



SOLE SOURCE



Newsletter of the Garden State
Chapter
of the
International Society of Logistics
District 10 Chapter 7

February 2006

Edited by Michael E. Harris, CPL

Volume 29, Number 6

SOLEful Musings

By Chuck Hodell – Chapter Chair

For those of you who missed our February luncheon, you missed an interesting, somewhat different type of luncheon presentation given by representatives for SAFT America, Inc.



Bill Hogelin and Maureen Boyette present Certificates of Appreciation to Mike Fredrickson and David Roller.
Photo by Westgate

Basically the topic dealt with evolving technology for battery power sources and its impact on logistics. We are speaking here of large, lithium-ion batteries, not flashlight cells. Development has now been able to achieve improvements such that for a 65lb, 28V, 80Ah lithium-ion battery used in the Army's Improved Target Acquisition System (ITAS), charge time has been reduced to less than 6 hours, operating time increased to more than 16 hours, and total life increased to 3-5 years. Therefore, you ask, "What's the big deal? Logistically speaking, here is the deal: the predecessor item had a lifetime of

only 9 months, a recharge time of 16 hours and 2-3 batteries were required to support each system as opposed to the single battery required now. Oh yes, the old battery required periodic maintenance, the new Li-ion unit requires no maintenance. For the Army's ITAS there has been a significant cost savings realized. Mike Frederickson of the American Competiveness Institute together with David Roller of SAFT Inc. summarized the advantages of lithium-ion technology: longer service life, reduction in spares required, less man-power to service and support the fielded batteries, distinctly smaller logistics footprint, improved performance features for the warfighter and a significant reduction in materials transported out of theater for disposal or reclamation. Given that batteries have been a recurring challenge for the Army, it is good to hear examples of how we are gaining on the problem.



The Garden State luncheon crowd assembled in Gibbs Hall for February's 2006 gathering.
Photo by Westgate.

Next month we have our winter gathering at the Old Orchard Inn. It will be a great chance to get around and mix with the membership – 2 hours

of comforts and good conversation. See you there.

Programs

By William Hogelin – Vice Chair Professional Development

Our next luncheon activity will be during April. To facilitate many schedules and other factors, we will gather on a Thursday, 13 April, rather than our normal Tuesday. At that time, we are lucky to have the MilDep of the L&RC as our guest. COL Joe Hollenbeck will share his insights of L&RC activities and its contributions to the War on Terror. He was commissioned in the U.S. Army Signal Corps from the University of Alabama in 1976. Colonel Hollenbeck holds a Master of Science Degree in Administration from the Central Michigan University. He is also a graduate of the U.S. Army Command and Staff College and the U.S. Army War College. His decorations include the Defense Superior Service Medal and the Legion of Merit.



Colonel Joseph C. Hollenbeck

Management Committee Information

By Maureen Boyette – Vice Chair, Administration

The Chapter Executive Committee Information is now on the Chapter website.

<http://gardenstatesole.org/>

Member Information

By Rich O'Donnell – Vice Chair, Membership Services

All members are reminded to submit their renewal membership forms, with the applicable yearly renewal fee (\$35 in almost all cases) **to me**, versus mailing it into SOLE National Headquarters. The \$95 per person subsidy is a local chapter nuance, and it only applies if you follow these guidelines. Applications and remittances sent to National Headquarters directly do not get the \$95.00 subsidy applied.

Once again, I can be reached at:

Richard O'Donnell
AMSEL-LC-COM
Ft. Monmouth, NJ 07703
Phone: (732) 532-3460
DSN: 992-5762
e-mail:
richard.odonnell@mail1.monmouth.army.mil

Thank you all for steering potential applicants my way.

Notice: If you change jobs, retire, etc. and have a new email address and still want to be listed on the SOLE email distribution list, please notify Janet Steinberg at janet.steinberg@lmco.com and Maureen Boyette at Maureen.Boyette@mail1.monmouth.army.mil of your NEW email address. Thus ensuring you do not miss any upcoming SOLE Chapter notices, etc.

Upcoming Events

By Gloria Richardson – Chair, Governmental Affairs Committee

LRC University

The LRC University has successfully completed training for the first quarter 2006. Classes were filled to capacity resulting in training for 283 students. With the continued help of our customers and subject matter experts, we can provide a quality training program to the Fort Monmouth workforce.

We hope that the job of identifying course offerings will continue to be a mutual endeavor and come from all aspects of our customer field – internal and external. Courses are open to the entire Fort Monmouth workforce at no cost.

If you would like to attend any of our courses, please have your training coordinator e-mail the undersigned.

Lois A. Montgomery
 Career Management Team
 Logistics and Engineering Operations
 Directorate (LEO)
 732-532-5780, FAX 24953
 lois.montgomery@us.army.mil

Technical Training Corporation

Note: These all start in February 2006; there are at least four sessions of each.

The following training will be provided by Technology Training Corporation:

- Configuration Management Seminar
- Advanced Configuration Management Seminar
- Integrated Logistics Support Seminar
- Integrated Master Plan/Integrated Master Schedule Seminar
- Quality for Program Managers Seminar

For dates, locations, and POCs go to <http://www.technologytraining.com>.

Making Interpersonal Communication Work!

27 April 2006 – Target Audience: Government Only

In today's team-based organizations, winning the respect and cooperation of bosses, colleagues, or staff members is critical if you want people to help you get things done. That's why interpersonal skills are essential to your own effectiveness as a manager.

At this seminar, you'll discover how perceptions influence your interactions with

others and their responses to your identify and flex your interpersonal style...use listening and feedback skills to build understanding...assertively manage conflict and turn potential adversaries into allies...direct and motivate others to high levels of performance...develop give-and-take relationships that produce results!

Upon successful completion of this seminar, students should be able to:

- Solve problems by clarifying the real issues
- Make trade-offs without being a pushover on big issues
- Gain support for implementing your plans
- Generate enthusiasm for your ideas and proposals
- Minimize conflict and build group commitment
- Influence others and motivate them to profitable action
- Save time, energy, and talent by improving the entire "people" side of your job
- Develop credibility based on respect and trust
- Find alternatives to working with "difficult" people
- Give criticism when necessary and use praise to produce results
- Provide direction while maintaining flexibility

Contact Kristine Ryskamp, Organizational Development Specialist at x22780.

2006 U. S. Army Modification Work Order (MWO) Workshop

1-5 May 2006 in Reno, Nevada

Hosted by the US Army, Aviation & Missile Command. Welcome to the 2006 U.S. Army Modification Work Order (MWO) Workshop hosted by AMCOM. Workshop dates are 1-5 May 2006, with the 1st and the 5th designated

as travel days. The workshop is scheduled to convene at the Silver Legacy Resort on 2 May 2006 at 8:30 a.m. Workshop early registration will be held from 3:00-5:30 p.m. on Monday, 1 May. Main registration begins at 7:30 a.m. on Tuesday, 2 May 2006.

The details and agenda for the workshop are still being planned. If you have a subject that you would like to see on the agenda, feel free to contact Mr. Grover Gibson, DSN 656-9058, or commercial 703-806-9058 or by email: gibsonG@hqamc.army.mil.

Logistics Education Foundation

J. MICHAEL RYSKAMP CPL, LEF Liaison SOLE LEF Scholarships

For more information on the LEF, and to download the scholarship application package, go the following website: <http://www.sole.org/lef.asp>. Be sure to contact Mike Ryskamp, Chapter LEF advisor, prior to sending the application in. You do not have to be a member of SOLE to apply. All scholarship award winners are required to submit a student paper to SOLE's professional journal, the Logistics Spectrum. Scholarships apply to the next academic year.

The Editor's Corner

By Michael E. Harris,
CPL – Editor



Intern Programs

Before I wax nostalgic, I would like you to know why I brought the topic up. When I talk about intern programs, I mean Interns, Fellows, Engineers-in-Training, Management Development, and any other professional “apprenticeship” program regardless of title.

I have seen too many interns and fellows doing database cleanup for six or eight months at a time. I never thought that clerical/administrative

work was the right thing to do with a logistics intern. I think this is a gross waste of the resources and could lead to the loss of the intern from the program before the agency gets any real value out of the intern. Okay, I have complained.

Almost 20 years ago, I was involved with the US Navy intern program at NAS Anacostia. Anacostia, for those of you who have never heard of it is one of the seven original towns in the District of Columbia; Washington was one of the seven and was where the Capitol and President's residence were located. I do not remember the names of all the towns, but I do remember Georgetown as being one of the seven.

Back to business. I am not sure which of the five Navy systems commands was in charge of the intern program, but the Supply Systems Command ran the school. The US Navy Acquisition, Logistics, and Management Training Center (NALMTC) was on the NAS in a dreary building that was converted to classrooms. Most of the students at the school were interns, but some courses were for supervisory-level logisticians. All five systems commands, the US Marine Corps, the US Coast Guard, and a few other agencies used the ILS training program.

While each command had some limited discretion on how to use the interns, most of them did the same things. Most of the interns were recent college graduates, while the rest were non-degreed administrative individuals with a demonstrated ability and desire to improve themselves. The program was a two-year program and most interns rotated every six months. I believe that they stayed in their original commands, but rotated among the various ILS elements and program organizations. They might do supply support for six months and then support equipment for six months before moving to an APM-Logistics (APML). The interns were expected to complete the 11 courses in the basic series by the end of their intern program. The final three courses were designed for APML candidates.

One of the nicest features of the program was the Intern Orientation. The managers of the intern program tried to catch the interns in their first six months for the orientation. The orientation was two weeks at NB Norfolk. The interns had half-day briefings from a senior official in each of the five systems commands and one from the USMC. They had no more than nine half days devoted to briefings. What did they do with the other half days? They did half-day visits to an aviation depot, warehouse facilities, ship repair facilities, whatever ship was available (aircraft carrier, guided missile cruiser, etc.), shipboard firefighting school, and shipboard damage control school. They had one morning and one afternoon with a short version of the ILS Overview class. The orientations were two or three times a year depending on the number of interns available.

I taught the Intern ILS Overview two or three times. Once, I taught the class in the morning and went with the interns to damage control training in the afternoon. The instructors had been damage control technicians on the USS Stark (an FFG-7-class guided missile frigate damaged in the Persian Gulf). We had hands-on training – about half the training that all shipboard sailors receive. We learned how to cut 4x4 timbers to make K-braces for sprung hatches; patch rips, tears, and holes in water and fuel lines; and patch rips, tears, and shell holes in bulkheads. We used wooden timbers, wooden wedges/shims, rags, and corks we found in the damage control lockers that are aboard ships. We got wet.

After we learned how to repair everything, we found ourselves the crew aboard the USS Buttercup – a big steel cube sitting in 30,000 gallons of water in the training building. We heard the cry of “Incoming!” and raced on deck to our braced positions. When we took a hit (we felt it), we went into action. Some teams had to go below decks to shut off all the pipes and repair the pipes, some teams had to take pumps down to the lowest part of the ship (simulating a lower engine compartment) to de-water the ship. The ship sank with all hands on-board.

We ran the exercise a second time and saved the ship. Notice how the training was set up. Static trainers to learn technique and then the dynamic trainer to learn teamwork and discipline. We lost the ship the first time and saved it the second time – under the same conditions. We lost and then succeeded and we felt great. We had an emergency egress exercise at the end that was limited to students over 5’4” tall – the short students would have drowned in the ship had they tried it. Think about the orientation – briefings alternating with tours. The firefighting school could not let them participate, but the interns got a front-row seat. The damage control school was hands-on training that none of us will ever forget.

Now, back to the schoolhouse. As I mentioned, the logistics program was 14 courses, with the first 11 being designed for the intern program. We recommended that the interns start with the ILS Overview course, which covered the acquisition process and introduced the students to the integrated nature of logistics. The second course was Configuration Management, which was one of the better courses and covered a lot of basic concepts that were helpful for all the other courses. As you can imagine, the other nine intern courses covered the ten elements of ILS (we doubled up on a pair of elements). The final three courses were logistics engineering principles, logistics engineering design, and logistics engineering management – the capstone course.

I taught the Intern ILS, ILS Overview, Configuration Management, Maintenance Planning, and Logistics Engineering Management courses. I also wrote training material to replace Configuration Management and Maintenance Planning course material.

The training for the interns was somewhat brutal, but those who made it through unscathed always did well in their careers. I will not say that all the interns did well, but the GS/GM-15 and SES logisticians had all come through the intern program.

What I have written here matches my view of how to run an intern program. The hands-on

portions of the intern orientation show how the program can be structured to make the program unforgettable.

ILS QUESTIONS

I received a short list of supportability questions from the Chapter Chair. The following (edited for readability) came along with the questions – it helps put them in perspective. I will give you about four each month until I run out of them.

“The following is a good exercise to test your basic understanding of supportability. Fundamentally, these are the type of questions that are used in general interviews before getting into the second and third indenture of your logistics knowledge for promotion or future employment.”

Oh, you have to hunt for the answers in the newsletter!

Q1. What regulation is considered the ultimate reference for Integrated Logistic Support?

Q2. Can you briefly describe the Materiel Release process?

Q3. What are the elements of ILS? In which elements are you strongest?

Q4. How can logistics influence the system design?

PEOPLE, PROJECTS, & COMPANIES

INSTAKNOW AWARDED CWID 2005 TOP PERFORMER STATUS

(March 6, 2006) South Plainfield, NJ. [Below remarks are extracted from their publication of 6 March 2006.]

Instaknow gained top honors and special recognition at the 2005 Coalition Warrior Interoperability Demonstration (CWID) sponsored by the US Joint Forces Command (USJFCOM) and hosted by the Northern

Command (NorthCom). “CWID incorporates aspects of Homeland Security and Homeland Defense with coalition operations that include government agencies, national and international law enforcement, first responders, and traditional military allies.” – CWID 2005

Instaknow’s patented software that builds custom integration and process automation solutions without writing code, proved to be unique and unmatched in meeting CWID objectives.

Instaknow was judged on its effectiveness, addressing Collaborative Information and **Integrated Logistics**. All solutions were scored on ability to enhance C4ISR, Homeland Security, Homeland Defense, and coalition interoperability and be deployable within (12) months. Major integrators, government and military agencies, and special technology companies participated but only after winning an invitation based on demonstration, successful completion of an arduous application process, and gaining a government “sponsor.” Instaknow, sponsored by the Northern Command (NorthCom), was demonstrated by “Warfighters” at several US sites.

Total solutions participating worldwide: 110.

CWID Warfighter and Interoperability Assessment: “InstaKnow performed exceptionally well, providing techniques, procedures and concrete solutions for collaborative planning across a bandwidth constrained operational environment. InstaKnow Active Collaboration Engine (ACE) provided real time customized business process automation and intelligent information integration and collaboration through unlimited business rules and logic across all disparate systems and platforms without creating a single line of code or changing the system configuration. During CWID execution InstaKnow automatically triggered either processes or other applications to run at scheduled times, read and updated systems, and provide automated interactive collaboration

among Warfighters, information, systems, whether internally or across the web.”

The assessment report: “InstaKnow *successfully demonstrated* the ability to facilitate information sharing across multiple information domains by pushing and pulling information from many different places, fully integrating the information within a timely manner, creating customized reports appropriate to the event and notifying designated recipients of the event via telephone.”

Instaknow builds process automation, systems integration without code or change to existing systems. Contact: Armida Macri, Bus. Dev., 732-778-9592; Jeff Sherer, SVP, 732-261-0074

www.instaknow.com

A1. AR-700-127, Integrated logistic support

TECHNICAL ARTICLES & OTHER ITEMS OF INTEREST

We have two items for your considered review this month.

The first item is a reprint from the 1 March 2006 issue of *Government Executive*; the article was in the **News & Analysis** section. As logisticians working in a computer-intensive environment, this article should get your attention.

Corrina Panduri discovered the second item. It is an account of an application of Combat Service Support Automated Information Systems Interface (CAISI) and Worldwide Port System (WPS) handheld scanners to capture cargo barcode information.

THE GREAT WALL

Forget the military secrets – Chinese hackers might really be after **logistics** data from the Pentagon’s unclassified computer network.

By David Perera

When revved up, today’s US military is just about unstoppable in a conventional war. Foreign nations with a yen to compete against the United States know this, and wars against governments in Iraq and Afghanistan offer plenty of evidence (insurgencies are another story).

Still, military giants are vulnerable. Achilles’ weakness was his pride. The United States’ flaw could be penetrable computer networks containing logistics information necessary to set in place the military machine.

Logistics information literally is the bread and butter of the military. Track the supply lines of materiel and personnel and you’ll know where troops are headed. Disrupt that supply line, and you will have created a barrier to getting there quickly. Amateurs study tactics, professionals study logistics, goes the Pentagon cliché. Yet

great chunks of logistics information flow across the unclassified Defense Department system, the Nonsecure Internet Protocol Router Network, or NIPRNet. The Pentagon maintains a separate network for secret information, but the NIPRNet is its daily workhorse.

“Most logistics is on the NIPRNet,” says John Gilligan, a former Air Force chief information officer, now deputy director of Fairfax, VA-based SRA International’s defense sector. The network isn’t open to just anybody – it connects to the Internet via protected gateways – but it is vulnerable, Gilligan says. About 700,000 Air Force desktop computers hook up to the NIPRNet, and finding a vulnerable machine and exploiting that hole “is certainly within the realm of a nation-state,” he adds.

For Americans today, war evokes images of roadside bombs and hidden snipers in the Middle East. But Defense Department planners who are paid to think about future wars worry about the People’s Republic of China. Rising powers long have challenged dominant countries for primacy – it’s an old story. And now, nobody is more powerful than the United States.

A2. Coordinate with the various functional areas to get approval to release the system.

A more immediate threat is a Taiwanese declaration of statehood, which could move China to react militarily, dragging the United States into conflict. Taiwan rests about 80 uneasy miles across water from China, neither an independent state nor part of Beijing's communist government, in most of the world's eyes. But ever since defeated Chinese nationalists fled the mainland for the island in 1949, Taiwan's security has mattered to the United States.

In March 1996, China fire-tested nuclear-capable missiles in the Taiwan Strait; in response, President Clinton sent in two aircraft carrier groups.

Chinese military analysts know they probably can't successfully invade Taiwan or defeat the United States in direct combat. But they're betting they don't have to, says James Mulvenon, director of Falls Church, VA-based Defense Group Inc.'s Center for Intelligence Research and Analysis. Instead, a rapid blow aimed at Taiwan's will to fight might do the trick. A key part of such a coercive strategy would be to delay likely American military response to the area, he says.

Taiwanese national self-confidence is weak, says Toshi Yoshihara, a visiting professor at the US Air War College in Montgomery, AL. When China lobbed missiles into the Taiwan Strait, "Taiwan's stock market basically crashed; there were people rushing to leave the island," he says. If the Taiwanese could be convinced early in a conflict that American military help wouldn't be forthcoming, it could further damage their resolve, according to Yoshihara.

Which is where hacking into the NIPRNet comes in. Chinese military theorists believe the way to delay American response is to crack the logistics systems, Mulvenon says. The Chinese think the United States is most vulnerable as it deploys, Mulvenon says, as it fuels and revs up the

military engine. Though hackers couldn't stop military action, they could slow it down. Hackers already have been "burrowing into really boring logistics networks," which suggests those perpetrators are state-supported, he adds. Those hacks could be preparation for a future crisis. In its latest annual assessment of Chinese military power, the Pentagon reports that China considers computer network operations "as critical to seize the initiative and 'electromagnetic dominance' early in a conflict."

In general, foreign disruption of military information technology networks would have a potentially major, even catastrophic impact, SRA's Gilligan says. Still, the military is in no position to simply shift everything onto its secret network. Classified networks are expensive – and the military needs to communicate with the outside world, especially for logistics. For example, before Operation Iraqi Freedom, the Pentagon relied heavily on airplanes lent and piloted by commercial carriers for soldier transport to the Middle East. "United and Delta ... don't have classified processing facilities," Gilligan notes.

Deteriorating geopolitical situations don't materialize instantaneously, so the United States would have time to prepare for any adversary's tactics. Chinese hacking "is a concern, but I don't see our strategy becoming unraveled because of it," says Stuart Johnson, a research fellow at National Defense University in Washington.

Especially in the early stages of a showdown with China, "We should be able to cope with work-arounds," he adds. Says Gilligan, "It's not like we're just sitting around, waiting for a potential adversary to attack."

Also, a Chinese strategy of hacking or coercing Taiwan is not risk-free. A rain of missiles and bombs from the mainland could end up galvanizing the Taiwanese populace; analogous tactics boosted the resolve of native populations in Great Britain during World War II and North Vietnam in the 1960s. "It could really piss people off and make them more inclined to hold

out," says Michael O'Hanlon, a senior fellow in foreign policy studies at the Brookings Institution.

And while network exploits can be plausibly denied, they still "usually get discovered and there's blowback," Mulvenon says. Plus, the Chinese underestimate the ability of logistics personnel to compensate, should their systems be hacked. But as those systems become increasingly automated, the danger rises, he says.

"If there's any good news here, it's that computers are getting attacked all the time," O'Hanlon says. Like an immune system made stronger in the wake of a disease, the military's network system should emerge stronger from a wave of foreign probes, he says.

The NIPRNet will become better protected through more secure enclaves for subsets of especially sensitive information, Gilligan says.

Still, the job of shoring up computer security never ends. Computer networks were built to be open. Security requires steady monitoring and attention as hackers exploit new holes when old ones are sealed. Defense Information Systems Agency officials say they "are constantly increasing our vigilance to ensure the free and secure flow of information."

The world's largest network once was one built from flagstone-paved roads extending 53,000 miles in Roman antiquity. The roads were designed as a tool for policing an empire, and also for trade and communications. Unfortunately for the Romans, barbarians found them equally useful for their own purposes – attacking legionnaires – and eventually the Roman Empire was no more.

A3. Maintenance Planning; Manpower and Personnel; Supply Support; Support Equipment; Technical Data; Training and Training Support; Computer Resources Support; Facilities; Packaging, Handling, Storage, and Transportation; Design Interface. (Should be able to list at least four).

CAISI AND WPS HANDHELD BARCODE SCANNERS PROVIDE WiFi IN-TRANSIT VISIBILITY AT THE PORT OF BEAUMONT

By Stephen Larsen

BEAUMONT, Texas – Army officials are one huge step closer to achieving in-transit visibility and total asset visibility for the thousands of tons of cargo that pass through the port here each month, thanks to the implementation of a new generation of RFDC (radio frequency data communications) handheld barcode scanners and secure, wireless CAISI – the Combat Service Support Automated Information Systems Interface.

The handheld scanners capture cargo's linear and 2D barcode information, such as the dimensions of cargo, or what work stevedores have performed. CAISI then wirelessly transmits the data to the Worldwide Port System (WPS) database at the port's terminal management directorate (TMD) office.

Both the handheld scanners and the CAISI system are products of the Program Executive Office, Enterprise Information Systems (PEO EIS). The scanners were acquired via the AIT-III (Automatic Identification Technology) contract managed by the Product Manager, Joint-Automatic Identification Technology (PM J-AIT), while CAISI is a commercial-off-the-shelf (COTS) solution provided by the Product Manager, Defense Wide Transmission Systems.



Photo by Stephen Larsen

The implementation at the port of Beaumont includes 16 CAISI (Combat Service Support Automated Information Systems Interface) Repeater Modules (inset), which are mounted on poles scattered throughout the port in small weather-tight boxes called NEMA (National Electrical Manufacturers Association) enclosures. The CRMs help to maximize WiFi coverage in the ‘canyons of steel’ of cargo that are staged at the port.

As port operations returned to normal after Hurricane Rita, the handheld scanners and CAISI were successfully tested together during full-scale loading operations the week of Nov. 14. That week, stevedores loaded more than 1,200 pieces of cargo, including tanks, Bradley Fighting Vehicles, wheeled vehicles and containers to an LMSR (large, medium-speed, roll-on/roll-off ship).

Key port for OIF cargo

“This port (Beaumont) is kind of a center of gravity for troop movements,” said Lt. Col. Timothy Whalen, Commander of the 842nd Transportation. “I’m a big advocate of CAISI. Testing CAISI here sends the right message.”

Whalen said that the ports of Beaumont and Corpus Christi, Texas transport 63 percent of the military’s cargo to Iraq. More than 80,000 pieces – some 14 million square feet of cargo – have passed through Beaumont for Operations Iraqi Freedom I, II, and III.

“CAISI streamlines things,” said Whalen. “Previously, as we’ve scanned, that equipment data was vulnerable until we brought back the scanner and downloaded. CAISI makes it much more efficient, more accurate, and less vulnerable.”

Chris Easton of the Headquarters, Surface Deployment and Distribution Command (SDDC) at Alexandria, Va., whose mission is to improve the cargo documentation process, agrees.

“CAISI gives us the ability to talk live to the Worldwide Port System (WPS) database from the cargo, instead of having to wait four-to-five hours until we get the scanner back to download at the TMD (terminal management directorate) office,” said Easton. “The real key is to allow the scanner to solve problems at the cargo, rather than going back to TMD, and CAISI gives us the wireless ‘bubble’ that allows us to do that. Our command’s goal here is to increase the efficiency of data capture and data QA (quality assurance) processes, with an eye toward reducing manual effort.

The CAISI WiFi network at Beaumont

The port of Beaumont implementation includes one CAISI Bridge Module (CBM), at the TMD office, and 16 CAISI Repeater Modules (CRMs), mounted on poles throughout the port in small weather-tight boxes called NEMA (National Electrical Manufacturers Association) enclosures.

“CAISI offers a flexible meshed network configuration which has multiple paths available for redundancy,” said Amon. “When one radio link is blocked or interfered with, CAISI radios create a self-healing meshed network. When one path to the root is down, the other radios automatically repeat for each other to form an alternate path to the root.”



Photo by Stephen Larsen

Chris Easton (left) of the headquarters, Surface Deployment and Distribution Command (SDDC) observes as a stevedore uses a new RFDC (radio frequency data communications) handheld barcode scanner to scan the barcode information from a vehicle in the hold of a ship at the port of Beaumont. The handheld scanners and secure, wireless CAISI (Combat Service Support Automated Information Systems Interface) were successfully tested together during full-scale loading operations at the port during the week of Nov. 14.

Easton said the coverage of the CRMs allows stevedores to transmit data from handheld scanners to the WPS database from nearly everywhere throughout the 50-plus acres of the port, except from inside the holds of vessels, which is why the handheld scanners can do both batch and real-time downloading of cargo data.

Another challenge is offered by the industrial nature of the water port

"Look around," said Easton in a staging filled with tanks, Bradleys and other vehicles area during the testing at the port of Beaumont. "Our cargo is very large and forms 'canyons of steel,' whose walls, in turn, are made of multiple corner reflectors. Sometimes down these 'canyons,' we may lose coverage. Part of the job is to solve as many problems as you can here at the cargo, without putting having to put it in 'the frustrate yard,' which, of course, costs dollars."

At the TMD office, traffic management specialist Kyle Lee sat at his computer terminal and opened a hatch list – a list showing, for each hold section of a cargo ship, a description of the

items stowed, their volume and weight, the consignee of each, and the total volume and weight of materiel in the hold.

"If we get real-time numbers out of this, this is good, but this is only the first full day using the system with a vessel – check with me after lunch," Lee said. He scrolled down the screen and nodded, liking what he was seeing. "The scanners have not been brought in for upload, but this list has already been updated – this is good."

After the test was completed, Lee gave the CAISI/handheld scanners tandem a thumbs-up, noting that it was the first test, and that SDDC personnel would have a better feel for what the system could do with additional missions under their belts.

"So far, I am satisfied they will provide a real-time numbers update to WPS," said Lee. "I see an added advantage for our Vessels Section (stow planners) in that they can pull updates from WPS into ICODES (the Integrated Computerized Deployment System) more quickly. This allows them to stow the vessel as the mission progresses. The real-time updates at least provide an opportunity for us to stay even with the operation, if not actually work ahead. I think we have a good thing going here."

Gloria Barnes, WPS system administrator, said of CAISI, "I love it. We don't have to upload scanners, so we have more real-time data. Before, we would see near-real-time data because we would upload the scanners a couple times a day, at lunch and dinner when the stevedores took a break. CAISI is better for stow planners, better for staging. It makes manifesting easier, reconciling easier, it makes everything easier. It gives better in-transit visibility, even down to stow locations on a ship or staging locations on the port."

Whalen said the SDDC selected CAISI in large part because it enables a WiFi capability in a port setting. This is a critical first step toward building a BCS3-based (Battle Command Sustainment Support System-3) 'digital

dashboard,' which Whalen said is the vision of Maj. Gen. Charles Fletcher, Commander of the SDDC. "From my dealings with Maj. Gen. Fletcher," said Whalen, "he envisions that the logistician should see things as the warfighter does. He calls it his BCS3-based dashboard."

This dashboard, explained Whalen, would allow logisticians every step along the way to 'drill down' at their laptop computer and see where pieces of cargo are in the supply chain. This would be possible with the near-real-time wireless exchange of data with WPS that CAISI allows, and provide port commanders with more timely information about the progress of an exercise.

"I shouldn't need to wait until it gets to Beaumont to see a piece of equipment in the supply chain," said Whalen. "I should see it in Ft Hood, and see it all the way through the system. I don't want the warfighter in Ft Hood to have to worry about it – he has other things to worry about, like fighting the battles. Right now, we have liaisons from Ft. Hood here watching over things. We could avoid them feeling they have to be here if we could give them the vision that gives them the confidence where their materiel is."

CAISI is a standard, accredited Army system

Army officials said they saw several advantages to the CAISI solution versus other COTS solutions, starting with cost – they said the cost of the current implementation at the port of

Beaumont was \$55,000, less than a third of what other commercial alternatives could have cost.

"CAISI is very cost-effective compared to other means to get this done at Beaumont," said Whalen. "We get a lot of bang for our buck."

Easton said another major advantage is that CAISI is a standard, accredited Army system. "It's a big advantage for the SDDC that the support infrastructure for CAISI is already in place," said Easton. "Also, compatibility with existing Army infrastructure is assured both now and into the future and host nation approvals for these radios and frequencies are already in place with major U.S. allies."

Another plus, Easton said, was the CAISI support team. "I spent some time in Kuwait and had an opportunity to meet several of the CAISI field service engineers," said Easton. "I found them to be both knowledgeable and proactive."

"We're sustaining the war now as opposed to surging," said Whalen. "What we send over there now, it's absolutely critical that we see these items as they go, because there's very little redundancy in the Army right now. CAISI facilitates seeing this very critical cargo for us."

Project Manager, Defense Communications & Army Transmission Systems (PM DCATS)
Release No: 05-12-02

Contact: Stephen Larsen (732) 427-6756
Stephen.Larsen@us.army.mil

A4. BIT; BITE, Fewer Tools, No special tools; Maintainability; Easy Warfighter Machine Interface; MANPRINT.

Meeting Notices

Luncheon Meetings: Third Tuesday of the month.

Date	Time	Location
February 21, 2006 (Tuesday)	1130-1300	Gibbs Hall
March 21, 2006 (Tuesday)	1130-1300	Gibbs Hall
April 13, 2006 (Thursday)	1130-1300	Gibbs Hall
June 20, 2006	1130-1300	Gibbs Hall

Executive Board Meetings: Last Thursday of the month.

Date	Time	Location
March 30, 2006	1145-1300	Lockheed-Martin, Tinton Falls
April 27, 2006	1145-1300	Lockheed-Martin, Tinton Falls
May 25, 2006	1145-1300	Lockheed-Martin, Tinton Falls
June 29, 2006	1145-1300	Lockheed-Martin, Tinton Falls

Other Functions:

Date	Time	Location
Winter Holiday Function (Wednesday) March 3, 2006	1700-1900	Old Orchard Country Club, Eatontown
Annual Chapter Symposium May 3, 2006	0700- 1600	Sheraton Hotel, Eatontown

Do not forget!
Garden State Chapter Symposium
3 May 2006, 0700-1600
Eatontown Sheraton

2005-2006 Executive Board Members

Please contact Janet Steinberg at 732-389-0390 with any corrections.

GARDEN STATE CHAPTER SOLE - Chapter 7 District 10 2005 - 2006 CHAPTER MANAGEMENT COMMITTEE

Revision date: 12/31/05

<u>TITLE</u>	<u>NAME</u>	<u>Phone #</u>	<u>E-Mail</u>
Chapter Chair	Charles Hodell	732-389-5359	chuck.hodell@lmco.com
Vice Chair, Finance	Bob Featheringham	732-818-0441	two_feathers@comcast.net
Vice Chair, Member Services	Rich O'Donnell	732-532-3460	richard.odonnell@mail1.monmouth.army.mil
Vice Chair, Administration	Maureen Boyette	732-758-0180	maureen.boyette@mail1.monmouth.army.mil
Vice Chair, Education	Al Viola	732-263-1808	aviola@enlogex.com
Vice Chair, Prof. Development	William Hogelin	732-427-6321	william.hogelin@mail1.monmouth.army.mil
LEF Liaison	Mike Ryskamp	732-427-4260	j.michael.ryskamp@us.army.mil
Awards Cmte. Chair	Maureen Boyette	732-758-0180	maureen.boyette@mail1.monmouth.army.mil
Newsletter Cmte. Chair	Dr. Michael Harris, C.P.L.	732-532-2453	harrisM100@comcast.net
Publicity Cmte. Chair	Steve Bromka	732-532-0682	steven.bromka@mail1.monmouth.army.mil
Symposium Cmte. Chair	Ken East, C.P.L.	732-460-1370	keast@logsec.com
Government Affairs Cmte. Chair	Gloria Richardson	732-532-6752	gloria.richardson@mail1.monmouth.army.mil
Industrial Affairs Cmte. Chair	Janet Steinberg	732-389-0390	janet.steinberg@lmco.com

No flying machine will ever fly from New York to Paris.

Orville Wright

Airplanes are interesting toys but of no military value.

*Marshall Ferdinand Foch [Professor of Strategy, Ecole Superieure de Guerre] (circa 1911)
Supreme Commander of Allied Forces, 1918*

Airplanes suffer from so many technical faults that it is only a matter of time before any reasonable man realizes that they are useless!

Scientific American (1910)

Even if a submarine should work by a miracle, it will never be used. No country in this world would ever use such a vicious and petty form of warfare!

William Henderson, British Admiral (1914)

Radio is just a fashion contrivance that will soon die out. It is obvious that there never will be invented a proper receiver!

Thomas Edison

