

(U.S. Army photo by SPC Alexis Harrison, 2nd Brigade Combat Team, 1st Cavalry Division Public Affairs.)

# Force Protection — Everyone's Responsibility

Christina A. Wright

**F**orce Protection (FP) is preventive measures taken to mitigate hostile actions against DOD personnel (including family members), resources, facilities, and critical information. An active FP program involving the Acquisition, Logistics, and Technology (AL&T) Workforce encompasses all aspects of protecting the force. The mission is to coordinate FP functions worldwide and perform oversight of antiterrorism, physical security, information assurance (IA), operations security (OPSEC), intelligence, and continuity of operations (COOP).



The U.S. Army Acquisition Support Center (USAASC), a direct reporting unit under the Assistant Secretary of the Army for AL&T, has the responsibility to implement an FP program for the center, 11 program executive offices (PEOs), and 2 direct reporting product managers (DRPMs). Each PEO and DRPM was tasked with appointing an FP officer to report to USAASC. In a short time, several big steps have been accomplished, including USAASC completing 100 percent of its antiterrorism level 1 training requirement.

The Army FP program includes daily practices most Soldiers and Department of the Army (DA) civilians conduct on a regular basis including keeping common access cards (CACs) secure, conducting daily inspections of safes containing classified or controlled items, and signing in visitors to the installation. Everyone can help minimize the threat by practicing staunch FP.

Antiterrorism is a well-known term that has come into wider use since the Sept. 11, 2001, terrorist attacks.

HQDA antiterrorism guidelines require annual level 1 training for all personnel. USAASC is generating and publishing tailored guidance for the AL&T Workforce, conducting training, and tracking and reporting to HQDA.

AL&T Workforce members can practice antiterrorism by being aware of

their surroundings and reporting suspicious activities or anything that's out of place to the appropriate authorities. Also, it's important to understand that random antiterrorism measures conducted at the gates and on the installation are not inconveniences — whether it means waiting extra time at the gate for an identification (ID) check or walking farther to enter the building — they are for everyone's safety and protection.

It's important to understand that random antiterrorism measures conducted at the gates and on the installation are not inconveniences — whether it means waiting extra time at the gate for an ID check or walking farther to enter the building — they are for everyone's safety and protection.

Physical security is probably the most widely practiced FP measure. It includes maintaining positive control of a unit's arms room, keeping CACs on hand at all times, and making sure visitors are always accompanied. When you enter a military installation, the guards check the car and conduct hands-on ID verification. These are physical security practices that are part of the installation's FP.

Safes are another form of physical security.

They have to be maintained at all times. A *Standard Form 702* must be initialed when the safe is opened and when it's secured. Also, Soldiers' charge of quarters duties help secure the barracks and ensure that there is no unauthorized activity.

To access installation computer systems, all personnel must take the



Using CAC certificates on each computer system is one step in securing personal information used on the global e-mailing system, file sharing, and other electronic communications. (U.S. Army photo by Richard Mattox.)

online IA course. This measure teaches anyone who has access to a computer on the installation how to keep information — one of the most important forms of intelligence — out of the hands of those who would misuse it. Using CAC certificates on each computer system is one step in securing personal information used on the global e-mailing system, file sharing, and other electronic communication.

IA is an OPSEC function dealing mainly with the intranet, Internet, and technology hardware and software. Under IA guidelines, outside computers cannot access the intranet because all users and computers are tracked and protected according to their authorization level. Each computer is assigned to a port that only works with that computer. Any changes must be made by the Directorate of Information Management.

According to *Army Regulation 25-2*, OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to defense acquisition, defense activities, military operations, and other activities to: (a) identify those actions that may be observed by adversary intelligence systems; (b) determine what indicators hostile intelligence



FP preventive measures require worldwide coordination. Here, a military police Soldier and her Iraqi interpreter input information into her computer for analysis in support of the theater's FP program. (U.S. Army photo.)

systems may obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and (c) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

In Iraq and Afghanistan, the threat is "just beyond the wall" and OPSEC is everyone's watch word. Every bag of trash is a hot commodity among the enemy and each unsecured communication is likely monitored, so a 100-percent shred policy is maintained to ensure snippets of information don't fall into the wrong hands. Mailing labels, junk mail, and phone rosters are shredded as

well. Every small bit of information can be gathered by the enemy to create a big picture and a possible security problem.

Shredding is one of the easiest ways to destroy sensitive information such as social security numbers, pay data, troop movements, supply shipments, and daily schedules. Destroying classified documents and information is a very important part of maintaining a strong FP program. IA guidelines authorize software for military computers and provide information on safeguarding against unauthorized users gaining access to military networks from outside sources.

Just as the enemy collects information on us, we collect information about

Just as the enemy collects information on us, we collect information about them. Intelligence is a big part of the FP program because it can be collected, analyzed, and developed to preempt major enemy threats or attacks.

them. Intelligence is a big part of the FP program because it can be collected, analyzed, and developed to preempt major enemy threats or attacks. USAASC collects intelligence from many different sources, including local law enforcement, HQDA, the Transportation Security Administration, and other agencies. The information is disseminated by USAASC to its lateral commands and to a threat working group that helps mitigate threats and prepares for possible incidents by raising the threat condition level.

COOP is the last part of the FP program. The COOP outlines organization operations when personnel are unable to get to normal work facilities. This requires extensive planning and organization to quickly set up alternate work sites, equipment, and network capabilities to minimize the disruption of the organization's work flow. Each unit is responsible for developing a plan and reporting to its headquarters. Ultimately, HQDA should have every unit's COOP on file in case of massive catastrophic events affecting a single unit or the entire Army.

The FP program, when implemented and maintained properly, is successful at protecting most military assets and deterring outside interference, malicious or otherwise. The goal is to be such a hard target to enemies and external forces that they move on to easier targets. Every Soldier, civilian, and contractor has the obligation and responsibility to uphold the FP guidelines.

**CHRISTINA A. WRIGHT** provides contract support to USAASC through BRTRC Technology Marketing Group. She is a U.S. Air Force Reserve Public Affairs Specialist and an honor graduate from the Defense Information School.