



SOLE SOURCE



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

April 2007

Edited by Michael E. Harris, C.P.L.

Volume 30, Number 11

Heart and SOLE

By Rich O'Donnell - Chapter Chair

Recently, someone at our CECOM Life-Cycle Management Command (LCMC) asked me what the difference was among the terms reset, repair, overhaul, and recapitalization of Army equipment. They wanted to know what the difference between resetting to 10/20 standards and resetting to Fully Mission Capable (FMC) standards was for Army equipment. Admittedly, sometimes these terms are confusing, used interchangeably by mistake, misunderstood, etc.; therefore, rather than give my personal definition of these terms, I did a little homework online and thanks primarily to a fairly recent GAO report to Congress on the topic, I came up with the following. I hope that it is of benefit to our newsletter readers.

The Army term for the equipment refurbishment process is called RESET. RESET is a series of actions to restore a unit to a desired level of combat capability commensurate with future missions. RESET consists of three components: repair, replace, and recapitalize.

Repair starts with an inspection followed by maintenance and possible replacement of some parts to bring equipment to original technical specifications.

Replacement is to "buy new," to replace equipment destroyed in battle or otherwise too damaged to fix. Also listed under replacement is

reserve-component equipment that's been left overseas for other units to use.

Recapitalizing involves overhauling or restoring equipment to improve performance or make it like new from the factory.

To ensure that deployed units receive required amounts of equipment critical for their missions, the Army has designated certain major equipment items, such as add-on-armor vehicles, up-armored HMMWVs, selected communications and intelligence equipment, and other items deemed critical for OIF and OEF missions as "theater provided equipment" (TPE). According to Army officials, based on operational decisions, these theater-specific items are being left in theater because these are force protection items. This equipment is taken from active, Guard, and Reserve forces when they return to the United States and is retained in theater to hand off to follow-on units. TPE includes equipment such as armored vehicles, individual soldier body armor, and equipment used to counter improvised explosive devices.

Fully mission capable, means that the equipment has no critical or safety deficiencies as outlined in technical readiness reporting instructions. However, equipment that is considered fully mission capable may have a number of deficiencies that will need to be addressed in the longer term.

According to the Army, RESET comprises a series of repair, recapitalization, and replacement actions to restore units' equipment to a desired level of combat capability commensurate with

mission requirements and availability of resources. The purpose of RESET is to bring unit equipment to combat-ready condition, either for the unit's next rotation in support of current operations or for other, unknown future contingencies.

The Army's standard level of maintenance is known as 10/20. This standard requires that all routine maintenance be executed and all deficiencies be repaired. Equipment at less than the 10/20 standard can be fully mission capable, which means there are no critical maintenance deficiencies as outlined in the technical manuals and instructions, and no safety deficiencies. Unit commanders have the authority to supersede the technical manuals and declare a system fully mission capable even though it has a non-mission capable deficiency. The Marine Corps's equivalent term is "mission capable." We RESET equipment to 10/20 standards within the Army Materiel Command (AMC).

The Army's RESET strategy for ground vehicles includes an additional set of maintenance procedures known as Delayed Desert Damage (3D) which are designed to address damage that results from these vehicles operating in a desert environment. These procedures are designed to address damage that might otherwise not be visible. These 3D checks are initially performed at the unit level. Equipment that goes to a depot is subjected to more extensive 3D maintenance procedures. Army aviation equipment is subject to Special Technical Inspection and Repair (STIR). Similar to 3D, this maintenance is designed to address damage caused by operation in a desert environment. STIR also includes other routine maintenance. We have STIRs for Generators, SINCGARS, and Night Vision devices currently.

Although the terms may be slightly different, the Marine Corps equipment repair and replacement process and equipment standards parallel the Army process and standards for equipment maintenance. The Marine Corps equivalent to the Army's RESET process is termed "recovery." Marine Corps equipment returning from combat

theaters is evaluated and transported either to a maintenance depot or to a Marine Corps unit's home station for repair. The Marine Corps's equipment recovery process entails restoring all equipment used in Global War on Terror (GWOT) operations to its pre-GWOT condition. For equipment in the Marine Corps prepositioning fleet, this means restoring to a "like new condition," for all other equipment, this means restoring to a mission capable status. The Marine Corps also applies procedures similar to the 3D as appropriate.

The Department of Defense (DoD) reported in April 2005 that they expected a new set of protocols to emerge based on experience with equipment used in OIF and OEF. These protocols may be similar to 3D and STIR which emerged as maintenance procedures based on experience from Operation Desert Storm. DoD, as part of its ongoing effort to assess stress on equipment, plans to look for unusual wear patterns and methods to address them as well as examining maintenance trends.

Depot maintenance is defined as the highest level of maintenance activity, where the most complex maintenance work is done, from overhaul of components to complete rebuilds. Military depots and defense contractors throughout the United States perform depot-level maintenance.

Overhaul – The restoration of an item to a completely serviceable condition as prescribed by maintenance serviceability standards.

"RESET, in simplest terms, will reverse the effects of stress on all our equipment."

Terms like recapitalization, refurbishment, repair, and replace are sometimes used interchangeably. However, the Army has specific definitions for each of these terms. RESET includes a series of actions taken to restore unit equipment to a desired level of combat capability after returning from contingency operations. The RESET process brings unit equipment to full combat-ready condition, either for its next rotation in support of current operations or for other, unknown

future contingencies. RESET actions include the repair of equipment, the replacement of equipment lost during operations, and the recapitalization of equipment where feasible and necessary.

In some instances, Army units retain equipment to reconstitute their unit quickly rather than send this equipment to depot for overhaul. According to officials in the Office of the Secretary of Defense, Warfighters are not readily willing to give up equipment, which contributes to fewer equipment items being returned to the depots for repair. Officials at the U.S. Army Forces Command and at Army depots echoed this concern, stating that availability of assets to induct into the depot repair program is limited by units' need and desire to have equipment available for training. These officials added that the units fear that they will have to wait for replacement equipment because their unit priority is not high enough within the Army to ensure immediate replacement of the equipment items. To increase the number of equipment items going to depots from units, the Army created a list of equipment that it will now require units to automatically send to the Army depots for RESET. The list, called the ARI, is based on lessons learned from earlier experiences that damage and wear to certain types of equipment items used in Southwest Asia require more extensive depot level repairs. For example, some equipment RESET at the units' home station was failing at higher than expected rates in theater during follow-on deployments. The list contains about 200 equipment items and has been updated several times, to include items such as the Bradley Fighting Vehicle and the Abrams Tank.

According to the implementing memorandum, unit commanders are required to nominate a minimum of 25 percent of the listed equipment for return to depots for RESET. According to the memorandum, the intent is to provide units the flexibility to maintain equipment for training while placing the maximum possible into RESET programs, and items retained for training

are to be maintained in fully mission capable condition.

Programs

By Ron Fulton – Vice Chair Professional Development

Our April 2007 luncheon featured Pat Shaw, ARFORGEN Branch Chief, Logistics Operation Center of the LRC. Pat's discussion was on the AMC Organizational Alignment/Synchronization Integrated Action Group (IAG). The Army Material Command DCG Chartered Integrated Action Group (IAG) members include HQ, AMC (G-3, G-5, and G-8), Army Sustainment Command, Life-Cycle Management Command (LCMC) Installation Management Command, and LOGSA. Pat provided interesting insight into this complicated process involving many variables. As noted during his presentation, the IAG focuses on codifying strategic imperatives, developing the "should be" process models, guiding by consensus versus unanimous agreement (which I am sure is not an easy task), and documenting unresolved issues for subsequent work by the IAG. The final products are approved by General Officer Steering Committee.

Our next event is the SOLE Symposium being sponsored at the Sheraton Hotel in Eatontown on May 15, 2007. Come join us for a full day of learning and networking.

Please do not hesitate to contact me if you have ideas on specific topics, subject matter or speakers you think will resonate with our chapter and the local C4ISR community. I can be contacted at ron.fulton@l-3com.com or 732.552.7092. I look forward to seeing you at future SOLE luncheons.

Education

By William Hogelin – Vice-Chair Education

During the previous months, the Chapter has been attempting to contract an all-encompassing course for Logisticians to aid and improve job performance. Its secondary purpose is to prep members for the spring or fall CPL exam. Twice we had kickoff days that have not been met because the course "is not ready yet". We have the support from management, student interest, but not the course program of instruction. The executive board recently met to discuss the direction we need to go. The course will still be held, but the negotiation might need to be started over. In the mean time, candidates need to continue getting a strong background in System Engineering through reading, courses, and hands on experience for that portion of the CPL exam. Please contact Gloria Richardson or me if you are interested in being added to the email address list for all notices. My new email is: William.Hogelin@conus.army.mil.

"If a man empties his purse into his head, no man can take it away from him. An investment in knowledge always pays the best interest."

- Benjamin Franklin

Management Committee Information

By Maureen Boyette – Vice Chair, Administration

12 April 2007 – Chapter Management Committee Meeting Minutes

Chapter Chair, Rich O'Donnell, convened a regular meeting of the Chapter's Management Committee at 11:45 a.m., on 12 April 2007, at the Lockheed Martin Corporate office in Tinton Falls, NJ.

Attendees: Rich O'Donnell, Ken East, Bill Hogelin, Bill McLean, Bob Featheringham, Janet Steinberg, and Maureen Boyette

Reports of Officers:

Reports were presented by the Chapter Chair R. O'Donnell, Bob Featheringham – VC Finance, Bill McLean – VC Membership, and Maureen Boyette – VC Administration.

R. Featheringham presented the Treasurer's report showing a financial statement with a balance on hand, as of 31 March 2007, of \$11,788.27. The Chapter donated \$500 for the annual LEF contribution.

Reports of Committees:

Membership: B. McLean reported four renewals last month for a total membership count of 273.

Newsletter: M. Harris was not present but submitted a report. All newsletter inputs must be submitted no later than the 15th of the month. All contributors will have headshots included in the newsletter.

Educational Committee: The Chapter has not met its goal to offer our membership certified professional logistician classes by April. The Educational Committee will look for alternative solutions in implementing CPL training.

Administration: M. Boyette reported that the quarterly activity report was submitted to SOLE Headquarters. Newsletter awards are due in April, Chapter Awards in May.

Symposium: Ken East reported that the May 15th Chapter Annual Symposium has progressed as planned within the estimated budget. There are currently six paid exhibitors. Goal is to have a minimum of 200 attendees. B. Hogelin suggested biographies be included with the symposium flyer. A final symposium committee meeting will be held end of April.

Publicity: Symposium posters will be displayed around Ft. Monmouth. R.

O'Donnell will send flyers to CERDEC, Tobyhanna, Lakehurst, etc. S. Bromka will post an announcement on the CECOM Knowledge Center.

New Business:

R. O'Donnell made a motion to fund donations of a personnel nature effecting Chapter Committee Members (e.g., loss of immediate relative, wedding). The motion passed with 6 votes "yes" 1 vote "no".

Chapter will support the Fisher House Benefit to be held at Gibbs Hall, Ft. Monmouth June 9th by sponsoring a table and program ad.

R. O'Donnell will contact Al Viola to coordinate the June election luncheon and C. Hodell to coordinate the Management Committee Award Dinner.

Adjournment:

The meeting was adjourned at 1:05 p.m.

Prior Chapter Management Committee meeting minutes are on the Chapter website <http://www.gardenstatesole.org/>.

Financial Update

By Bob Featheringham – Vice Chair Finance

Monthly Summary Financial Report – April 2007

Income for the month was \$3,200.00, and expenses were \$1,871.14. Our books in Quicken were reconciled to the bank statement. The chapter's planned reserves remain intact. A detailed report was provided to the Chair and remanded for annual audit and subsequent approval.

Member Information

By Bill McLean – Vice Chair, Member 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:

William McLean
AMSEL-LC-RE-FSSD, Bldg. 555
Ft. Monmouth, NJ 07703
Phone: (732) 532-4569
DSN: 992-4569
E-mail: william.mclean2@us.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.

Members

Next, I would like to welcome the New and Renewing members of our Chapter, as indicated below.

New members

Michael Dazio – Datatek
Kevin Joyce – LRC-COMM-DIR

Renewing members

Warren M. Dasczynski – US Army

Robert R. Featheringham – Two Feathers Consulting

Robert Hague – LRC-COMM-DIR

Allen Hardison – LRC-COMM-DIR

Hayward T. Hubbs – LRC-COMM-DIR

Mike Jackson – PM DCATS

Phyllis Krebs – CECOM-LRC

Richard F. O'Donnell – CECOM – LRC

William J. Powell – Lockheed Martin

Nancy Soper – LRC-COMM-DIR

Lucille T. Tanguay – LRC-COMM-DIR

Thank you all for joining or rejoining, SOLE.

Upcoming Events

By Gloria Richardson – Chair,
Governmental Affairs Committee

Defense Executive Leadership Development Program (DELDP)

04 September 2007-07 June 2008. The Army has opened the window of opportunity for submission of applications for the Defense Executive Leadership Development Program (DELDP). The program is open to GS-12-14s. Erika Valerio may be contacted for additional information. See <http://cpol.army.mil/library/train/catalog/ch04deldp.html>.

Logistics Education Foundation



J. MICHAEL RYSKAMP C.P.L. –
LEF Liaison

Do you want to further your logistics education to advance your career? Do you have a family member who is interested in a logistics education? If so, contact any member of SOLE's

Garden State Chapter Management Committee – <http://www.gardenstatesole.org/>.

LOGISTICS EDUCATION FOUNDATION

SOLE founded the Logistics Education Foundation (LEF) – a non-profit foundation – to collect funds for and provide financial support to the educational activities and programs of SOLE. This includes providing the funding for SOLE's annual scholarship and doctoral dissertation awards programs; grants; publication of technical/educational material (e.g., monographs); and other assistance to individuals and organizations furthering logistics education, as determined by the LEF's Board of Trustees.

Programs and initiatives undertaken by the LEF in support of SOLE's educational agenda include scholarships and doctoral dissertation grants for eligible students (members and non-members) working toward undergraduate, graduate, and post-graduate degrees in logistics and logistics-related subjects.

ANNUAL LOGISTICS SCHOLARSHIP COMPETITION

Deadline is May 15 each year for the following academic year.

Are you pursuing a bachelors or masters degree in logistics or a logistics-related major?

Are you enrolled at an accredited educational institution, carrying a full-time course load?

Then you are eligible to apply for a \$1,000 scholarship award from LEF.

Each year, the LEF awards a number of scholarships supporting logistics study at undergraduate and graduate levels. Applicants are evaluated based on their intention to pursue a career related to logistics, scholastic achievements, as well as indications of current and future contributions to the logistics profession, as evidenced by course work, special projects, research, and/or on-the-job logistics experience.

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.

You will need to submit a Complete Application Package:

- Completed Application Form
- Official Transcripts for all University/College coursework completed
- Two letters of recommendation from faculty or employers

Please contact Mike Ryskamp, C.P.L. at 732-427-4260 or cell 732-822-0009 j.michael.ryskamp@us.army.mil.

Download Application Form:
<http://www.sole.org/downloads/lef-02.zip>.

The Editor's Corner

By Dr. Michael E. Harris, C.P.L. - Editor-in-Chief



Homeland Security

In my research for this column, I found an interesting distinction between homeland security and homeland defense – homeland defense is the military component of the overall governmental actions of “homeland security”. Homeland defense is spearheaded by the US Northern Command (NORTHCOM), but we want to look at the civilian portions of homeland security.

One of my sources indicated that homeland security refers to government actions to prevent, detect, respond to, and recover from acts of terrorism or other national security threats to the country's home territory, domestic population, or critical infrastructure. Until the September 11, 2001 attacks, the term homeland security was rarely used – we called it civil defense until the attacks. I believe that the US Congress took

almost 10 weeks to create the Department of Homeland Security (DHS). Much of what is now DHS existed in some form and was “bureaucratized” into a major component of the Federal government. However, the concept of homeland security is not limited to the Federal government; the state and local governments are significant parts of the infrastructure. While DHS gives out money to the states to implement security measures and the states pass this out to the localities – sometimes the DHS sends it directly to the major urban areas, there is a component that has always been funded at the local level. Homeland security involves the local first-responders – the police, firefighters, and emergency medical services (EMS).

I found the scope of homeland security – a list of good items and some fuzzy items: emergency preparedness and response, including volunteer medical, police, EMS personnel, and firefighters (this includes terrorism and natural disasters – and natural disasters involves FEMA); domestic intelligence activities – FBI, but not CIA; critical infrastructure protection; border security, land and sea; transportation security – usually limited to air and sea; biodefense; detection of nuclear and radiological materials; and research on next-generation security technologies.

Keep in mind that while the facts are real, the opinions are the Editor's. The first item in the list is emergency preparedness and response. This is the piece that has been with us for as long as there has been a USA – people helping people, the volunteer medical, police, EMS personnel, and firefighters. In my criminal justice coerces, we tend to think of these as ‘first responders’. These are the front line of security in times of natural disaster or acts of terrorism. The only drawback is that the Federal Emergency Management Agency (FEMA) still exists [fact] and this is not good [opinion]. FEMA need to be overhauled – or scrapped completely and a new organization created. I know that scrapping an entire dysfunctional organization and building a replacement from the

ground up is possible. I may write about the JJC in New Jersey soon to show you how it is done.

Domestic intelligence is tough. I have been reading about what the United Kingdom, France, Israel, the former East Germany, and the former Soviet Union do/did. Like the US, they all had internal and external security organizations. In the US, the FBI in internal and the CIA is external. Communications and data/information sharing are the big issues. Sounds like the Communications-Electronics Life-Cycle Management Command (C-E LCMC).

Even though the tragic events of September 11 were a quarter century in the future, we used to play Terrorist. The goal was to develop a terrorist attack on the DC metro area with as much disruption to the business of government while killing or harming the fewest people. I know this sounds a bit odd, but one of my operations research professors taught it to us. The professor worked at the US Army Concepts Analysis Agency (I have not idea if it still exists); their goal was to play terrorist games or Soviet attacks through the Fulda Gap and see what happened. They developed strategies for mitigating the damages. That is what this is all about. Think of ways that the terrorists could hurt us and then find an appropriate response – either before or after. Call this disaster preparedness. I did something similar in on of my criminal justice classes last fall – destroyed all seven of the Potomac River bridges with minimal loss of life, but major disruption to the DC metro area. I can supply the details, but only to the FBI or DHS – and then under Federal court order.

Border security and transportation security take up took much ink the media as it is, and you know what is happening. If he wins a seat in the House, Mr. Adame has wall and moat approach he wants to push; but you know how liberals are. Biodefense and the detection of nuclear and radiological materials are beyond what most of us around Fort Monmouth have experienced – and I do not want to research this topic right now.

You might ask what next-generation security technologies are; I am not sure. I did find a small, interesting article on cybersecurity. The Editor wants you to understand that his opinion of the problem is that many complaints about DHS are politically motivated. There are Congressional charges (published 04/19/07) that DHS does not have a clue about cybersecurity. The House committee on homeland security said that the infiltration of Federal government computers by foreign nationals is "one of the most critical issues confronting our nation." Someone in Congress just realized that if sensitive information is stolen and used by enemies, the United States is "strategically harmed." Your Editor's response is Duh, of course we will be harmed if sensitive information is stolen – what does this liberal Congressman think the term 'sensitive information' means? I am not liberal bashing, but I know that the politically-motivated statements are all from Democrats whose voting records (I checked) are all liberal to the point of harm to the US.

The penultimate point is that for my intended audience, you have transferable skill-sets to address the critical infrastructure problems. You may not have done that work before, but it is set up for logisticians – cradle-to-grave mentality – and for systems engineers (logistics is a systems engineering discipline) – everything-is-connected-to-everything else.

If you are interested in homeland security for personal reasons or new-business opportunities, Jeanette M. Moyer of the US Army War College Library compiled a selected bibliography almost a year ago – more than two dozen pages of references (and links). If you are interested in this bibliography and cannot find it on your own, send me an email – HarrisM100@comcast.net – and I will send it to you (PDF with active hyperlinks).

SOLE Notices

By Janet Steinberg, Industrial Affairs Committee Chair

My SOLE Notices email database list is growing every day. If you have a coworker or business associate who would like to receive emails regarding upcoming SOLE Garden State Chapter luncheons and the annual Garden State Symposium announcements, etc., they can contact me at janet.steinberg@lmco.com. I will be happy to input their email address to our database. Or just leave their business card with me at the monthly luncheons and I take care of it for them. Remember you do not have to be a chapter member to receive these email announcements.

Editor's Note: The Chapter Management Committee agreed to continue having the monthly luncheons at the Sheraton-Eatontown if possible. Please confirm the location of the luncheon each month.

PEOPLE, PROJECTS, & COMPANIES

By the Publications Committee

RESET Stars

Strong hint to Bill McCarthy – you still owe me bios on all your leadership team.

**Garden State Chapter of
SOLE**

Annual Logistics Symposium

**“Successful
Logistics
Strategies for
Increasing
Readiness”**

15 May 2007

Sheraton-Eatontown

Mark your calendars

TECHNICAL ARTICLES & OTHER ITEMS OF INTEREST

We have two articles for you this month.

The article on Real ID Act technologies is one of the first that seemed to be unbiased. Most articles seem to bash the law. Alice Lipowicz wrote this for Washington Technology in April 2006. Please note the RFID issues. I had an entire issue of The SOLE Source devoted to UID/RFID; RFID is coming.

About a year before this second article, Col. Greene started to explain the concept of System-of-Systems. In this article, he gets much closer to the concept. He uses an analogy with a single desktop computer with Word, Excel, and PowerPoint on it. One computer for multiple applications. If you were to use my computer, your CAC would give you a different set of capabilities that I have on the machine. This is what Col. Greene is trying to explain.

REAL ID TECHNOLOGIES: A TWO-WAY STREET

States Should Not Leave Technology Choices to DHS

By Alice Lipowicz

Washington and other states should be more involved in choosing technologies for meeting the Real ID Act of 2005 requirements, according to an industry group.

The states should not leave the decision about the best technology solely up to the Homeland Security Department, the Smart Card Alliance's Identity Council recommended in a new statement.

The group's assertion follows the signing of a memorandum of agreement last month by Washington state and the DHS to launch a pilot program to offer upgraded driver's licenses that may serve as proof of US citizenship in crossing the US border. The Smart Card Alliance believes the memorandum allows DHS alone to select the technology specifications for the enhanced driver's license.

States considering additional pilots should insist on having input into the technology decisions, the group said.

"We believe that the technology chosen for enhanced driver's license pilots should be a cooperative decision between states and DHS and that the decision should consider whether the chosen technology meets states' requirements for citizen privacy and security," the statement said.

The smart card alliance warns against selecting long-distance radio frequency identification tags for enhanced driver's licenses under the Real ID Act. It states that this is a possibility for the Real ID Act because the Homeland Security Department has selected long-distance RFID for another border-crossing card to meet Western Hemisphere Travel Initiative requirements.

One of the dangers of long-distance RFID is its potential lack of security due to its capability of being skimmed by unauthorized readers, according to the Government Accountability Office report. However, DHS officials have said that risk can be addressed by limiting the information that can be skimmed to a single number. That number must be linked with a secure departmental database in order to obtain personal information about the cardholder.

Furthermore, GAO recently noted the high failure rate of long-distance RFID in tests performed in the US Visitor and Immigrant Status Indicator Technology pilot program for identifying visitors as they exit the United States.

COL. GREENE: WE'RE TRYING TO CHANGE CULTURE

By Josh Davidson, Team C4ISR KC,
Symbolic Systems Inc. – Date: 23 Jan.
2007

The Communications-Electronics Lifecycle Management Command (C-E LCMC) is experiencing a culture shift, where its personnel are asked to think and function beyond stovepipes. Senior leaders have indicated that less stove piping will reduce the creation of redundant systems and lessen the technology gaps among the many Team C4ISR systems.

During a recent interview, Col. Harold Greene, Project Manager for Battle Command (PM BC), emphasized that integration of systems and staff will yield improvements for both the taxpayer and Warfighter. PM BC is an example of a PM whose systems rely on capabilities or organizations that span across the C-E LCMC. Like other C-E LCMC leaders, Greene requires his staff to think in terms of an overarching System of Systems rather than a singular product.

PM BC physically demonstrated the System of Systems concept in April 2006 at Fort Dix, NJ, when it took three of its own systems and consolidated them onto one server stack called Tact-Pak. This allows individuals to use all three systems – the Battle Command Sustainment Support System (BCS3), Maneuver Control System (MCS), and All Source Analysis System-Light (ASAS-Light) – with only one laptop. One might consider Tact-Pak a leap for an Army where most systems require a dedicated terminal and an improvement for the Warfighter who used to use grease pencils and acetate maps to plan missions. And, of course, the use of less hardware and software will save taxpayer dollars in the long run.

During April's successful proof-of-concept evaluation for Tact-Pak, Soldiers from the Army's 1st Brigade, 78th Division used 10 BCS3, 30 MCS, and six ASAS-Light systems. Rather than requiring a dedicated laptop computer for each of the 46 applications, the Tact-Pak allows multiple Battlefield Functional Area systems to be consolidated into a single cluster made up of fewer servers.

Col. Greene recently spoke with the Team C4ISR Knowledge Center about C-E LCMC-wide efforts to remove stovepipes, the System of Systems concept, and the recent renaming of Product Manager MCS to Product Manager Tactical Battle Command (PdM) TBC.

Team C4ISR Knowledge Center: As you're moving towards a System of Systems, how important is it to move away from stove piping and for Project Managers (PMs) to be aware of what other PMs are doing.

Col. Greene: We're trying to change culture here. We're trying to take away the mentality that it's all about my product and change people to thinking that it's all about the capability provided by the System of Systems. And that requires a change in thinking.

With most of these problems, there is a technical element to it, but the far bigger problem is the people problem of getting people to think about the whole as opposed to their one thing. So, that's part of why we put together (Product Manager) Tactical Battle Command. Those five products (core server infrastructure, publish and subscribe engine, MCS, the Command Post of the Future (CPOF), and the Web portal) frequently had duplicative capabilities. Frequently, more than one product would be developing a similar capability at the same time because they didn't know what the other guy was doing. So, not only was it inefficient, but we frequently created interoperability problems because 'A' didn't know what 'B' was doing. So, let's put it all together in one place and give ourselves a core that makes sense.

Team C4ISR Knowledge Center: How has PdM TBC progressed? How is it moving the Army towards more of a System of Systems and less redundancy?

Col. Greene: First, we're reducing the footprint. Just one initiative they're doing, server consolidation, we estimate saves nearly \$2 million per division that we field in hardware costs and over time it's even more because we don't have to pay for field support for the vast array of servers.

As an example, there're five main components to what the Tactical Battle Command folks are fielding, that came from five separate offices, previously, who designed five separate support strategies and all had field support representatives out there. So, what we've done now is – we're reducing the amount of hardware – about a 40 percent reduction in server hardware costs per division is what we believe we'll get. We're reducing the amount of field service support and it's physically smaller because we're sharing assets now. So, the units don't have to have as many generators to run them. You don't have to have as much cooling; you don't have to have as much space, weight and cube when you deploy to a theater of operations.

Team C4ISR Knowledge Center: So, I guess it's becoming a little closer to what we're using in our offices when it's moving towards one server and one seamless system?

Col. Greene: What we want to do is follow a commercial model. To give you an analogy, Army Battle Command in the old days was based around functional systems. That came from requirements from functional TRADOC (US Army Training and Doctrine Command) schools. So, if you wanted to do fires calculations you went to AFATDS (Advanced Field Artillery Tactical Data System). If you wanted to do intelligence, you went to ASAS. If you wanted to do maneuver, you went to MCS. That's not how you do things on your desktop.

You don't go to a different computer to do word-processing and PowerPoint and Excel. They're different applications that you access through a common client laptop or desktop computer. That's where we're trying to go. We're trying to move functionality to the network and then have a common client that can access that functionality so that the box you're looking at, the actual desktop or laptop, is multi-functioning and we've put the functional capability on the network not on each individual box, so that the box becomes a multi-purpose box.

So it is a fires box right now, based on who is using it, if he logs off and an intel person comes; now it's an intelligence box. If he logs off and a logistician logs on, now it's a logistics C2 (Command and Control) box. So that we don't have the one-to-one relationship between functional system and box and that box can only do that one thing. It's not what you do with your home computer.

Team C4ISR Knowledge Center: Will it build kind of a profile for say a logistician, so when he logs on he will have everything he needs in front of him?

Col. Greene: As we migrate to the future, what we're trying to do is go to role-based access; both security and capabilities. It's going to be a few years, but as we adopt the Net-Centric Enterprise Services (NCES) security model and the active directory security model, which are the standards that OSD (Office of the Secretary of Defense) is going to use in garrison network settings, we'll be able to provide role-based access.

So, what you can access on that tactical system will depend on who you are and what permissions you've been given. So, if you're an intelligence person and you have a top-secret clearance and a need to know, then you would get access to the appropriate intelligence information. If you were a fire support person and you logged on you would have a profile and a set of permissions that would allow you to do what it was that you needed to do and so forth.

What we would like to get to and this is a few years away is: you don't have a one-to-one correspondence between your functional position in the operation center and a piece of hardware. Today, we have that. If you go into an operation center, you'll see rows of laptops, each of which have one functional purpose. It might be AFATDS to do fire support and targeting, tactical, and technical fire direction. It might be ASAS to do intelligence analysis. It might be MCS to do management of the common operational picture and so on.

But I can't take an ASAS box and use it for MCS functions because it only has the ASAS functions. We want to get away from that and get to a model where the functional capabilities are on the network as oppose to being on particular individual box and the box is a generic laptop.

Team C4ISR Knowledge Center: That concept I guess was something that was proven during the Tact-Pak demonstration?

Col. Greene: Absolutely.

Team C4ISR Knowledge Center: Was that the first time it was ever demonstrated like that?

Col. Greene: That was the first time we did virtualization and using a common server stack to do that. Yes. So, that's where we're headed. That's an example of what we're trying to do but larger. We really designed Tact-Pak to support, right now, the training environment. Over time, we're going to use the technologies there to do what I am talking about.

Josh: So I guess that was a big step, to be able to do that successfully in training?

Col. Greene: Absolutely.

Meeting Notices

Luncheon Meetings: Third Tuesday of the month.

Date	Time	Location
17 April 2007	1130-1300	Sheraton Eatontown

Chapter Management Committee Meetings: Last Thursday of the month.

Date	Time	Location
26 April 2007	1130-1300	Lockheed Martin Offices – Tinton Falls
31 May 2007	1130-1300	Lockheed Martin Offices – Tinton Falls

Other Functions: Annual Chapter Symposium

Date	Time	Location
15 May 2007	All day	Sheraton Eatontown

"Knowledge is of two kinds. We know a subject ourselves, or we know where we can find information on it."

Samuel Johnson (1709-1784), quoted in Boswells' Life of Johnson

"Learning is not attained by chance; it must be sought for with ardor and attended to with diligence."

Abigail Adams (1744-1818), 1780

"Logistic considerations belong not only in the highest echelons of military planning during the process of preparation for war and for specific wartime operations, but may well become the controlling element with relation to timing and successful operation."

Vice Admiral Oscar C. Badger, USN

Think of this as a guiding principle behind Performance-Based Logistics (PBL). "Not everything that can be counted counts, and not everything that counts can be counted."

Albert Einstein (1879-1955)

Here are two from great warriors.

"Age wrinkles the body. Quitting wrinkles the soul."

General Douglas MacArthur

"A military operation involves deception. Even though you are competent, appear to be incompetent. Though effective, appear to be ineffective."

Sun-Tzu (~400 BC), The Art of War

2006-2007 Chapter Management Committee Members

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

Chapter Chair
Rich O'Donnell
732-532-3460

richard.f.odonnell@us.army.mil

Vice Chair, Finance
Bob Featheringham

732-818-0441

two_feathers@comcast.net

Vice Chair, Administration

Maureen Boyette

732-758-0180

mboyette@multimax.com

Vice Chair, Prof. Development

Ron Fulton

732-552-7092

ron.fulton@L-3com.com

Awards Cmte. Chair

Maureen Boyette

732-758-0180

mboyette@multimax.com

Publicity Cmte. Chair

Steve Bromka

732-532-7984

steven.bromka@us.army.mil

Government Affairs Cmte. Chair

Gloria Richardson

732-532-6752

Gloria.richardson1@us.army.mil

Vice Chair, Member Services

Bill McLean

732-532-4569

william.mclean2@us.army.mil

Vice Chair, Education

William Hogelin

732-427-6321

william.hogelin@conus.army.mil

LEF Liaison

Mike Ryskamp, C.P.L.

732-427-4260

j.michael.ryskamp@us.army.mil

Publications Cmte. Chair

Dr. Michael Harris, C.P.L.

609-997-0489

harrisM100@comcast.net

Symposium Cmte. Chair

Ken East, C.P.L.

732-460-1370

keast@logsec.com

Industrial Affairs Cmte. Chair

Janet Steinberg

732-389-0390

janet.steinberg@lmco.com

Immediate Past Chapter Chair

Charles Hodell

732-389-5359

chuck.hodell@lmco.com

