WORTH REPEATING

“Relationships are what this is all about. I think, in truth, relationships are what everything is all about, whether our own home life or international relations. And all we are trying to do is, sort of, one handshake at a time or one smile at a time, one Beanie Baby at a time, to add a little joy and strength to this relationship.”

— Gen. David H. Petraeus, emphasizing the importance of relationships in achieving common goals in Iraq

Soldiers at the NTC to Train in Largest Simulated City, PEO STRI Supports After Action Review Instrumentation Efforts

By Kristen A. Dooley, PEO STRI Public Affairs Officer

Soldiers at the National Training Center at Fort Irwin, Calif., will soon receive the largest Military Operations on Urban Terrain (MOUT) site in the Army. This type of instruction prepares Soldiers to defeat enemies intermingled with noncombatants in an urbanized environment.

The U.S. Army PEO STRI is responsible for instrumenting the facility with video capabilities to include internal and external cameras, microphones and battlefield effects. “MOUT video instrumentation allows the units to capture their actions and conduct more immediate and effective After-Action Reviews (AAR) while the unit is still occupying the training site,” said Lt. Col. Jack Emerson, PEO STRI’s product manager digitized training. “Having the capability to conduct immediate AARs allows the unit leaders and observer controllers the opportunity to critique the team’s short comings and re-train those actions to achieve the desired training objective before deploying,” Emerson added.

The first phase of the MOUT site, otherwise known as the National Urban Warfare Complex, was completed last October. PEO STRI’s instrumentation was emplaced after the construction was finished. For the remainder of the four phases, PEO STRI is working with the Army Corps of
PEO STRI Celebrates the Holidays
Army aviation continues to successfully “fight the fight” in support of operations while simultaneously transforming and modernizing its forces. That was the consensus of a panel of aviation commanders at the Association of the United States Army’s Institute of Land Warfare Aviation Symposium and Exposition.

“As rapid as innovations occur, we are challenged daily with updating our doctrine, improving our training and sharing lessons learned, all while continuing operations in theater,” said Col. Kevin W. Mangum, commander of the 160th Special Operations Aviation Regiment (Airborne), at Fort Campbell, Ky. “We have the systems, we just have to continue to train with them,” he added.

In recent years, the combination of a significantly increased operational tempo and advancing technologies has presented various challenges, said the commander of the 25th Combat Aviation Brigade, which redeployed from northern Iraq recently back to Schofield Barracks, Hawaii.

“We are making vast improvements materially, but our training capacity to integrate new systems into the war fight as soon as they are received needs to be enhanced,” said Col. A. Thomas Ball Jr., 25th CAB commander. “It is vital that we have the ability to train before we are ‘in the box.’ Not individual training, but collective training to synergize as a unit.” Ball praised training exercises, which he says allow simulation and integration of everything from personnel and materials to system utilization.

Challenges aside, Ball said improvements include the development and continued refinement of advanced intelligence, surveillance and reconnaissance platforms. Unmanned Aerial Vehicles and manned aircraft equipped with aerial sensor platforms have proven invaluable in theater, he said.

“We can look at an area from thousands of meters out and see real-time what assets need to be deployed,” Ball said. “We have the ability to be that far away and engage a target, removed from heavy machine-gun fire. It is amazing.”

Another issue facing the aviation community is maintaining a “fix forward” capability in support of operations. “We have the money and tools, but not necessarily the engineers, machinists and others on the lines,” Col. Daniel J. Shanahan, commander of the 1st Air Cavalry Brigade said.

According to Ball, even while maintaining a high operational tempo year in and year out, the system improvements and sustainments have seen them through battle. “That is a testament to our Soldiers, our contractors, and our equipment.”

Mangum added that as the Army continues to employ emerging technologies, it is more reliant on contractors for their technological expertise. “We could not do what we do without a large contractor footprint.”

Retention is a future challenge all three commanders anticipate. “Vibrant force maintenance is a must,” Shanahan said. “We need to put more money into incentives to keep our senior NCOs [non-commissioned officer] and warrant officers,” he added.

“It comes down to retaining the best and the brightest,” Mangum concurred. “They are the Soldiers with the experience, expertise and commitment needed.”

All agreed that there is an Army-wide concern for the well being of Soldiers and their Families. Some Soldiers have been in theater supporting Operations Enduring Freedom, Iraqi Freedom and various other operations three times in six years.

“Soldiers, ‘ruck up,’ and do a great job,” Ball said. “The family challenges are the biggest concerns when things like deployment schedules change. They don’t have that Soldier there to assist them with things like moves, changing schools, finding new jobs. There isn’t anyone to help shoulder those burdens.”

As Soldiers continue to train and operate in an ever-changing environment, and their Families continue to deal with the pressures that come with deployments, commanders take lessons learned and training developed in theater and apply them to Army aviation’s future role. “The best thing to come out of the fight is the teamwork of program managers and Warfighters,” Ball said. “We are sharing feedback and making improvements every day.”
PEO STRI employee received a phone call Dec. 11 from a person who claimed to work for the Department of Labor. Our employee recognized the caller’s phone number to be an out-of-country number and became suspicious when the caller began to ask for contact information for another employee. Our employee continued the conversation and tried to obtain as much additional information as possible. At the conclusion of the call, our employee immediately reported the incident to the Security Office.

Another PEO STRI employee received a phone call Jan. 4 from a telephone number that registered as “private” on the caller ID phone display. The caller had a heavy foreign accent and requested information regarding the employee’s fax number and e-mail address. The caller refused to identify himself or his organization other than making a vague reference to the Bureau of Labor. Our employee did not provide any of the information requested by the caller and at the completion of the call, immediately reported the incident to the Security Office.

In both instances the responses and actions of our employees were both timely and correct. Both employees provided the Security Office with a brief statement explaining their experience and that information was immediately forwarded to the Orlando Resident Office of the 902d Military Intelligence Group. Intelligence assets of the 902d and other federal agencies become involved in an attempt to identify and act on these and any other suspicious activities directed against the United States.

What we know for certain is that two of our employees were probed within a 30 day frame of time. We don’t know how many other employees have been probed and might have decided not to report the information.

Please remember, phishing can happen via phone or e-mail. If you have been the recipient of similar suspicious inquiries within the past two months, please contact the Security Office.

If you receive a suspicious inquiry:
• Don’t try to determine if the person has a malicious intent.
• Don’t dismiss it as a nuisance.
• Do try to remember as much information as you can; document the conversation or e-mail and immediately report it to the Security Office.

Advisory: Phishing Is Not Limited to E-mail

By Bill Osborne, Chief Security Officer

In October 2007, the U.S. Army Corps of Engineers finished construction on the $12 million phase one of the Military Operations Urban Terrain training site at the National Training Center. PEO STRI is instrumenting the facility with video technology for after-action review capabilities.

Endorsed by our Directors and all of STRI’s employees, PEO STRI’s involvement with this facility is a model for the Corps of Engineers. Since the program’s inception in 2003, the Mobile MOUT has been fielded to 41 locations to support Army, Marine Corps, Air Force and Homeland Security training.
Report Suspicious Cyber Incidents

SYSTEM FAILURE OR DISRUPTION
Has your system or website’s availability been disrupted? Are your employees, customers, suppliers, or partners unable to access your system or website? Has your service been denied to its users?

UNAUTHORIZED CHANGES OR ADDITIONS
Has anyone made unauthorized changes or additions to your system’s hardware, firmware, or software characteristics without your IT department’s knowledge, instruction, or consent?

SUSPICIOUS QUESTIONING
Are you aware of anyone attempting to gain information in person, by phone, mail, e-mail, etc., regarding the configuration and/or cyber security posture of your website, network, software, or hardware?

SUSPICIOUS E-MAILS
Are you aware of anyone in your organization receiving suspicious e-mails that include unsolicited attachments and/or requests for sensitive personal or organizational information?

UNAUTHORIZED ACCESS
Are you aware of anyone attempting (either failed or successful) to gain unauthorized access to your system or its data?

UNAUTHORIZED USE
Are unauthorized parties using your system for the processing or storage of data? Are former employees, customers, suppliers, or partners still using your system?

UNAUTHORIZED CHANGES OR ADDITIONS
Has anyone made unauthorized changes or additions to your system’s hardware, firmware, or software characteristics without your IT department’s knowledge, instruction, or consent?

We encourage you to report any activities that you feel meet these criteria for an incident. Note that our policy is to keep any information specific to your site and system confidential unless we receive your permission to release that information. US-CERT has partnered with law enforcement agencies such as the U.S. Secret Service and the Federal Bureau of Investigation to investigate cyber incidents and prosecute cyber criminals.

Report an incident to the
U.S. Computer Emergency Readiness Team
Incident Hotline: 1-888-282-0870
or
www.US-CERT.gov
For more cyber tips, best practices, "how-to" guidance, to sign up for technical and non-technical cyber alerts, and to download this poster, visit www.US-CERT.gov
U.S. Army Program Executive Office for Simulation, Training and Instrumentation Interactive Simulation Technology Displays on Capitol Hill

PEO STRI will be demonstrating the world’s best training and testing simulations provided to the world’s best military force.

Members of Congress will be able to see, touch and experience some of the simulation technologies that prepare our Warfighters for their global missions.

**Tuesday, February 5, 2008**
10:00 a.m. - 6:00 p.m.

Senate: Dirksen Auditorium, Room G-50
Sponsors: Senator Bill Nelson (FL)
Senator Mel Martinez (FL)

**Thursday, February 7, 2008**
10:00 a.m. - 6:00 p.m.

House: Rayburn Foyer
Sponsors: Representative Tom Feeney (FL-24)
Representative Randy Forbes (VA-4)
Representative Ric Keller (FL-8)
Representative Solomon Ortiz (TX-27)
Looking Ahead: STOC II Poised to Train Soldiers Efficiently, Effectively

By Kristen Dooley, Public Affairs Officer

The Simulation and Training Omnibus Contract (STOC II), scheduled for award this fall, marks an important milestone for the U.S. Army as it will provide Warfighters with the next-generation of simulation and training devices to meet the challenges of the joint operational environment. According to PEO STRI acquisition center officials, the contract will also facilitate the Army’s transformation toward a fully interoperable training environment.

PEO STRI intends to release the final request for proposal in the near future. The deal is slated to be the second largest contract awarded by the agency. With the award potentially valued at $11 billion over a 10-year period, this comes in just under the $11.2 billion Warfighter Field Operations Customer Support contract.

The omnibus contracting vehicle is a set of multiple-award indefinite delivery, indefinite quantity contracts to provide troops with simulation, training and instrumentation products and services beginning with concept development and continuing through lifecycle support.

Thomas Bunch, PEO STRI contract specialist, explained the significance of awarding STOC II to multiple prime contractors: “It’s good because not only does it sustain the industry base, but it also allows the PEO more choices to satisfy the customers’ needs.”

In other words, the contract will establish a set of pre-qualified contractors. When PEO STRI receives a requirement for a product or service, they will turn to the predetermined industry base that is situated to meet the customer’s needs in a highly expeditious manner.

The contractors can consolidate efforts to offer a “best-of-breed” solution. They can also solicit work to companies not on the STOC II contract. Teams, therefore, are assembled on an order-by-order basis and come together at the delivery and task order level.

Contractors not awarded the STOC II contract can still do business with PEO STRI. “STOC II is anticipated to be the main, but not only, contracting vehicle,” Bunch said. “It is our hope that the prime contractors team up with other companies, STOC or not, to provide our customers with the best possible solution.”

GOLF CHAMPS

More than 50 PEO STRI employees and their family members participated in the fourth annual PEO STRI team golf championship Dec. 26 at Eastwood Golf Club in Orlando, Fla. The Business Operations Office team, including Carol Murphy, Rob Reyenga, and Walt Pezzolo pictured here, won the event. Congratulations to long drive champions Kristy Murray, Jim Skurka, Pete Gaffney, and Caleb Ryan.

2008 Conferences & Events

Capitol Hill Demonstration
Feb. 5 - 7 – Washington, D.C.

IDE Conference
Feb. 16 - 19, New Delhi, India

Association of the U.S. Army Winter Symposium
Feb. 27 - 29, Fort Lauderdale, Fla.

Department of Defense Modeling and Simulation Conference
March 10 - 14 – Orlando, Fla.

Army Aviation Association of America Convention
April 6 - 9 – Washington, D.C.

International Training Exhibition and Conference
June 10 - 12 – Stockholm, Sweden

Training, Simulation and Industry Symposium
June 16 - 18 – Orlando, Fla.

National Guard Association of the U.S. Conference
Sept. 20 - 22 – Baltimore, Md.

Association of the U.S. Army Annual Meeting
Oct. 6 - 8 – Washington, D.C.

Interservice/Industry Training, Simulation and Education Conference
Dec. 1 - 4 – Orlando, Fla.
I think most of us are doomed when resolving to do something new, just because it's a New Year. I've decided to take a few things that I enjoy and try to do them more frequent, like taking photos of my son as he grows, reading some good books and cooking for my family.

Amanda Zinnert, PM ITTS

My New Year's resolution is to exercise regularly and maintain good health. I also plan to read the entire Bible this year so I can strengthen myself both physically and spiritually in 2008.

Vicky Wei, Acquisition Center

My New Year's resolution is to live a healthier life in 2008. I plan to cut back on eating at fast food and buffet-style restaurants.

Skyler White, PM ITTS

I did not make a formal New Year's resolution this year, however my first day of 2008 was pleasantly uneventful—a quiet day at home with family. That actually represents my aim for 2008. I will strive for excellence and discipline in my work and physical health, but more importantly, my goal is to make time to 'be still,' enjoying my beautiful son, cherishing my amazing husband, and thanking God more often for all of His mercy and provisions.

Glynn Vincent, PSG

Want your opinion heard? Answer February's Question! Who is your favorite celebrity and why? Send your response to kristen.dooley@us.army.mil and put Citizen STRI in the subject line.
Many of us travel overseas for official business and take a laptop along for the ride. Laptops have become a necessity when conducting business. Unfortunately, computers are a high-target item for theft as well as the compromise of information. There are steps that can be taken to minimize the risk to laptops and information when traveling abroad.

Ideally, the best course of action is not to take a laptop on travel, however it is sometimes unavoidable. If you take your permanently assigned laptop on travel, there is specific guidance from the PEO STRI Information Assurance Manager that you should bear in mind.

All data carried on the laptop must be in the encrypted file system. Also, your laptop should have both a label stating that it is authorized to be used for travel and a label stating the laptop contains only unclassified information. Both labels are available through the laptop shop.

Remember that all users who take laptop computers out of the workplace for periods exceeding 10 working days must have the computer scanned by the Help Desk before it can be reconnected to the PEO STRI Local Area Network, or LAN. This scanning can be scheduled through the Help Desk.

Airports offer an inviting atmosphere for thieves due to large crowds, hectic schedules and weary travelers. The most basic guidance for protecting your laptop from theft while traveling is to treat it as you would your wallet or purse. First of all, hold on to it and do not let it out of your site in airports and other public areas. If you must set it down at the airport counter or registration desk, hold it between your feet. Keep an eye on your laptop as it goes through the security check point at the airport. Always carry your laptop and do not stash it in your checked luggage. And of course, never leave your laptop unattended.

You must also remember to protect information if using your laptop in the airport while waiting for your flight. While in any public place, do not display anything on your laptop screen that you would not want anyone else to see.

This may seem obvious, but it is easily forgotten as we tend to focus only on our work and not our surroundings. A survey of 600 travelers found that one-third of the responders admitted to looking at someone else’s laptop screen while flying.

Many of us are unaware of vulnerabilities other than theft that exist overseas. In addition to protecting your laptop in airports, you have special vulnerabilities in your hotel room, while in transit, and in any office that local foreign nationals have unrestricted access. Laptops are an extremely attractive target for foreign intelligence collectors since they concentrate so much valuable information in one place.

“Bag Operations” is the term commonly used to describe surreptitious entry into hotel rooms to steal information. This type of operation is quite common and routine practice in several countries, frequently with cooperation of the hotel staff. Government travelers often report that their belongings have been searched while they were absent from their hotel rooms. Seldom is anything missing, but the purpose is to copy documents or download information from laptops.

The best course of action is to take your laptop with you when you leave your hotel room. If you must leave your laptop behind, lower the risk of theft by keeping it out of site. Never keep passwords anywhere in the room. Lock it securely in another piece of luggage. Placing the computer in a hotel vault or room safe should make it secure from theft, but in some foreign countries it may not be secure from access by local intelligence or security personnel.

One recommendation is to leave your permanently assigned laptop at home. It is a good idea to check a “blank” laptop out from the Laptop Shop and place the files you will need to access on the AKO or DKO portal. After all, when packing for a trip most people would not pack their entire closet of clothing, they only take what they need. The same holds true for your laptop. Why risk all of your computer files to potential loss or compromise when you can avoid it by borrowing a laptop for your trip?

Finally, remember that foreign government offices are vulnerable to both burglary and theft of information by local national employees. In many countries some of these employees cooperate voluntarily with the local security or intelligence service. Be aware of your surroundings and do not leave your laptop unattended.

As always, a travel briefing is required prior to your departure. We will notify you of any known vulnerabilities you may face when using your laptop in your destination country.
The presidential primaries kicked-off a few weeks ago and the competition among the candidates has been exciting to watch. Politics is at the top of the news and on everyone’s minds.

You may wonder what the rules are for federal employees who would like to take part in the political process. This article describes the “dos” and “don’ts” of participating in political campaigns for federal employees and military members.

### Federal employees in the Department of Defense MAY:

- Run as candidates for public office in NONPARTISAN elections;
- Register and vote as they choose;
- Participate in voter registration drives;
- Express opinions about candidates and issues;
- Contribute money to political organizations;
- Attend political fundraising functions;
- Attend and be active at political rallies and meetings;
- Join and be an active member of a political party or club;
- Sign nominating petitions;
- Campaign for or against candidates and issues, including placing bumper stickers on personally owned vehicles;
- Make campaign speeches for candidates in partisan elections;
- Distribute campaign literature (off-duty and off work premises); and
- Hold office in political clubs or parties, including serving as a convention delegate.

### Federal employees in the Department of Defense MAY NOT:

- Wear political buttons on duty;
- Engage in political activity while on duty, while wearing an official uniform or while using a government vehicle;
- Use official government resources, such as e-mail, to send political information to other employees or engage in political activity;
- Use official authority or influence to interfere with an election;
- Solicit, accept or receive political contributions on duty or from subordinate employees;
- Solicit or discourage political activity of anyone doing business with the agency;
- Run as a candidate for public office in partisan elections.

For more information, see the Legal Tab on the Knowledge Center under the topic entitled “Political Activities.”
Welcome Home

Operation Enduring Freedom and
Iraqi Freedom Warfighters

Saturday, Feb. 23, 2008, 10:00 a.m. - 3:00 p.m.
5201 Raymond St., Orlando, Fla. 32803

Sponsored by the Orlando VA Medical Center's OEF/OIF Program

For more information, contact Fanita Jackson at 321-397-6272 or
Tracy Lee Baker at 321-397-6192.

Celebrating Gratitude for Veterans and Their Families!
Gina Guerzon joined PEO STRI in December 2007 as the organization’s first Freedom of Information Act (FOIA) officer. She is responsible for releasing sought-after information and documents controlled by the U.S. government to the public.

“I respect and understand our accountability to the public and their right to know. I am also very aware of the government’s sensitivity toward certain information,” Guerzon acknowledged. “It’s my job to protect the government as well as inform the public.”

Before Guerzon assumed the role of the organization’s FOIA officer, the Naval Air Warfare Center Training Systems Division handled PEO STRI’s requests. When PEO STRI gained Army contracting authority, the office was stood-up to support any external petitions for contractual information.

“Once the information is released to the requestor, it is considered to be a public document,” Guerzon noted. “For instance, I can’t release certain information to one person and not release it to another.”

“A seemingly daunting task, Gina applies all the appropriate laws, regulations and processes in determining what information is releasable for the public,” said Walt Pezzolo, business operations manager who oversees the FOIA office. “So far, working for PEO STRI has been a great professional experience because I am able to constructively increase the public’s knowledge of PEO STRI,” she said.

In her relatively short time with the agency, Guerzon said she has been quite busy with the number of FOIA requests she has already received. Since December, PEO STRI has received seven requests, four of which have been on the Warfighter Field Operations Customer Support contract.

Fulfilling each request is a tedious process, Guerzon noted. If the requested information falls under PEO STRI’s authority, she contacts the contracting officer or specialist responsible for the procurement.

Once the contracting employee obtains the files, Guerzon goes through the paperwork and redacts any material that meets the disclosure exemptions. Classified material, labor rates, proprietary information, trade secrets, profit margins, contractor names and their contact information are all qualifications for redaction.

The company who was awarded the contract also gets the opportunity to redact any information they deem necessary, however the PEO STRI legal counsel has the ultimate say in what does and does not go into the public domain, as they are the Initial Denial Authority.

“Several media outlets were interested in the information surrounding disaster victims from the 2004 Florida hurricanes, specifically how much federal assistance they received and which counties they lived in,” said Guerzon, who worked nearly three years supporting the agency’s Florida Disaster Operations.

After her mission was complete, she became an intermittent disaster assistance employee and was awaiting her next assignment from FEMA. During that time, she was contacted by Stanley Associates, Inc., who asked her to interview for an open FOIA position at PEO STRI.

“And, the rest is history,” Guerzon said.