

The DEPLOYER

<http://tcaccis.army.mil>



Volume VII Issue 1

Spring 2002

Message from the PM



As I write this, the JPMO, TC AIMS II is preparing for the follow-on evaluation of improvements made based on OT findings, work is underway with block 2, HQDA is selecting a TC AIMS II CONUS beta site and we are midway through a physical that consolidates all of our offices. The initial OT highlighted some areas requiring improvement to which we addressed.

With nearly 200 software improvements since IOT&E, new documents to help the user operate the system and improved training (updated lesson plans, new student guides) etc., we can claim a better overall product. We expect to undergo a series of assessments, beginning with the Navy on 13 May that will verify the system's operational effectiveness, suitability and survivability. During the post OT phase, we met with FORSCOM, HQDA G-4, The Army Testing and Evaluation Command ([ATEC](http://www.atec.army.mil/) (<http://www.atec.army.mil/>)) and the Deployment Process Modernization Office ((DPMO) <http://www.deploy.eustis.army.mil/>) to review the initial OT findings in excruciating detail at very senior levels (both the FORSCOM G3 and G4 participated). This was a very worthwhile exercise to directly explain some OT issues to key participants. A separate article covers the establishment of a new CONUS beta site. There are many details to attend to with this seemingly simple charge. We're looking forward to the lessons we can learn about overseeing the transition of current CONUS users of TC ACCIS and SIDPERS to TC AIMS II. The establishment of beta sites is important in another way: It moves the

PM Message, Continued on page 2



The Deployer Mission Statement

The mission of the Deployer is two-fold:

To provide information on an improved Defense Transportation System brought by TC AIMS II. and to provide the current TC ACCIS community of system endusers, sponsors, and interested parties with useful information on technology, procedures, and organizational matters. ☐

TC AIMS II Moves to Windows 2000

The TC AIMS II application will migrate to the Windows 2000 operating system in June 2002 however the TC AIMS II application on the Windows NT operating system baseline will continue to be supported until all organizations complete the transition. As TC AIMS II has not begun formal fielding yet, this OS migration will have limited effect.

Why the move?

Certain modifications in Windows 2000 will make it more "in synch" with Office 2000. Windows 2000, unlike Windows NT 4.0, will support the universal serial bus (USB) technology. With USB, up to 127 devices can be linked together (with hubs). Moreover, the USB is hot swappable and the plug-ins are configured such that it cannot be inserted incorrectly. 2000 will offer full Plug & Play capabilities. Plug and Play is that capability that allows a computer system to recognize and adapt to hardware configuration changes with little or no user intervention. Plug and Play will allow one to insert, say, network cards (the cards that allow the computer to "talk" to the network) which the computer will subsequently identify and for which find the correct driver. Plug and Play allows a user to change a computer's configuration with the assurance that all devices will work together and that the machine will boot correctly after the changes are made. ☐

In This Issue

	In This Issue
2	PM Message (Continued)
2	Windows 2000 Mover Drives Training Change
3	Upcoming Ft. Lewis Beta Site Dry Run for Full Fielding
3	Upcoming TC ACCIS →GFM Interface
3	WinQvt: Reminder
4	Army Presents Deployment Excellence Awards
4	Can you say "I Secure"?
5	TC ACCIS →PowerTrak Interface Continues Fast Pace
5	Software Update Required for DAMMS-R Support
6	Technical Tips
7	Technical Tips (continued)
8	Transitions
9	Update of TC ACCIS Urged
9	Current TC ACCIS Installs

PM Message, Continued from page 1

system out of "lab" and into the actual users' hands. There is simply no substitute for the genuine and useful feedback evinced when users are given the mission to use a particular system.

We have survived our recent physical office move intact. We have had a few of the expected miscues, but we are settling in. Although the impetus for this move was a financial consideration; the move also has had the affect of bringing together the once dispersed assortment of TC AIMS II managers, developers, testers and other stakeholders. This is a good thing. The more you can collocate a project's stakeholders, the better the communication flow. The better the communication flow, the better the resultant product.

On the subject of communication flow, I want to report that our first ever TC AIMS II worldwide community meeting, held 19-20 March, was a solid success in that there was a generous attendance, a good exchange of information and either the formation or strengthening of relationships. Over one hundred folks participated from organizations ranging from USAREUR to the Navy, from the Marine Corps to HQDA. A copy of the PowerPoint presentation given at the conference are at <http://www.tcaimsii.belvoir.army.mil/wwuc.htm>.

I continue to look forward to making this system meet the deployment and transportation communities needs. ☐



Ft. Lewis Strong Contender

FORSCOM to Select New Beta Site

In June/July, members of the JPMO will arrive at a FORSCOM installation, to be determined, and convert it into a TC AIMS II beta site. This is no small feat. Before the team arrives, equipment will have been configured, tested and loaded with legacy data. Coordination will have occurred with the local DOIM for network access.

One of the most important jobs is that of providing training to unit movement officers, unit movement coordinators and system administrators. Each unit movement officer course lasts one week, the unit movement coordinator classes runs for nine days and the system administrator course will last five days. The plan is for a total of 24 classes.

To help provide the most useful TC AIMS II data, the JPMO will first scan the TC ACCIS data looking for particular instances of troublesome data. This scan will produce a customized checklist for each unit alerting it to specific instances where records should be modified to facilitate a better transfer to TC AIMS II. For instance, the scan will produce a list of known expired Lin/Lin Indexes.

Even after units have completed this "scrub," some work will have to be done once the data is in TC AIMS II. This is because TC ACCIS and TC AIMS II are two different systems, which sometimes have distinct data requirements. The JPMO is actively looking at automated ways to speed up the data transition process, but there is no escaping the requirement for the active involvement of the units. ☐

Windows 2000 Move Drives Training Change

Prospective students for TC AIMS II Systems Administration training course should have knowledge and experience of systems administration in the Windows 2000 operating environment. The Windows 2000 operating system knowledge may be acquired through either a commercial or government course - classroom, web based or computer based formats are acceptable

Doug Garrell, the TC AIMS II JPMO Chief, ILS division reminds you that the TC AIMS II systems administration course is designed for a student who has attained level 1 systems administrator skills as defined by ASD(C3I) Memorandum, dated 29 June 1998, Subject: Information Assurance Training and Certification. This memorandum defined level 1 skills and task as:

Skills include zero to one year experience administering the relevant operating system, formal training for the operating systems and command language (commercial or government course), and strong customer relations skills. Task for level 1 include backups; restores; adding/modifying/deleting user accounts; installing operating systems, applications, and peripherals; troubleshooting user problems; debugging command language scripts and assisting he ISSO in access control security.

Questions or comments for this action should be addressed to Mr. Doug Garrell (703) 752-0759 ☐



Upcoming TC ACCIS → GFM Interface May Require Extra User Diligence

The next TC ACCIS release, expected within months, will provide an interface with the Global Freight Management System (GFM). TC ACCIS data sent to GFM through this interface will be converted to electronic feeds to commercial carriers and PowerTrack, a financial clearinghouse. These electronic feeds will be in a form specified by the American National Standards Institute (ANSI) in their Electronic Data Interchange (EDI) format 858 and 404. The 858 is an electronic version of a Commercial Bill of Lading, while the 404 provides specific information to rail carriers.

When this new interface comes on board, TC ACCIS will retire the interim direct-to-PowerTrack Financial feed that has served us so well for the past 20 months (see latest article on page 5 regarding usage level of the TC ACCIS PowerTrack feed). For the system to work, users must be attentive to two things: The rail car type code and hazardous cargo information.

The rail type code is a two-character shorthand indicator that is associated with a specific type of rail car (e.g., Gondola, 89ft DODX etc). The upcoming TC ACCIS→GFM interface introduces far more capability and ease of use in terms of Hazardous Cargo. First, TC ACCIS has revised the Hazardous Material screens to allow the UMOs to enter equipment and load hazardous material information. TC ACCIS will automatically populate certain fields based on an entered proper shipment name. It will determine compatibility, UN code and other essential information elements. The UMC can review the data entered by the UMOs through a new TC ACCIS summary report. This report is designed to help the UMO produce the DD Form 836.

Although TC ACCIS will introduce features to facilitate the entry of this information, the final responsibility for ensuring that all information is entered and that all the information is correct is with the individual unit. Remember that the law provides for strict penalties or fines in instances where the appropriate statutes are not followed. ☐

Use of Valuable Utility Still in Contention WinQvt: REMINDER

In a previous "Deployer", we endorsed the use of WinQvt as a way for remote units to connect to their host sites, update their DELs, transfer the data back to a local PC, and print the information locally. This utility proved invaluable for a number of users who would otherwise have had to use TC ACCIS Microcomputer Utilities with a telephone connection.

Regretfully, we have learned that there is some contention about the allowance of TC ACCIS to use this valuable utility. This contention exists even though the utility was downloaded from an Army website.

Because of this contention, we must ask that you refrain from using WinQvt until the license issue has been resolved. In the interim, should you need to use a remote utility, we suggest that you download and set up EWAN and WS_FTP LE. These utilities are shareware, and a license is not required. We have once again explained the use of these utilities in the Fall 2001 and Winter 2002 Newsletters. The primary difference between the combined use of EWAN and WS_FTP LE as opposed to the singular use of WinQvt is that, in the former case, two products are required to accomplish what the one product, WinQvt, accomplishes. You may call the TC ACCIS Hotline for updates.

If you choose to use EWAN, please know that there is a function key issue that must be resolved prior to its use. Call the Help Desk at 1-866-TCAIMS2 for assistance.

EWAN can be downloaded from:
http://www.lysator.liu.se/zander/ewan_dl.html

WS_FTP LE can be downloaded from:
<http://www.shareware.com>.

On the search line enter ws_ftple to download.

We are working on this issue to ensure the legitimate use of WinQvt and will advise you of the outcome of our efforts. ☐

Internet Address Change

The address to the TC ACCIS Website has been changed. The new address is:

<http://tcaccis.army.mil>



ARMY PRESENTS DEPLOYMENT EXCELLENCE AWARDS

Army Logistician March-April 2002 Issue

In December, the Army recognized units that strived for excellence when deploying soldiers and equipment by air, land, or sea with the first presentation of the Chief of Staff of the Army Deployment Excellence Awards. The awards were established to recognize units and installations for outstanding deployment accomplishments that meet or exceed established standards. The awards were presented to Active Army, Army National Guard, and Army Reserve units for specific deployments completed during fiscal year 2001. Units receiving awards were:

Active installation: Fort Sill, Oklahoma, for deployment to Kuwait in support of Operation Desert Spring.

Active large unit: 3d Squadron, 4th Cavalry Regiment, 25th Infantry Division (Light), Wheeler Army Airfield, Hawaii, for deployment to El Centro, California, in support of the Joint Task Force 6 Readiness Exercise.

Active small unit: 235th Signal Company, Fort Gordon, Georgia, for deployment to Haiti in support of Operation Justinien Cause.

Active supporting unit: 266th Transportation Detachment, 24th Infantry Division, Fort Riley, Kansas, for deployment to the National Training Center, Fort Irwin, California.

Army National Guard large unit: 76th Infantry Brigade, Indianapolis, Indiana, for deployment to the Joint Readiness Training Center, Fort Polk, Louisiana, for the brigade's rotation exercise.

Army National Guard small unit: Task Force Alpha, 1st Battalion, 133d Infantry Regiment, Waterloo, Iowa, for deployment to Saudi Arabia and Kuwait as a security task force.

Army National Guard supporting unit: State Area Command, Indianapolis, Indiana, for providing full logistics support during a deployment to north Fort Polk, Louisiana.

Army Reserve supporting unit: 1395th Transportation Terminal Brigade, Seattle, Washington, for its support of Operation Puget Thunder at the Port of Tacoma, Washington. ☐

Can You Say “I Secure”?

Information Assurance (IA), often referred to as Computer Security, Information Security, or Cyber Security is currently a very hot topic and will be for many years to come. Unfortunately, the cyber world of security has tended to concentrate solely on technical solutions, rather than the human solution...YOU!



A bold statement, but true never the less. Organizations spend thousands on technical solutions such as firewalls, intrusion detection systems, biometrics and other fancy devices, but unfortunately most fail miserably when it comes to the personnel side of IA. I'm not saying we don't need those devices, of course we do. They symbolize the locks on our doors and windows etc. It does not matter how much we spend on technical solutions, there are plenty of other crude ways to penetrate the castle walls. You can have your moat, your fortified walls, and your hot oil ready to go, but if you have just one villager inside reeking havoc undetected, or the innocent villager who accidentally leaves the back door to the castle open, then watch out here comes trouble!

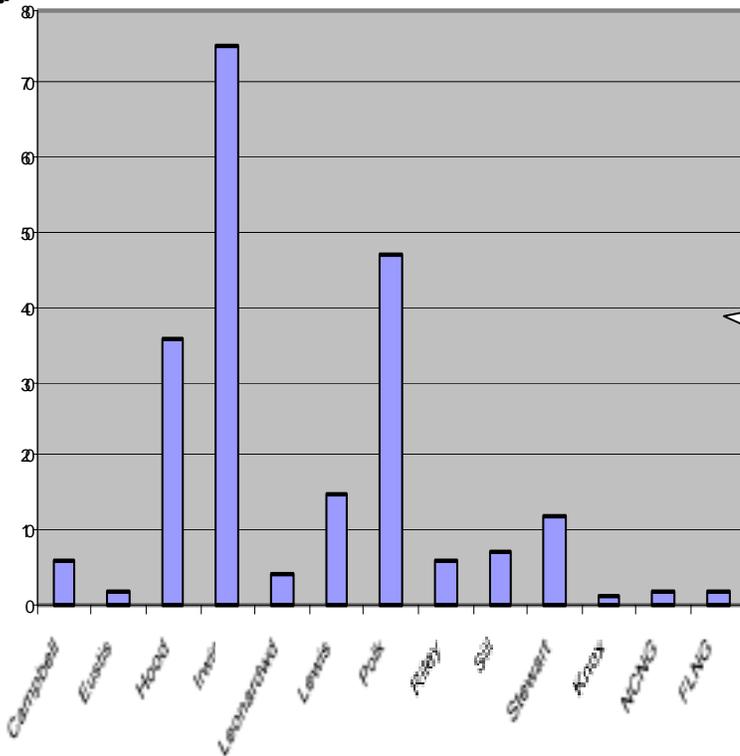
So what can you do? The first step I would always say to people is to locate your organizations security policy. Read it at least once and attempt to understand it. Knowledge is power and ignorance is no excuse. Next, take the time to find out what malicious code is, how it spreads and whether the virus warning you got from your email buddy is in fact legitimate, or a hoax. And please, please don't send out virus warnings, even if you are one hundred percent sure of its authenticity. That job function is the role of your Information Assurance Security Officer, or System Administrator. By all means forward reports to them for further investigation, or questions, but never send it out to the user community. Many hoaxes exist just to cause network congestion by users forwarding them to fellow workers, which results in a mini denial of service. The reason I mention virus research as the next thing to do after the security policy is because it is by far the most prevalent risk to the company.

Next go out and gain knowledge on what social engineering and identity theft is. It's a major problem within the US, and right now as you read this article you

Security Article. Continued on page 9

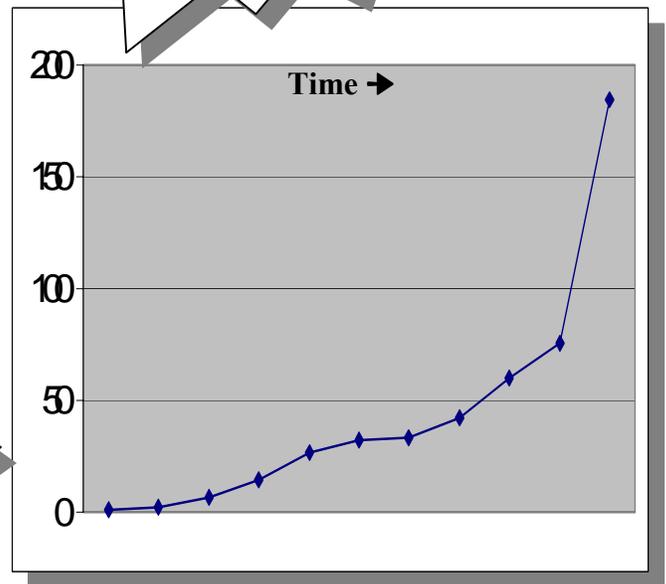
TC ACCIS → PowerTrack Interface Continues Fast Pace

Installed sites & level of use



Carriers so far:
 Burlington Northern
 Santa Fe, CSX
 Transportation,
 Kansas City Southern,
 PAL and Union

Culminate Trend line shows increasing use



Intermec Printer Supplies

Many of our users are find they are running low of Intermec 8646 printer labels and ribbons. If you find yourself in this situation and need to place an order, keep in mind that it takes approximately 2 weeks for Intermec to print and ship your supplies.

To reorder printer labels and ribbons, contact:

Intermec Government Sales
 1-800-227-9947 (Cathy)

Part numbers:

Labels: E04321 - TC ACCIS Whitewash
 Ribbons: 13084106



Software Update Required for DAMMS-R Support

Effective 18 January 2000, DAMMS-R will no longer support software package LZA-00-07. DAMMS-R enacts this "fresh software" policy to both minimize problem resolution times and save on resources.

The DAMMS-R Program Office strongly urges DAMMS-R users to have LZA-00-08 loaded at your sites as rapidly as possible. DAMMS-R delivered software package ICP LZA-00-08 to Europe in September 2001 and to Korea in early December.

Beginning immediately, the DAMMS-R technicians will require that LZA-00-08 be loaded prior to providing support.



Technical Tips

Updating Port Codes and Country Codes

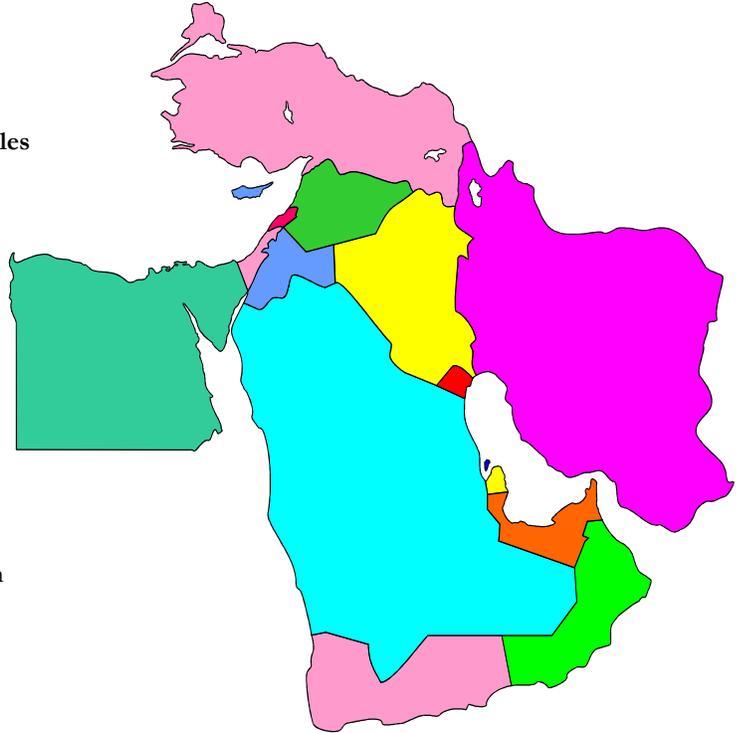
The ITO user may change the Port Codes and Country Codes within TC ACCIS. These codes are used when generating Military Shipment Labels. Changes may be due to local needs or may be prescribed by MTMC MILSTAMP as interim changes to update Port Code and County Code tables on TC ACCIS.

When required to add a new independent country:

- 1) Login in as **ITO level**
- 2) From the Main menu, select **3-Shipment Planning**
- 3) From the Shipment Planning menu, select **6-Reference Tables**
- 4) From the Reference Tables menu, select **J-Country**
- 5) From the Country Code ring menu, select **1-Add.**
- 6) At the Country Name field, enter the country name and press **ESC.**

To update a Country (perform 1-4 above):

- 5) From the Country Code ring menu, select **2-Modify.**
- 6) Type in
 - a) The **Country Name** and press **ESC**, or
 - b) To select from a list press **F6**
 1. Then press **ESC**
 2. Highlight the country desired and press **ESC**
- 7) Overtyping the **Country name** with your required change then press **ESC**



When required to add a new Port Code:

****Note**** Three-digit Port Code is prescribed by MTMC and recorded in MILSTAMP.

- 1) Login in as **ITO level**
- 2) From the Main menu, select **3 - Shipment Planning**
- 3) From the Shipment Planning menu, select **6 - Reference Tables**
- 4) From the Reference Tables menu, select **H- Port Codes**
- 5) From the Port Code ring menu, select **1 - Add.**
- 6) All information for the fields that follow will be extracted from MILSTAMP or given to you when a new port entry is required.
 - a) Port Code - Unique three-digit Port Code (Required)
 - b) DMOD - "A" for Air and "S" for Surface (Deployment mode required)
 - c) Port Name - Common Port Name (Required)
 - d) Address - Freight Address (NOT Required)
 - e) City - City (NOT required)
 - f) State - State (Required ONLY if it is in the U.S.)
 - g) Country - Country (Mandatory blank if it is within the U.S.A., otherwise required for all others.)
 - h) Zip - Zip Code (NOT required)
 - i) Ammo Ind. - "y" if ammo is accepted, "n" if isn't (Required)

Technical Tips Continued

To modify a Port Code (perform 1-4 on Page 6):

****Note**** Three-digit Port Code is prescribed by MTMC and recorded in MILSTAMP.

- 5) From the Port Code ring menu, select **2 - Modify**.
- 6) Type in
 - a) The existing **Port Code** and press **ESC**, or
 - b) To select from a list press **F6**
 1. Then press **ESC**
 2. Highlight the country desired and press **ESC**
- 7) Update the specific fields needed.
 - a) Port Code - Unique three-digit Port Code (Required)
 - b) DMOD - "A" for Air and "S" for Surface
(Deployment mode required)
 - c) Port Name - Common Port Name (Required)
 - d) Address - Freight Address (NOT required)
 - e) City - City (NOT required)
 - f) State - State (Required ONLY if it is in the U.S.)
 - g) Country - Country (Mandatory blank if it is within the U.S.A., otherwise required for all others.)
 - h) Zip - Zip Code (NOT required)
 - i) Ammo Ind. - "y" if ammo is accepted, "n" if isn't (Required)



Individual instructions may be found in the TC ACCIS – End User Manual, Sections **11.3.1.16** and **11.3.1.18**. 

Are You Missing Your F Record Serial Numbers?

One of the functions of an ITO is to "Copy" or "Reassign" equipment under the ITO's Equipment List Administration menu selection "Transfer Unit Equipment." If the ITO uses the "Copy" function to copy a unit's equipment from one TDC to another TDC and answers "1-Yes" to include serial/bumper number, TC ACCIS will replace all serial numbers for the F records with the default serial number for the F records. For example, if SUN "F0001" in TDC "D" has the serial number "112341133" then after the ITO copies TDC "D" for the unit to TDC "AF" the serial number for SUN "F0001" in TDC "AF" is now "AF-WGEH11-F0001." The UMO for the unit would have to use "Maintain" Special Handling Equipment to correct the serial numbers.

To avoid this problem, the UMO can execute a "Full Copy" or a "Partial Copy" after creating a "Unit Header" for the TDC. The serial numbers for F records from the source TDC are copied into the destination TDC. For example, if SUN "F0001" in TDC "D" has the serial number "112341133" then after the ITO copies TDC "D" for the unit to TDC "AF" the serial number for SUN "F0001" in TDC "AF" is now "112341133." The step would be:

1. ITO creates the TDC.
2. Have the UMOs create their header for Echelon/ULN for the new TDC.
3. Have UMO copy to this new TDC from TDC "D" (AUDEL) using the "Full Copy" or "Partial Copy".

This highlights another area the UMO needs to check. Currently, TC ACCIS creates a default serial number for F records. Before, it was possible to leave the serial number field blank. If the UMO executes a "Full Copy" or "Partial Copy" from one TDC to another with blank F record serial numbers then the new TDC's F records will have blank serial numbers. The UMO should review the entire unit's F records and enter a serial number for every F record. The UMO can cause a default serial number to be created in "Maintain" Special Handling Equipment by highlighting the F record and pressing <F9> to move to the detail screen and press <TAB> to move to the bumper number field. 

Transitions

We've Moved, Again

We've moved from our location at 7435 Boston Blvd in Springfield to 8000 Corporate Court Springfield, Virginia 22153.

The move was driven by cost concerns, but it had the collateral benefit of moving the entire JPMO as well as developers, testers and help desk personnel under one roof.

Brian Coady	703-752-0763
Alain Wampouille	703-752-0792
Garry Haun	703 752-0787
Mike Wang	703-752-0790
Rich Wilson	703 752-0804
Raquel Soranzo	703-752-0788
Steve Oge	703 752-0805
Valerie Sparks	703-752-0791



Dave Metheny Moves On

Dave Metheny, who began work in the JPMO TC AIMS II ILS division in 1 September 1999, is returning from whence he came; namely, the Scott AFB area. More a work horse than a show horse, during his tenure, Dave Metheny was instrumental in establishing and maintaining the TC AIMS II website, but his contribution went beyond that important role: He was directly involved in multiple fielding and training plans, authored many essential acquisition documents, contributed to the peerless TC AIMS II multimedia package and performed as a site observer for OT's

After putting in twenty-seven years for the government, Dave plans to retire in the Scott AFB area and spend time with his three children and four grandchildren. Thereafter, he plans to work with the SRA Corporation and is apt to contribute on TC AIMS II in that capacity.

Dave remains very committed to the goal of a purple system and reports that he has enjoyed the challenge of working on a program with such dedicated professionals. We wish him the best in the future. ☺

Project Manager, TC AIMS II Becomes Project Manager, Transportation Information Systems

PEO STAMIS Becomes PEO EIS

The October 2001 Army Reorganization led to the name change of PEO STAMIS to PEO EIS (for Enterprise Information Systems). The reorganization resulted in the addition of several Communications-Electronics Command Systems Management Center programs as well as the Research, Development and Acquisition Information Systems Activity to the former PEO STAMIS. The name change reflects the growth of overall responsibility that the PEO has seen from an original 13 systems to know over 50 systems and products.

The business of Program Executive Office, Enterprise Information Systems is the business of the US Army. PEO EIS systems touch every soldier, every day, regardless of their location or mission. They are therefore directly involved in achieving the Army's Vision.

The information management systems PEO EIS acquires and fields, assist with the accession and training of our soldiers, track the Army's personnel, provide and maintain the war fighter's equipment, and plan the movement of their supplies and assets. ☺

Security Article, *Continued from page 4*

could already be a victim of identity theft, or have been subjected to a social engineering attack that was aimed at you. I would also advise that gaining knowledge on—

- What constitutes network abuse within your organization
- When you use your work PC for personal use (if at all)
- What are the incident reporting procedures for your organization
- Laws and regulations, such as the Computer Security Act 1987 and Army Regulation (AR)380-19.

You don't need an in-depth knowledge of all these subjects, but a general awareness is a good idea. Of course most, if not all these things should be covered within your organization's security policy. But don't worry if you can't find everything, or don't have the time to go out and research, because I will cover these topics in later articles.

Lastly, DoD/AR policy states that all users of DoD Automated Information Systems (AIS), regardless of being military, government employees, or government contractors, must receive Information Assurance Awareness training on an annual basis at a minimum. If you have not received such training, please ask your Information Assurance Security Officer, or Chain of Command. It's the best way for you to keep abreast of the current threats and what is expected of you by your organization. If you have any questions or comments I can be emailed at the following address:

mark.logalbo@eis.army.mil

Until the next article, stay secure! ☒

Mark LoGalbo
Senior Computer Security Specialist
Titan Corporation

Update of TC ACCIS Urged

In every newsletter we update the **Current TC ACCIS Install** chart. This chart has not changed much in the past several months. We still have **4 sites** working from version



5.0.116. It is very important that you upgrade as soon as possible to take advantage of the more recent reference data and the GATES interface. If you have misplaced your install tape, please contact us at the customer support number **(703) 752-0806** or **1-866-TCAIMS2**. We will send you another tape. Please make the time to upgrade your system. ☒

Help Desk Toll-Free Number is Back!

Great news for Transportation Information System customers. We have a toll-free line for customer support. For questions about either TC AIMS II or TC ACCIS, dial--

1-866-TCAIMS2 (822-4572)

CURRENT TC ACCIS INSTALLS

E-Mail of the Deployer Newsletter

The TC ACCIS PM is requesting that all recipients of the TC ACCIS/TC AIMS II newsletter send their e-mail address to the TC ACCIS POC.

Newsletters will continue to be mailed to those who do not have e-mail available.



POC: Valerie Sparks (703) 752-0791
E-mail: Valerie.Sparks@eis.army.mil ☒

