recognized by ASA [ALT] for project replication across all PEOs. So, we are not just complying with LSS policy; we embraced it, internalized it and are using it to propel our organization to new heights. Hooah!

Q: What role is PEO EIS playing in the Army's data center consolidation initiative?

A: Cloud computing is transforming the IT industry, and the federal government, DoD and Army are jumping on board. PEO EIS was pivotal in the Army's server consolidation initiative years ago, and data center consolidation is the next step. We first started planning for data center consolidation when Lieutenant General Peter Cuviello was the Army CIO/G-6, and under Lieutenant General Steven Boutelle, we implemented the first two Army data centers in DISA Defense Enterprise Computing Centers. However, in addition to government-owned and -operated data centers, many federal organizations are also leveraging the power and economies of commercial data centers. My office currently has a procurement called "Army private cloud," undergoing source selection, that will provide the Army and select DoD organizations with commercial data center services. The procurement includes both fixed data centers as well as containerized data center capabilities. Army Materiel Command's Software Engineering Center is designated to assist organizations with moving applications to approved data centers. My office is providing procurement support and subject matter expertise, specifically in cost estimating and technical advice.

Q: What do you see as the key challenges facing the data center consolidation project?

A: There are two main challenges with the data center consolidation initiative. The first is the cost to migrate applications from hosted location to another data center. That cost will vary between applications and is not being centrally funded, which means that each application owner will have to fund moving the application. I would expect that applications will migrate to approved data centers when it is economically advantageous and affordable, most likely when significant hardware refresh/updates are required. Secondly, the Army's global network does not have uniform capabilities throughout the globe, so application owners will have to do some analysis as to the data center location to host their system to serve their user community. Consolidating 300 data centers represents a significant engineering and logistical effort, and like everything else, declining budgets and competing priorities will come into play.

It almost goes without saying that, in order for the data center consolidation initiative to be successful, system/application performance will have to be at least equal to current levels at much reduced costs, or performance will have to be significantly better [if required] at equivalent costs. In addition, users want to be able to obtain assistance when problems arise, and they are used to having that locally. Turning the control over to a third party to manage and administer may be a difficult mindset for many units.

Q: Your office recently issued a request for information [RFI] on software development for mobile devices. What is your vision for how this type of technology will transform Army operations?

A: The wireless mobile device revolution is ongoing, and the Army is going to capitalize on it with secure mobile device computing. The idea is that we want to harness the power of soldiers and civilians to create and share mobile device applications throughout the enterprise. The Global Network Enterprise Construct objective is global, secure, ubiquitous access to a soldier's applications, data and network services. Secure wireless devices are part of this vision, as are all application that can ride on those devices. Ultimately, we would like to extend our large enterprise-class systems to mobile devices, but in the interim, soldiers and organizations can benefit from more simple applications to streamline mission tasks no matter where the user is located. Ideally, users will no longer be tethered to an office or wired network to securely access their data, applications or network services, but will be able to work from anywhere.

The RFI was intended to do some market research in advance of releasing a request for proposals [RFP] to industry for development of applications for smart phones. We plan to issue that RFP this year, and once awarded, any Army organization that needs mobile device applications to support their operations will be able to award a task order under that contract.

Q: The RFI mentions plans to open a "store" for mobile apps. How do you plan to proceed with this and other aspects of mobile-device technology development?

A: This concept is something that private industry has been doing for some time. The Army will need a capability to upload and download apps that people or contractors will write. There are several prototype app stores in existence throughout DoD, and we are looking at those. However, we will need the capability to either build out those prototypes, or develop a new apps store. The procurement should be of sufficient scope to allow us to go either way. But we need to hurry because users are already starting to write and share mobile applications, and they need a place [apps store] to do this securely.

Q: According to some media reports, a number of users are expressing dissatisfaction with Army Knowledge Online [AKO]. How do you respond to criticisms of slow performance and other issues, and what changes if any are you looking at in its operations and technology?

A: We view all feedback as a method of identifying areas where we've got it right—and where we can improve. AKO routinely polls users on a variety of topics. During one of their recent polls, they asked users what they thought of AKO. Out of almost 20,000 responses, 4 percent indicated that they don't like it, 17 percent said they use it because they have to, 49 percent gave it an "OK," and 30 percent said AKO was "awesome."

User satisfaction has always been one of our highest priorities, with all of our systems, and we'll continue to work toward getting 100 percent of the users to think AKO is "awesome." We've made recent changes to enhance both security and performance and, unfortunately, not everyone is happy with the changes. One security enhancement was the implementation of knowledge-based authentication [KBA], which requires users logging in without a Common Access Card [CAC] to answer three questions that they had previously selected. KBA has proven to be effective against keystroke-logging software and is common practice in industries where security is a concern. We have gotten negative feedback about this change, but it is necessary as security comes first.

On the performance side, AKO conducted a thorough analysis of its architecture to identify areas for improvement. We made a number of changes a few months ago and are in the process of implementing blade technology that will yield additional capacity in storage and throughput. We also procured additional tier 2 storage, which is less expensive and allows us to expand e-mail storage. Both of these upgrades will improve performance.

When investigating specific complaints, we often find that local networks don't have the adequate bandwidth for their user community and, as a result, all users on that local network experience poor performance; this is not an AKO problem. Technical teams regularly collaborate with network service providers to optimize network performance on both sides.

The AKO contract will be up for recompete shortly, and we are looking to both simplify the architecture and lower costs. I also have to note that AKO now has a CAC-enabled iPhone solution for its e-mail and calendar system, so it's leading the way in secure mobile computing in DoD!

Q: After a number of years of work in the military in implementing enterprise resource planning [ERP] systems, what

is your current thinking on the effectiveness of this approach? Has this concept's time come and gone?

A: Definitely not. The Army has a sense of humor—I hated ERP systems, so they put me in charge of implementing them. But seriously, our ERP programs have come a long way and are doing well. We are now fully deployed with the Army's Logistics Modernization Program supporting our depots and arsenals, and we are about 30 percent deployed with the General Fund Enterprise Business System supporting our financial community. The Global Combat Support System-Army is poised to undergo its initial operational test and evaluation later this summer, en route to a fielding decision. Our ERP challenge has been two-fold: evolving our business processes to optimize our investment in the COTS ERP product, and getting smarter on ERPs in order to properly allocate functionality between them, and to know how and when to configure the ERP versus implementing a "bolt on" capability or meeting a requirement some other way.

The Army's chief management officer has rallied the Army staff and other ERP stakeholders over the past five months to examine our programs to see what refinements we may need to make in governance and program execution. The result is a refined ERP strategy that the secretary of the Army will likely approve soon. This new strategy contains some changes to ERP governance, as well as functional allocation between ERPs and other programs of record. It also lives within the current cost, schedule and performance baselines of the current programs, thus no cost growth or schedule slips. We will present the details of such refinements when any of our ERP programs goes to a milestone decision review with OSD.

Q: How has the standup of U.S. Cyber Command and ARFORCYBER affected PEO EIS operations and policies? What is your office's role in countering the cyber-threat?

A: Army systems are attacked constantly from multiple sources. Standing up U.S. Cyber Command, and particularly the ARFORCYBER, puts the emphasis that was needed on this growing threat.

Major General Rhett Hernandez, the new ARFORCYBER commander, visited PEO EIS in January with Major General Susan Lawrence, the Army's incoming CIO/G6. We had some great discussions on how our three organizations can work together to ensure our systems and data are secure, and our networks protected. The role of PEO EIS is to build the Army's systems and networks. In that regard, we look to ARFORCYBER and CIO/G-6 for the requirements to which we build to. As with all of our systems, we take sustainment into account, therefore coordination with NETCOM [under ARFORCYBER] is always critical when building our systems because NETCOM will operate and manage our systems once they achieve full operational capability. We are looking to CIO/G-6 and ARFORCYBER to develop policies relating to secure mobile devices and accreditation of smart-phone applications. To date, no accreditation process exists in DoD or the Army to approve smart-phone applications for use on the network.

Hari Bezwada, our new chief information officer, has restructured his organization to create a PEO EIS CIO Cyber Office and has expanded its mission to include threat collection, analysis and dissemination, security engineering, and network operations in collaboration with the Army Global Network and Operations Center. This positions us to take a more pro-active approach to cybersecurity.

Our partnerships with ARFORCYBER, NETCOM, CIO/G-6 and ASA [ALT] have continued to grow stronger with regular, synchronized meetings with our cyber-staff. The staff is working with all PMs to ensure knowledge dissemination and coordination. With this added emphasis on cybersecurity, we are in a better position to protect our networks.

Q: What message would you most like to communicate to industry about how it will work with your organization in 2011?

A: We value our industry partners and really appreciate their flexibility in working with us through these tumultuous times. We will be very cost conscious, and ask our industry partners to do the same. Our large programs will be targeted for significant funding cuts, yet there will be many opportunities for many small, quick-turnaround efforts that provide immediate capability and/or immediate return on investment. I would advise our industry partners to make sure they are accessible through pre-competed contract vehicles, and to keep attuned to evolving Army efforts and focus areas. They need to recognize and know what our needs are, and then be ready to respond. We will have to obligate our funds quickly [putting them on contract], or risk the chance of funds being taken for other projects if not quickly put to good use. Build relationships in order to stay tuned into what the Army needs and when we need it. Lastly, take a look at Dr. Carter's efficiency initiatives so you know where our sensitive spots are, and maybe how you can help us meet our fiscal objectives. LSS isn't just for the government, and our industry partners might be able to help us meet our mission more cost-effectively by implementing LSS inside their organizations to lower costs to the government, allowing us to acquire more capability for our warfighters. We need industry to think out of the box and help us find those ways to get capabilities out better, faster and cheaper!

Q: What are some of the most noteworthy contract opportunities from your office coming up in 2011?

A: It seems we always have contract opportunities in various stages of solicitation, with several RFPs on the street now or being finalized. I already talked about some of our secure mobile wireless procurements and data center procurements. However, a couple more big ones planned for this year are worth mentioning: the Communications and Transmission Systems [CTS] and the Information Technology Enterprise Solutions-3 Hardware [ITES-3H] procurements.

CTS will be released later this fiscal year. The scope for this contract includes almost all the communications and transmission systems currently controlled by the Project Manager Defense Communications and Army Transmission Systems. This is a multiple award indefinite delivery/indefinite quantity [IDIQ] contract. We anticipate 10 awardees, with three awards reserved for small businesses.

ITES-3H is scheduled for late this year. This is a follow-on to our current ITES hardware IDIQ contract. It is also a multiple award with small business reserves. With the increased oversight required for these large contracts, we have to build in more time for reviews and processing.

Q: Your office oversees so many programs and projects that some no doubt get lost in the shuffle. What are some of the "unsung heroes" that may not have received the attention they deserve, but you would like to highlight here?

A: I can assure you, nothing gets lost in the shuffle. Some of the projects just don't have the high visibility of AKO or biometrics, but they are still critical to their users. The Reserve Component Automation System [RCAS] is one of those programs. RCAS supports the Army National Guard and Army Reserve component, which makes up more than 50 percent of our war fighting force. The RCAS suite of systems provides web-based functionality across the personnel, force management, mobilization and safety management arenas and connects every reserve component unit across the 54 states and territories and reserve units permanently located in EUCOM. The flagship application in RCAS is the Mobilization Planning Data Viewer [MPDV].

MPDV plans and executes mobilization activities and movement to mobilization stations located on Army power projection platforms. The visibility and importance of this functionality skyrocketed following the September 11, 2001, attacks because of the unprecedented volume and pace of reserve mobilizations for deployment to Southwest Asia. MPDV was originally developed as an administrative tool to replace the endless binders of unit personnel readiness and training status information. It quickly became a true combat multiplier, allowing leaders to spend more time conducting training than digging through stacks of paperwork to identify issues impacting individual soldier deployment readiness. Because of its flexibility, the National Guard Bureau recently began using MPDV to support traditional National Guard missions—natural disasters and homeland defense.

The Army's active component is testing MPDV to streamline soldier readiness processing [SRP]. Every soldier has spent mind-numbing hours standing in line to verify personnel and medical tasks before they can be certified ready to deploy. The SRP module within MPDV is a "common operating picture" that provides the unit and installation-level leaders a single source for visibility into soldier readiness. This "virtual SRP" identifies soldiers who have specific deployment deficiencies and then only those soldiers report to the installation SRP site to have these deficiencies addressed.

RCAS is currently conducting an exercise at Fort Hood, Texas, using MPDV's SRP module to prepare a division for deployment to Afghanistan. The exercise will formally assess the ability of the SRP module to reduce the time soldiers spend standing in line at SPR sites, freeing them to complete their pre-deployment training or spend time at home with their families. You can imagine the thousands of hours that may be saved using this tool.

This is the type of "out of the box" thinking I was referring to earlier. Rather than develop a new system, we are using current capabilities and saving the Army a lot of time and money. ✯

SATCOM for ISR

Ability to shift SATCOM capabilities within minutes enables planners to quickly react to new missions.

*(**Editor's Note:** *Military Information Technology* recently posed the following question—based on a discussion topic of a workshop scheduled for the Satellite 2011 conference in Washington, D.C., March 14-17—to some of the leading companies in the field of commercial satellite communications: "What role do you see for the commercial SATCOM sector in providing connectivity for government/military UAVs and ISR capabilities?" Following are their responses.)*

Embrace the Investments

Commercial SATCOM players stand ready to introduce new delivery approaches that will provide the government with enhanced service and performance.

By Andy Beegan, Senior Vice President and Chief Technology Officer
Segovia Inc.

The commercial SATCOM industry is well-positioned to provide U.S. government UAV and ISR users with significant increases in connectivity performance and cost efficiency, particularly through global managed services providers. Antiquated processes, however, currently create a formidable barrier to entry and keep government from fully benefiting from the commercial sector.

Ten years ago, as U.S. military activities ramped up overseas, commercial SATCOM was quickly integrated as a significant component of Department of Defense mission planning. Today, commercial SATCOM could play an even more central role because of advances in technology and the development of more mature and repeatable service delivery methods. Deploying these delivery methods is quick and secure, and reduces the per-unit cost of satellite bandwidth.

These advances are particularly important to UAVs and ISR, which rely on airborne applications that require four to eight times the space segment to deliver equivalent data rates compared to land-based VSAT links.

As was the case with land-based networks 10 years ago, UAV and ISR communication platforms are currently limited by legacy terminal hardware, rigid airborne certification requirements and outdated spectrum usage. All of these issues form a major obstacle to the introduction of new solutions that would be more cost efficient and use bandwidth more effectively.

Given that the satellite space segment is the primary commodity cost factor in an end-to-end network solution, government should look to the commercial SATCOM industry's managed services providers. They have demonstrated significant value by maximizing the efficiency of space segment utilization as a core driver of their business operations, and can transfer the cost savings to government customers. Furthermore, managed service providers lean forward to make the necessary investments that produce a

WE BOTH AIM TO BE AGILE

That's why we fully equip ourselves to quickly deliver the communication infrastructure and connectivity that you need to maintain your speed of command and remain nimble in battle. Agility is what allows us to confidently stand accountable for every component of your network, ensuring that it runs uninterrupted, remains interoperable and features the flexibility, security and speed you need for a faster and stronger networked force – with improved information sharing, collaboration and situational awareness; greater sustainability of forces, speed of command and ready-access for global mobility and rapid response across the GIG.

From the core to the edge, anytime, anywhere, Segovia keeps you moving.

Visit www.segoviaip.com/agile
to download your FREE *Segovia Solutions for Defense* Kit.

segovia

Segovia features a suite of end-to-end global communication solutions, offered through a world-wide network of integrated and scalable, custom-fit communication hardware and services. Our customers trust us for our fully-managed, secure, global, redundant terrestrial and satellite infrastructure. With our DIACAP accreditation, 99.9% network availability, and 24/7/365 U.S.-based network and technical support, Segovia remains a value-added partner of the defense community.

▪ 866-SEGOVIA ▪ WWW.SEGOVIAIP.COM ▪ INFO@SEGOVIAIP.COM total solution, not just the components, offering both savings and capabilities to the government.

Providers such as Segovia offer far more than raw bandwidth bundles. They engineer, build and manage communications infrastructures designed for customers' specific needs and situations. Services such as monitoring can bring down costs, through careful management of the transponder loading, for example, while simultaneously improving bandwidth efficiencies and increasing the quality of mission-critical communications.

The commercial SATCOM sector is highly adaptable and agile, and as a result, can also achieve increased efficiency through the implementation of new and emerging technologies. In particular, the emergence of Ka-band platforms will deliver greater capability at a lower cost per bit than the traditional Ku- and C-band operators.

As the UAV and ISR market continues to expand, the government needs to embrace the investments that commercial companies are making in this space that will enable the next generation of UAV and ISR applications. The benefit from the commercial SATCOM players who stand ready to introduce new delivery approaches will provide the government with enhanced service and performance with greater value.

Critical Link in UAV Operations

The satellite industry is accelerating its capacity to support high-bandwidth requirements like those imposed by advanced ISR systems.

By Britt Lewis, Vice President, Marketing and Business Strategy
Intelsat General Corp.
britt.lewis@intelsatgeneral.com

Time magazine ran a cover story recently on singularity, which is the concept that robotics and artificial intelligence are progressing so rapidly—indeed at an exponentially accelerating rate—that by 2045 we can expect a "cyborganic" environment in which civilization is completely and irreversibly transformed.

Nowhere is this envisioned robotic transformation and impact seen more readily today than in the military's use of UAVs. Indeed, over the last decade or so, the military has seen such an evolution in technology that today, the warfighter has the capability to project power through the use of remotely piloted/unmanned systems that reduce risk to human life while also improving the timeliness of battlefield situational awareness.

Largely behind the scenes in the transformation from manned to unmanned flight lines, however, is the critical role of satellite communications as an enabler of semi-autonomous and, in the future, fully autonomous UAV flight. Reliable satellite communications are a critical enabler for medium- and high-altitude UAVs. Increasing demand for UAVs overall and the increasingly sophisticated sensor suites employed on the vehicles have dramatically increased demand for satellite services.

UAVs have been the most dynamic growth sector of the aerospace industry in the past decade. The Teal Co. expects that trend to continue, projecting that U.S. government spending on UAVs will grow from $3 billion in 2011 to approximately $49 billion by 2020 for medium- and high-altitude combat-equipped UAVs. Based on a static operations tempo scenario, Intelsat projects the U.S. government alone will operate some 800 high-capacity, long-range, high-endurance missions annually by 2018.

For the Predator and Reaper, both of which are medium-altitude, long-endurance UAVs, product roadmaps call for data rates climbing steadily to more than 45 MBps, from today's range of 3.2 to 6.4 MBps. Similarly, the very high altitude long endurance UAVs like Global Hawk and the Broad-Area Maritime Surveillance vehicles will progress to 100s of MBps in the future, from 8, 20 and 47 MBps throughput today. This higher throughput is being driven by high-definition cameras, multiple video feeds, wide-area airborne surveillance radar, and modular, multi-intelligence payloads.

Manned ISR platforms are also transitioning from narrowband communications using L-band satellites to wideband commercial and military SATCOM, creating even greater demand for high-capacity bandwidth. Based on the progression of data rates described above, Intelsat projects that ISR bandwidth demand will reach 16GHz by 2018. This is more than double the commercial SATCOM in use today to support operations in the Middle East.

Moreover, Intelsat foresees that there will be a global expansion of UAV operations, UAV capabilities will be apportioned to combatant commands beyond CENTCOM, and coalition partners will make greater use of this technology. In short, assuming a continuing high operations tempo into the future, Intelsat's expectation is that this proliferation is likely to challenge the availability of bandwidth for years into the future, whether on wideband MILSATCOM or commercial SATCOM.

The satellite industry has been successful in supporting this recent growth due to the scale and flexibility inherent in commercial satellite fleets and the frequent technological upgrades offered by robust fleet replenishment schedules. Intelsat and Eutelsat, for example, have redeployed satellites and steerable spot beam capacity over Southwest Asia to meet the current bandwidth demands for UAVs in the CENTCOM area of responsibility. Intelsat today provides some 1 GHz of total wideband capacity, representing more than 50 simultaneous flights of manned/unmanned ISR missions in a number of theaters.

Intelsat believes that changes in the UAV concept of operations can improve the efficiency and effectiveness of the UAV's use of satellite capacity. Such changes might include the use of inclined-orbit satellites as a low-cost alternative to station-kept satellite capacity; increasing the flexibility of the ground control stations to provide greater spectrum/frequency band access and flexibility; more aggressive coding efficiencies to reduce bandwidth usage; and enhanced video compression techniques.

Intelsat is working with satellite manufacturers on specialized payloads, some with the economic advantages of hosted payloads, for next-generation capabilities that would provide dramatic increases in overall bandwidth. These new payloads will also have coverage flexibility, connectivity, gain and wideband channelization that will allow operators to support many additional airframes at much higher data-throughput rates. With a satellite launch cadence of three to five spacecraft per year at minimum, the continuing advances in these future customized UAV-friendly payloads should offer superior long-term performance for UAV operations over the satellite assets flying today. The industry is also evaluating additional security features that can be built into the next generation satellites to enhance overall service resilience.

The critical link in UAV operations is now, and will continue to be, satellite bandwidth. The satellite industry is accelerating its capacity to support high-bandwidth, sophisticated requirements like those imposed by UAV operations. Careful and far-sighted cooperation between government requirements and commercial capabilities will be essential to the success of this enterprise.

Flexibility and Security

Ability to shift SATCOM capabilities within minutes enables planners to quickly react to new missions.

By Jim Ramsey, President
MTN Government Services
james.ramsey@mtnsat.com

Whether an ISR/UAV is deployed to swoop over the mountains of Afghanistan or quietly track potential threats in Iraq, the commercial SATCOM sector delivers solutions that are flexible enough to adapt to rapidly shifting missions and environments, within a highly secured network environment.

Most of us within the commercial SATCOM community have the ability to quickly re-groom, re-shape and even re-allocate committed information rates or maximum information rate within minutes. This gives the mission planners and our intelligence community the ability to quickly react to new targets or new missions.

This is especially true for a company such as MTN Government Services, which owns its own teleports, satellite hubs and 24/7 network operations centers (NOC). We have the ability to optimize bandwidth within the area of operations to perform best in specific missions and/or requirements. We can do this within minutes, with a simple call to our NOC. Our community can also see across various satellites, to spot beams and regions throughout the globe and identify the best solution for the government in relationship to the mission(s). This means the customers won't be stovepiped into a single solution. It allows us to plan a seamless transition from coverage to coverage. It's essential for any commercial SATCOM service provider to understand the underlying military mission and the requirements. Because we do, we provide the best possible solutions for the government.

Within this industry sector, we clearly understand the mission and the critical deployment of UAVs and ISR mission. We know our support can't fail—not when lives and global security is at stake. We strive every day to improve our services and sharpen our skills and technology, to support "those who do so much for all of us."

COMSATCOM Flexibility

Commercial solutions can accommodate smaller remote antennas and unique waveforms to create more cost-effective solutions.

By Steve Johnson, Director, Government Services
Globecomm
steve.johnson@globecommsystems.com

It is vital to the security of any nation to defend its borders and analyze both manmade and natural threats while also monitoring conditions that enhance quality of life. Autonomous aerial vehicles (AAVs) and ISR programs play an integral role in facilitating homeland security.

As a satellite communications integrator, Globecomm has been keenly engaged in the development of AAV communications services, specifically for ISR applications. Over the past few years, the company has investigated and modeled various technologies and modulation techniques to maximize the bit-per-dollar ratio.

When a government, NGO or private organization is interested in data collected by an AAV, that data still has to be transported from the vehicle to the ground in an effective, efficient manner that retains the integrity of the data. Today the cost of the payload transport is relatively high because of the current usage of relatively inefficient links over the COMSATCOM constellation.

MILSATCOM is not a realistic option because of the large amount of bandwidth required for this transport and the fact that MILSATCOM is being used for other critical tactical missions. The challenge to industry is to make the link more efficient and cost effective while supporting the ever-growing mission of any single AAV or fleet.

COMSATCOM is more flexible in accommodating smaller remote antennas and unique waveforms to create more cost-effective solutions. This flexibility is the key to addressing two of the most important questions posed to COMSATCOM managed service providers: How can industry develop new compression techniques (along with on-board processing) to lower the amount of data that needs to be passed; and can higher modulation schemes such as 64 QAM be utilized using ever smaller antennas? Various frequency bands can enable smaller remote antennas to pass larger amounts of data. Having the ability to transmit from a vehicle in Ku-, X- or Ka-band to leverage current availabilities and missions is just part of the answer.

The other part of the solution is more advanced compression algorithms and better on-board processing techniques. Globecomm has engaged multiple companies about their technologies and is looking at how manufacturers of high-end audio/video codecs are able to handle large data packages through SATCOM connections between 2 and 18 Mbps in size. Engaging with non-SATCOM industries is the only way to solve the data processing challenge.

A combination of swappable optics on the vehicles antenna before it takes off; allowing commercial teleports/integrators to be able to transmit/receive Ka- and X-band commercial and military frequencies, and new processing and compression algorithms is ideal. Codec, antenna and modem manufacturers need to work with others in the industry to develop a system that will both adapt to high throughput needs and be easily altered to change to the frequency band required at the time of the mission.

With these improvements installed in these systems, AAVs and ISR data delivery can be transported with a much better bit-to-dollar ratio and allow more vehicles to operate within an era of tightening government budgets. The new AAVs are great tools that allow us to increase our quality of life and security simultaneously and transport the data in or near real-time, enabling the analyst to utilize the data to the fullest extent possible.

A “Must” Relationship

Through true partnership between industry and government, providers can develop turnkey solutions that support the mission across the entire network.

By Jim Tran, Vice President, Defense and Federal Solutions
and **William Hartanovich**, Account Manager, Airborne ISR Programs
CapRock Government Solutions
jtran@caprock.com, bhartanovich@caprock.com

ISR delivers indispensible strategic and tactical advantage across all sectors of our nation’s defense and homeland security forces. Former Secretary of Defense Donald Rumsfeld and his successor, Robert Gates, each have insisted the U.S. military accelerate procurement and deployment of ISR platforms in theater and across the globe. An ISR task force was developed and approval was given to “reprogram” funds from other areas, in order to support these additional ISR projects.

The number of missions the United States is flying in support of ISR has grown significantly in the last few years. The Department of Defense flew an estimated 400,000 flight hours with unmanned aircraft in 2008. At the time, it sought funding to increase overall UAV missions by 2010. Today, the Army has about 250 Shadows in its inventory, while the Air Force has 147 Predators, 48 Reapers, and 17 Global Hawks. The preceding does not include the vast number of smaller UAVs used by Marines and special operations forces.

The majority of tactical UAVs, such as the Raven, used for close proximity missions make use of line of sight communications for command and control and sensor data. Flying distances between the aircraft and ground control device are relatively short—between 10 and 50 miles.

There are, however, special breeds of UAVs that utilize beyond line of sight (BLoS) communications. The BLoS class of UAVs such as Broad Area Maritime Surveillance (BAMS), Global Hawk, Predator/Reaper, Grey Shadow and Warrior A, utilize geostationary spacecraft to cover vast operational areas—hundreds of square miles—and up to thousands of miles from ground control systems. Of the aforementioned aircraft, all except BAMS utilize commercial satellites.

Currently, BLoS UAVs rely on satellites having unique technical capabilities. These aircraft use satellites to send immense quantities of imagery and sensor data from their remote locations to geographically dispersed sites in the United States. Equipping the aircraft with high-definition video, synthetic aperture radar and other sensor packages creates demand for larger quantities of a finite satellite resource: bandwidth.

Due to technical constraints, data throughput requirements, and satellite availability, in some regions of the globe it is unrealistic to operate more than one or two BLoS UAVs at the same time. In other regions, dozens of simultaneous sorties are possible. These problems can be resolved through a combination of efforts, the largest of which involves partnership and planning between commercial satellite services providers and government UAV users.

A recent Northern Sky Research study predicts that “future SATCOM requirements are likely to further increase such that managing the bandwidth, hardware and software available to militaries around the globe will be a tremendous challenge. In enabling the warfighter, the mix and the management of proprietary and commercial satellite capacity will have to be fairly easy and seamless in order for the warfighter to continue to be effective.”

An estimated 30 GBps of capacity is expected to be in use by DoD by 2014. This capacity may still be inadequate to support all U.S. government requirements, and there are not enough government spacecraft in orbit to handle the load. Commercial satellite capacity remains the number-one viable solution.

With extremely tight capacity and skyrocketing satellite fleet operator prices, key service providers have focused on developing a more comprehensive approach to providing SATCOM solutions for UAV missions. By tracking customer bandwidth utilization, trends and inventory, and developing network optimization tools, service providers dedicated to the customer mission are able to make informed decisions about the build-out of their

DEFEND YOUR COUNTRY WITH A WHOLE DIFFERENT WEAPON.

Today's new battlefield is in cyberspace. And everyone needs trained cyber warriors immediately—from our nation's new Cyber Command to banks, utilities and defense contractors. You can be ready, with a bachelor's or master's degree in cybersecurity, a master's degree in cybersecurity policy or one of three new graduate certificates from University of Maryland University College (UMUC). Our cybersecurity courses are offered online, providing in-depth study of the theory and practice of preventing cyber attacks. Military or civilian, public or private sector, UMUC can help you advance your career and defend your homeland.

- Designated as a National Center of Academic Excellence in Information Assurance Education by the NSA and the DHS
- Graduate certificates in Foundations of Cybersecurity, Cybersecurity Policy and Cybersecurity Technology added for 2011
- Earn undergraduate college credits for learning from work experience, military service or volunteer activities
- Scholarships exclusively for servicemembers and their families, plus loans and an interest-free monthly payment plan available

The Council of College and Military Educators (CCME) has awarded UMUC the 2011 Institution Award, which demonstrates dedication and leadership in providing quality voluntary off-duty education programs to the armed forces.

ENROLL NOW.
877-275-UMUC
military.umuc.edu/cyberspace

UMUC
University of Maryland University College

network infrastructure to pre-position services on behalf of government clients, so they will be available when needed.

Service providers know satellite communications are important to the ISR mission. We must be more than a vendor to the government and offer reliable and competitively priced solutions that deliver an end-to-end capability. Industry needs to understand the challenges facing the warfighter, such as the slow transition to the H.264 (MPEG-4) feed standard, mostly due to cost, and be flexible in developing solutions that mitigate these issues.

The government also needs to stop buying independent systems and the disjointed management of the myriad of separate components operated to achieve the same basic results. Service providers should seriously consider partnering with ground suite providers and vendors to offer complete, compatible exploitation capabilities and cost-effective solutions for government customers.

Through true partnership between industry and government, providers can develop and offer turnkey solutions that support the mission across the entire network as an integrated military-grade package, to include air and ground links, connectivity to the ground stations, and the return path back to CONUS. Together we can better address issues of interoperability among the services as well as assure the quality management of video distribution capabilities and more effectively prepare for dynamic changes in missions and growth. Only this type of solutions packaging will bring true value to our national interests.

Great Fit for ISR

Commercial technology is a low-cost way to implement service because the network products are COTS and a global network is already in place.

Paul Baca, Vice President, Mobile Broadband Systems
ViaSat
paul.baca@viasat.com

We see commercial SATCOM playing a very prominent role in providing connectivity for government/military ISR. Commercial technology and services are a great fit for the application and for today's budget environment for several reasons, including:

- Very low-cost way to implement service because the network products are COTS and a global service network is already in place
- Current network system matches up well with airborne ISR requirements
- Very advanced commercial technology, so government/military customers benefit from current and future research and development dollars, as opposed to having to bankroll development programs.

ViaSat is already operating a global mobile satellite network that is providing connections for aircraft as well as ground mobile and maritime platforms. The network has been operational for over five years, and customers include a wide mix of U.S. and international commercial clients, as well as many U.S. government and military users. It is simple and inexpensive to run service trials or connect to the network just by buying and installing terminals.

In addition to this worldwide service, we also operate several turnkey service regions dedicated to specific military missions. For added security, these regional coverage areas generally terminate in hubs located at U.S. government facilities in the specific areas of responsibility (AORs). But because of our worldwide coverage, aircraft operating in these private hub AORs also have the option to "roam" onto the worldwide network as needed.

This is particularly valuable for enroute communications applications, including USSOCOM C-17 and C-130 missions. So where there are concentrated enclaves of U.S. government aircraft, there can be dedicated, private service. But in areas where aircraft only occasionally pass through, then those aircraft rely on an existing, but enhanced commercial service.

The coverage area for this network also continues to expand, and communication speeds continue to increase as we increase the network capacity to serve a growing commercial customer base, which in turn is available to government/military customers.

The current network is based on our ArcLight modem and networking technology, which was expressly designed to operate with very small antennas, including conforming to the off-axis emissions requirements necessary to avoid adjacent satellite interference within ITU and FCC regulations. Almost any size aircraft can use the service, because it routinely operates with airborne antennas as small as 11.5 inches.

To match up with ISR needs for more video at higher definition, the current shared forward link operates up to 24 MBps, while the individual return links operate at up to 1 MBps. A software upgrade in 2011 will increase the forward link data rate to over 30 MBps. Additional near-term upgrades using commercial technologies such as adaptive coding, spreading, and modulation will provide even more robust performance and additional capabilities for mobile users.

With the advent of Ka-band satellites that bring a lower cost per bit and higher performance, plans are also well under way to augment our global mobile network with Ka-band coverage. We can see a future need for Ka- and Ka/Ku-dual band plus multi-band, multi-beam electronically steered array antennas to ensure seamless transition between frequency bands, satellite beams and coverage areas. Government/military customers will benefit from those developments without paying full development costs.

We are building a series of Ka-band high-capacity satellites, with the first one being launched in the second quarter of 2011 (ViaSat-1). Other satellites will follow, with each providing well over 100 Gbps of usable throughput.

ViaSat has also entered into agreements with other Ka-band operators including Eutelsat (KA-SAT, successfully launched December 26, 2010) and Yahsat (first satellite launching later this year) to share technology and bandwidth access that will ensure maximum Ka coverage throughout North America, Europe, the Middle East and portions of Africa—the areas of greatest need for government and military customers.

Demonstrating the validity of all that we have said here, we are already serving hundreds of military and government customers. We have logged approximately 150,000 flight hours on commercial aircraft and more than 400,000 on military aircraft.

New SATCOM Synergies

It is important to value SATCOM across a number of future mission areas.

Frank Prautzsch, Senior Vice President, Government Programs
ORBCOMM
prautzsch.frank@orbcomm.com

Commercial SATCOM capabilities, as always, are essential to future UAV and ISR missions and requirements. Developments in select markets bring new synergies that stretch beyond the atypical boundaries of connectivity and telemetry for UAVs and special sensors.

Let me frame five major focus areas for the future of SATCOM from ORBCOMM's perspective:

Dynamic Capacity. SATCOM core functions tied to capacity for UAV payload backhaul, telemetry, tracking and control, data processing, and high capacity broadcast of products will continue to stay core to these missions, and such capabilities will continue to be the major consumers of bandwidth for the war-fighter and first responder. Of importance will be expansion of services to support cloud computing, edge network capabilities, and inter-switch IP network trunking for 3G/4G and other wireless services. Continued work on high capacity communications "on the move" and "on the pause" is needed for future operations both on air and ground C2 platforms.

Mobility. UAV and ISR functions are not broadband only. The need for intelligence collection and dissemination that remains network agnostic, agile and securable is essential. Additionally, SATCOM cannot be treated as an independent enterprise, and tomorrow's requirements must focus on the integration of spectrum, waveforms, terrestrial carriers and versatile open standards. Continued use of MSS services, integrated 3G/4G wireless and other civil and commercial wireless standards is key to future operations. Moving from stovepipes to "netpipes" is not the answer. This perhaps can be best defined by the need to integrate such concepts as an Android operating system within military device structures for core security, applications development, man/machine utility and visualization, or the need to integrate national, theater and local data tailored to an operation with access with a mobile warfighter or responder.

Machine-to-Machine, Distributed Sensors and Telematics/Telerobotics. These SATCOM functions sit in ORBCOMM's "sweet spot." The C4ISR community is significantly lagging behind commercial best practices in M2M programs. The state of affordability in advanced micro-processing and micro-networks hosted off a parent modem device and sensor concepts across all senses and domains offer our forces a technical advantage elegantly based upon the transfer of bytes as opposed to manipulation of terabytes. The complexity of machines can be overmatched by the simplicity of telematic reporting and sensing, and simple remote control and manipulation of robotic assets will carry the day as force structure or operational risks impede mission success.

The introduction of advanced satellite RFIDs and TTL devices act both as asset management and tracking devices, and also "surrogate" SATCOM links for sensor devices. Distributed unattended C4ISR information "mines" allow for cueing of events, their 3-D location and even their characterization. This limits the need for painting the sky with energy, or placing troops in harm's way in many missions. Such capabilities also can apply to integrated cooperative tracking of small and large vessels tied to the Automatic Identification System and its

current and future missions, which ORBCOMM performs as a worldwide service.

Cyber-Support and Timing. Commercial space offers plausible future means to mitigate risk in network mission success. Commercial space offers the potential to rectify shortfalls in network timing and Internet-based cyber-attack. Selected space links should be provisioned to inoculate networks and resurrect or ensure PNT for network continuity of operations. Network-centricity is the main enabler of future UAV and sensor programs. The denial of such services in network attack cannot be tolerated. Some attainable provisions for cyber and timing protection remain essential in supporting network centric operations in the future.

Social networks, stability operations and nation building. In recent months we have seen the impact of civil and partisan C2 over Twitter and other Internet-based social media. This arguably has emerged as an ISR tool, if not a "weapon" of the future. Commercial SATCOM can play and should play a major role in offering infiltration and exfiltration communications to those societies that seek our help, be it social or political reform. SATCOM becomes a great enabler in support of news gathering, local intelligence and assessment, situational awareness to the world and, in many cases, stability in crisis. Multiple systems and hosts offer the flexibility to function through Internet denial or filtering. Additionally, entertainment and educational broadcasts still matter with regard to supporting a population generating and expecting change.

In closing, it is important to value SATCOM across a number of future mission areas. In many cases it will be more important to work the elegance of a byte than the processing of a terabyte, and perhaps just as critical to see a YouTube or Twitter feed as that of a UAV.

Adopt Open Standards

A standards-based strategy will allow military systems to operate much more efficiently and facilitate closer cooperation with commercial industry.

By Rick Lober, Vice President and General Manager, Defense and Intelligence
Systems Division
Hughes
rick.lober@hughes.com

The military's demand for SATCOM has increased exponentially in the past 10 years. Much of this demand has come from the increased use of commercial SATCOM in ISR efforts via UAVs and other tactical communications needs. The military is currently utilizing commercial satellites to meet its mission requirements, and we will continue to see greater engagement with the commercial satellite sector as the military's need for SATCOM continues to rise, enabling complete situational awareness on all fronts.

Acquisition vehicles such as the General Services Administration (GSA)-Defense Information Systems Agency (DISA) Future COMSATCOM Services Acquisition (FCSA) will also help the military and intelligence communities work with industry to not only meet their requirements, but also increase the bandwidth efficiency of systems. For example, current SATCOM technology in use within DoD for ISR systems is often based on full-time, dedicated channels, such as Single Channel per Carrier links or dated standards such as the Common Data Link, which is generations behind commercial technology with regard to bandwidth efficiency. Increasing bandwidth efficiency will help the military decrease the cost of both SATCOM hardware and operations.

To help meet the needs of current and future military and intelligence requirements, open standards should be adopted, such as IP over Satellite (IPoS), which is the world's leading satellite air interface standard, developed by Hughes and approved by ETSI, TIA and ITU organizations, and supports Multi-frequency Time Division Multiple Access (MF-TDMA) links.

Following a modern standards-based strategy will allow military systems to operate much more efficiently and facilitate closer cooperation with commercial industry in developing integrated fixed and on-the-move implementations. In particular, as airborne missions become more critical across military and homeland defense operations, IPoS/MF-TDMA links have proven ideal for supporting fixed wing platforms, and tests are progressing rapidly for rotary wing applications.

Hughes is also developing new signal waveforms that will allow military users to greatly reduce antenna size and cost in Ku- and Ka-band applications. These new waveforms will operate at a fraction of the cost of current L-band systems and will significantly lower antenna hardware costs in Ku-, X- and Ka-bands. As the military shifts to Ka-band and more advanced Ka-band commercial satellites become available in the market, partnering with industry will be the only cost-effective way to meet the military's ever-growing demand for bandwidth, while providing the best value for government.

A good example is Hughes' latest satellite under development, Jupiter, a next-generation, high-throughput commercial Ka-band system with more than 100 Gbps of capacity, approximately 100 times greater than conventional Ku-band satellites. Scheduled for launch in the first half of 2012, Jupiter is designed with an advanced multi-spot beam, bent-pipe architecture that is able to support multiple waveforms, and Hughes is exploring the possibility with partners around the globe to bring this technology to military and government users wherever the mission may take them.

Hughes is committed to developing advanced solutions which help our military and government customers meet mission objectives anywhere in the world—on budget, and on time and creating best value for those that serve. ★

Contact Editor Harrison Donnelly at
harrisond@kmimediagroup.com.
For more information related to this subject,
search our archives at www.MIT-kmi.com.

MIT CALENDAR & DIRECTORY

The advertisers index is provided as a service to our readers. KMI cannot be held responsible for discrepancies due to last-minute changes or alterations.

Advertisers Index

Deloitte Services www.deloitte.com/us/cyber	3
Fujitsu www.govt.definingnetwork.com/mit	25
Harris RF www.harris117g.com	C2
L-3 GCS www.l-3com.com	20
Orbcomm www.orbcomm.com	33
Paradigm www.paradigmservices.com/connect/mit1	5
Paradigm www.unitingforces.com	C4
Pelican-Hardigg www.pelican.com/mit	13
Quintron Systems www.quintron.com	11
Segovia Inc. www.segoviaip.com/agile	27
Sprint www.sprint.com/4g	C3
TCS www.telecomsys.com	7
Tellabs www.tellabs.com/olan	23
Titus www.titus-labs.com	15
Ultra Electronics-DNE Technologies www.packetassure.com	9
University of Maryland University College http://military.umuc.edu/cyberspace	31

Calendar

March 14-17, 2011
Satellite 2011
Washington, D.C.
www.satellitetoday.com

March 28-30, 2011
AFCEA Belvoir Industry Days
National Harbor, Md.
www.afceabelvoir.org

March 31-April 2, 2011
CyberFutures Conference
National Harbor, Md.
www.afa.org

April 11-13, 2011
Sea-Air-Space 2011
National Harbor, Md.
www.seaairspace.org

April 19-21, 2011
Tactical C4 Conference and Exhibition
Atlanta, Ga.
www.technologyforums.com

May 1-5, 2011
DoDIIS Worldwide Conference
Detroit, Mich.
www.ncsi.com

May 10-12, 2011
GSA Training Conference and Expo
San Diego, Calif.
http://expo.gsa.gov

NEXT ISSUE

April 2011
Volume 15, Issue 3

Military Information Technology

Cover and In-Depth Interview with:

M.G. (P) Rhett Hernandez
Commander
Army Cyber Command

Special Report:
DISA Campaign Plan

Features:

- **Industry Roundtable: Cybersecurity**
- **COTM Antennas**
- **Message Classification**
- **GSM-Operations Contract**
- **Smartphones for Soldiers**
- **Cybersecurity Commission**

Insertion Order Deadline: March 25, 2011
Ad Materials Deadline: April 1, 2011

Michael Bristol
Senior Vice President and General Manager
Government Solutions Group
TeleCommunication Systems Inc.

Q: Please remind readers what TCS' Government Solutions Group is, what it does and which markets it addresses.

A: Sure. TCS is a value-added systems integrator that provides mission-critical total communications solutions globally. What that means is we offer the end-to-end solutions that military, government and commercial organizations need to enable seamless, highly secure communication between fixed sites and remote operations. In support of our customers' needs, we offer the SwiftLink family of deployable communications systems and end-to-end managed services for IP-based voice, video and data. We also build our own equipment and provide our own worldwide global support organization and global teleport infrastructure. At the same time, we provide best-of-breed partner technologies—Cisco, AvL and ViaSat, to name a few.

Put all that into a one total package and it's the kind of organic capability that customers demand, that we deliver, and that makes TCS one of a kind.

Q: What's changed at TCS since we spoke together last year?

A: Lots of things. In February, we completed our acquisition of Trident Space & Defense, which adds to our advanced engineering and packaging capabilities. We've also integrated our 2009 Solvern Innovations acquisition, now our cyber-intelligence group, which enables us to develop successful partnerships with commercial enterprises and government agencies. 2010 also saw rapid expansion for our integrated logistics support capabilities. This very moment, we have more than 200 field service reps deployed around the world.

Then there are the new offerings. These include the Inclined Tracking Terminal, the Hyperlite Microsat, the Wireless Point-to-Point Link Lite, and the TMCNet product of the year—the Tactical Transportable TROPO. These four products help military customers reduce bandwidth-associated costs in high-demand areas. We also launched TCS TotalCom, which is our unique approach to the provision and service of global end-to-end communications solutions.

On another front, we were named sole awardee of a $315 million contract to deliver U.S. Navy satellite communications infrastructure and service globally. This win is especially exciting for us, as it brings our end-to-end communications expertise to the growing maritime market.

Finally, we announced an exclusive arrangement with Cisco to commercialize IT communications services via their IRIS platform. It's been a very busy year, to put it mildly.

Q: Tell us more about the Cisco deal and what it means to you and your customers.

A: Cisco chose TCS as the exclusive service provider for the successful commercialization of its Internet Routing in Space (IRIS) platform—the world's first space-based Internet routing platform. Our launch of Cisco IRIS services means that our customers will have increased bandwidth availability and reduced latency for land, sea and airborne platforms over four continents. So now we're in space. Here at TCS, not even the sky is the limit.

Q: There's been a buzz about TCS TotalCom. What exactly is this offering, and why is it getting attention?

A: In a nutshell, TotalCom is our comprehensive approach for securely delivering mission-critical voice, video and data whenever and wherever customers demand. So TCS TotalCom isn't just a product or service—it's an entire approach to end-to-end communications. Basically, the offering provides customers with total communications solutions from the face of the satellite to the desktop. The solution includes TCS GeoNet managed satellite services, SwiftLink wireless communications systems, integrated global support, information assurance and a suite of applications. Given the holistic approach TotalCom represents, we think the buzz is justified!

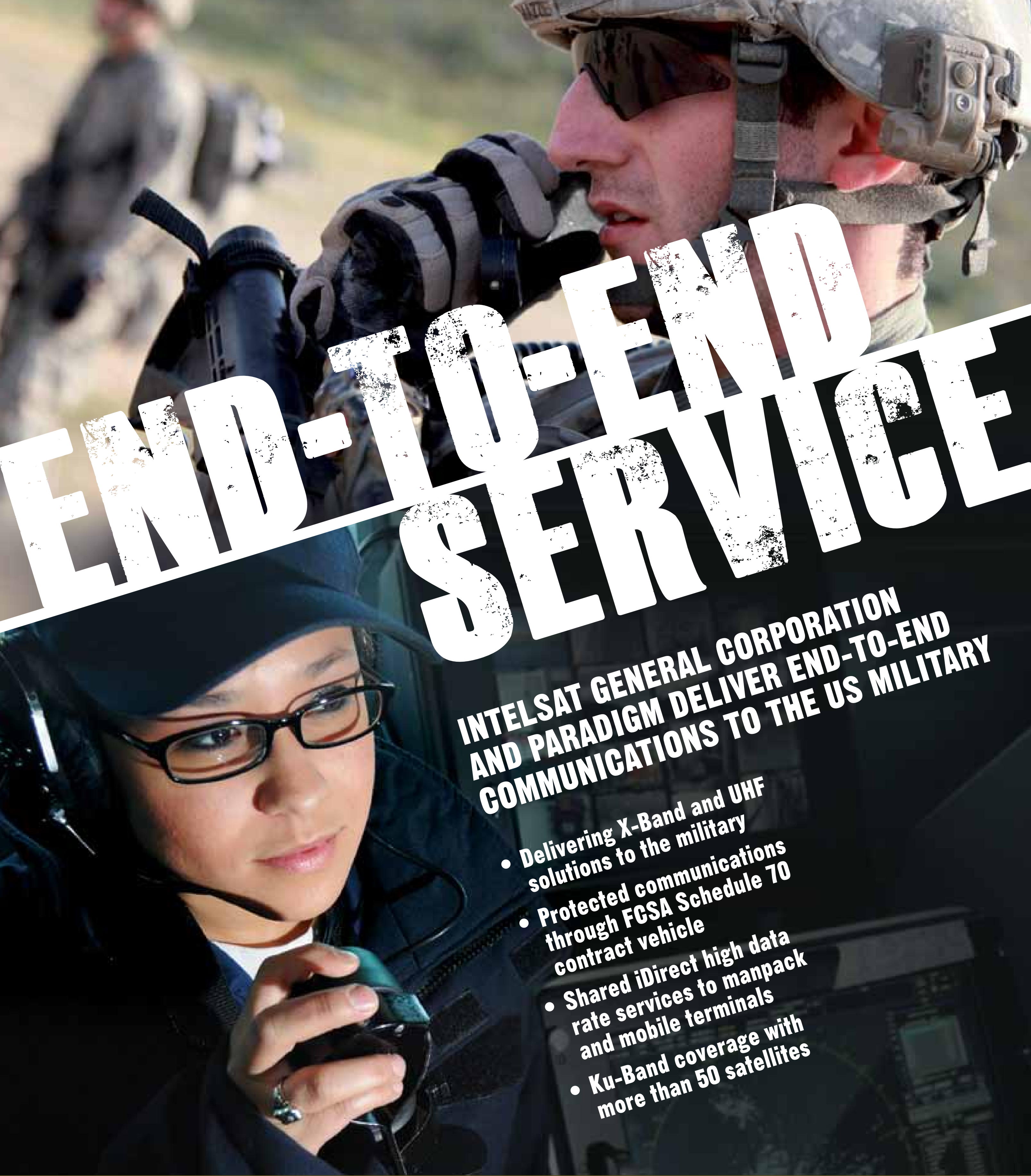
Q: You rolled out TCS Maritime Communications recently. This is a highly competitive market. Why is TCS diving in?

A: For two reasons at least. First, it's a natural extension of what we've been doing on land for 25 years. We're a leader in communications for the Army and Marine Corps, so now we're applying our know-how to ventures that demand highly reliable and secure communications at sea. Whether it's ship-to-ship or ship-to-shore, we can provide a total communications offering with exceptional bandwidth reliability and operational availability. Second, maritime fits with the company's overall end-to-end communications solutions strategy.

Q: You mentioned that 2010 marked yet another TCS acquisition—Trident Space & Defense. What does Trident offer that you didn't already have?

A: Trident is the third government-oriented acquisition we've made in the past 18 months. They're a leading provider of engineering and electronics solutions for global space and defense markets. Trident focuses on electronic components, solid-state drives, ground systems, and advanced products supporting worldwide aerospace, military and industrial markets. They also have a tremendous advanced engineering capability in the miniaturization and ruggedization of electronic systems—something we're already applying to our SwiftLink line of deployable communications. ★

mbristol@telecomsys.com



END-TO-END SERVICE

INTELSAT GENERAL CORPORATION AND PARADIGM DELIVER END-TO-END COMMUNICATIONS TO THE US MILITARY

- Delivering X-Band and UHF solutions to the military
- Protected communications through FCSA Schedule 70 contract vehicle
- Shared iDirect high data rate services to manpack and mobile terminals
- Ku-Band coverage with more than 50 satellites

INTELSAT General Corporation

PARADIGM SERVICES BY ASTRIUM

To register your interest visit
www.unitingforces.com