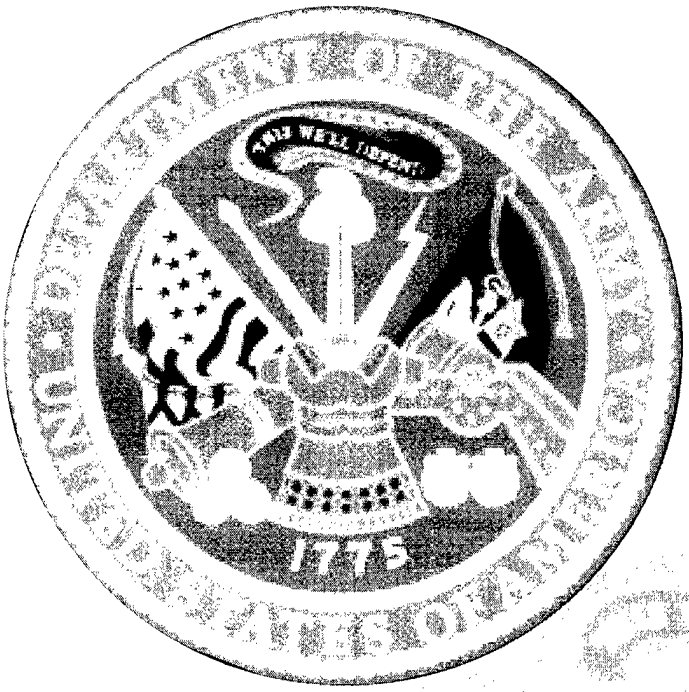
UNITED STATES ARMY

ANTITERRORISM & FORCE PROTECTION

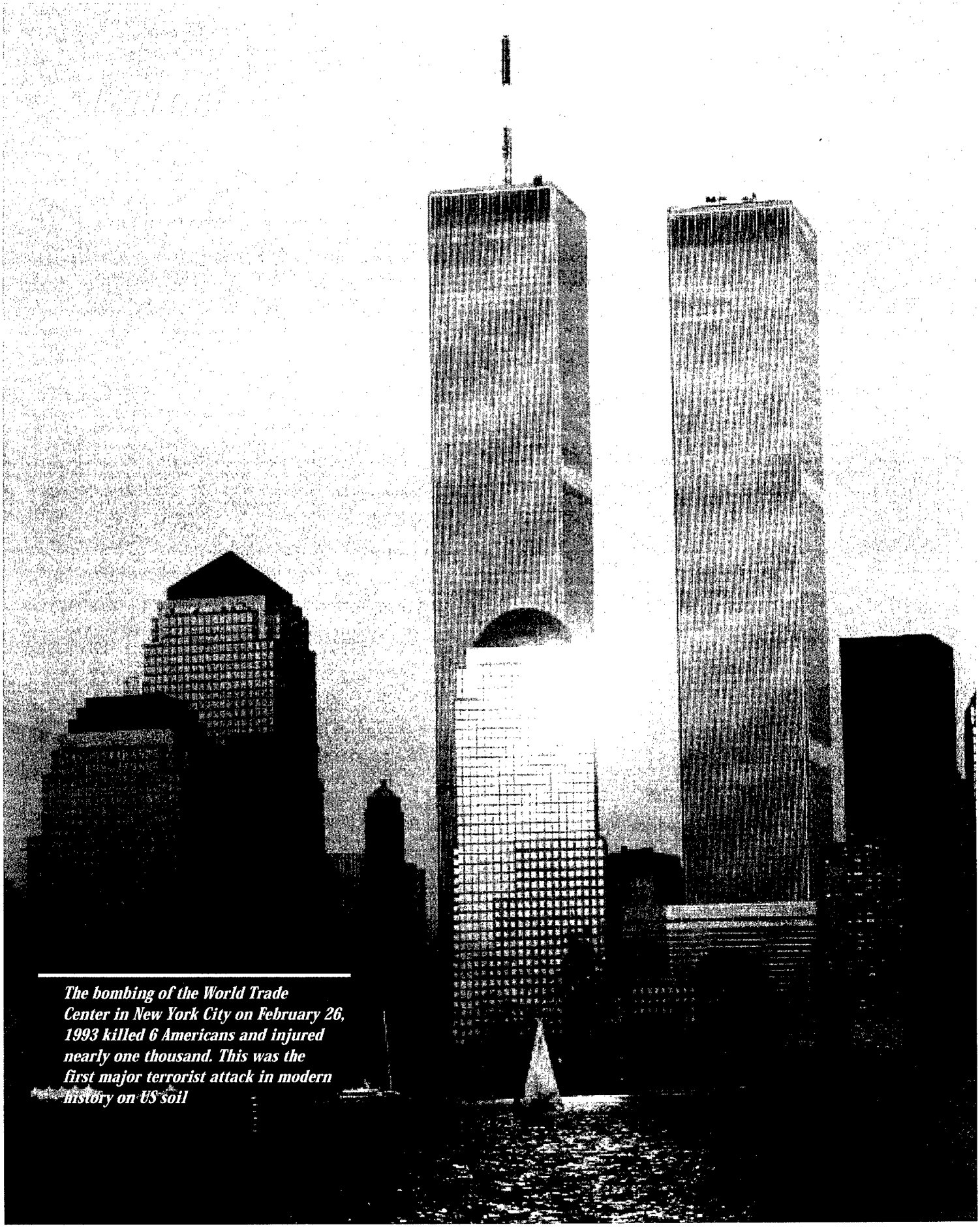


INSTALLATION COMMANDERS' GUIDE

20011018 061

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

AQU02-01-0040



The bombing of the World Trade Center in New York City on February 26, 1993 killed 6 Americans and injured nearly one thousand. This was the first major terrorist attack in modern history on US soil

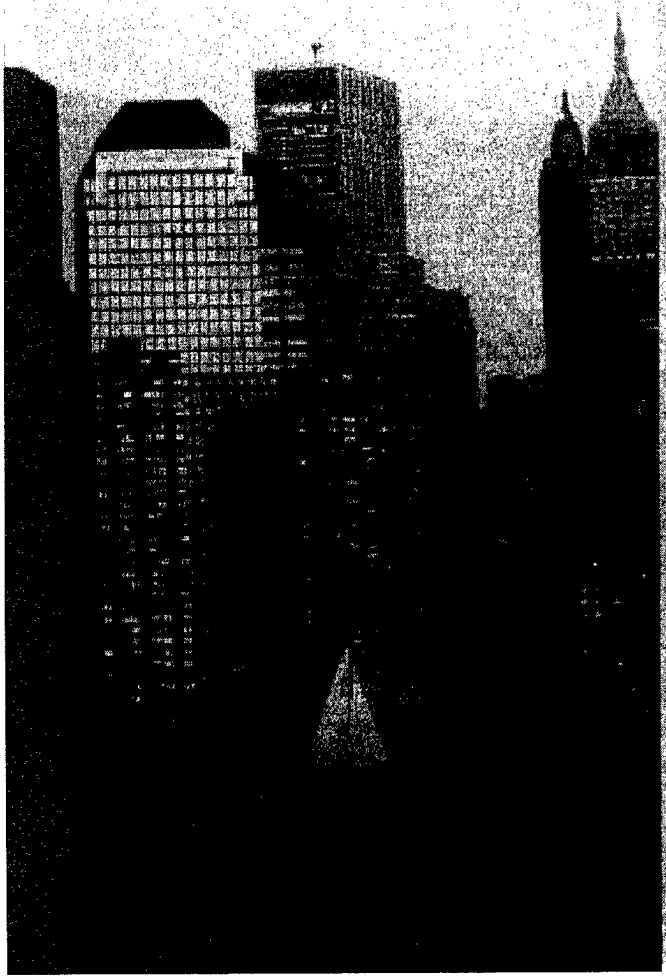


TABLE OF CONTENTS

Part I – Introduction 4

Part II – Antiterrorism Force Protection (AT/FP) Critical Tasks 5

- Commanders Take Personal Charge of their AT/FP Program 6
- Commanders Provide Intelligence Support 8
- Commanders Assess and Reduce Critical Vulnerabilities 10
- Commanders Increase AT/FP Awareness in Every Person– Soldier, DA Civilian and Family Member 13
- Commanders Must Exercise and Evaluate their AT/FP Plans, to Include WMD Planning 16
- Commanders Maintain Installation Defenses IAW Threat Conditions 17
- Commanders Create a Civil/Military Partnership for WMD Crisis Response 19
- Commanders Ensure WMD First Responder and Consequence Management Capabilities 22

Part III – Conclusion 24

ANNEX A – References and Sources for Assistance 25

This Installation Commanders' Guide on Antiterrorism and Force Protection provides timely and valuable direction to ensure our soldiers, property and military capabilities are properly protected. This initiative is extremely important given the ever present threat of terrorist attacks, and the need to protect our forces from becoming targets of opportunity to anyone who would harm our nation and our people. Acts of transnational and domestic terrorism have already struck here at home. Their devastation is no different that that of an attack by an armed enemy in battle. We must be prepared to defend against these threats *now* to ensure we are always mission capable.

It is my charge, therefore, that Installation Commanders rise to the challenge presented in this Guide. There are many actions that we can take on to respond to such incidents should they occur. This Guide identifies the most important actions for commanders to undertake.

This program will require a great amount of effort from our commanders, their staffs, and all Army personnel, including civilians and family members. However, the accomplishment of these tasks will assist immeasurably in the Army's ability to protect its people, critical resources and information from acts of terrorism. As we work to accomplish our missions in support of U.S. national securities interests, we must *succeed* in doing what is necessary to protect the homes, lives and property of the best Army in the world!

Louis Caldera
Secretary of the Army

"We must be prepared to defend against these threats *now* to ensure we are always mission capable."

IT IS NO USE SAYING,
"WE ARE DOING OUR BEST."
YOU HAVE GOT TO SUCCEED
IN DOING WHAT IS NECESSARY.

SIR WINSTON CHURCHILL

The U.S. Commission on National Security/21st Century concluded on a September 1999 report that America will become increasingly vulnerable to hostile attack at home, and that "Americans will likely die on American soil, possibly in large numbers." This is a sobering assessment of the era that we expect will last some number of years. Some of these attacks, if they occur, will most likely be carried out by terrorists.

The number of terrorist incidents has declined in the last several years, but the lethality of the attacks that have occurred has increased. The spread of technology and material needed for weapons of mass destruction (WMD) also increases the risk that terrorists or disaffected group may use WMD. Commanders must, as the law and available resources permit, act proactively to deter would-be attackers and establish procedures to enable effective response to save lives and contain damage if an attack does occur.

Traditionally, AT/FP programs have relied on physical security measures to deter and defend against possible attack. Use of such measures should certainly continue. But there is another dimension of antiterrorism: of actively using information technology and human expertise to gain an understanding of terrorist motives and operational patterns, and actively engaging in the environment in which terrorists may operate. Again, commanders must operate as bound by law and regulations when executing AT/FP programs but this cognitive dimension must be incorporated into installation programs.

Put the concepts in the Guide to real use to protect our soldiers, civilians, family members, and property, as well as the neighbors who live and work near our installations.

Eric K. Shinseki
General, United States Army
Chief of Staff

"THE TERRORIST THREAT TO THE U.S. MILITARY FORCES IS REAL...THIS THREAT CAN ONLY BE COUNTERED THROUGH THE CONCERTED EFFORTS AT ALL LEVELS TO PLAN, PREPARE, AND ENFORCE AT/FP MEASURES....IT WILL TAKE ENERGY, COMMAND ATTENTION, AND RESOURCES."

DOWNING REPORT ON THE KHOBAR TOWERS BOMBING, AUGUST 30, 1996

This Installation Commanders' Guide is intended to serve two major purposes. It explains to Installation Commanders the most important things they must do to enhance the AT/FP Program on their installations. More specifically, it disseminates these in the form of critical AT/FP tasks, to include key actions to accomplish these tasks. Secondly, this guide will serve as an information source and a reference where commanders can find assistance on specific aspects of AT/FP. For example, commanders can find information on training of personnel and sources that may be contacted for further assistance. In this sense, the guide should be a valuable reference tool.

Prior to a more detailed explanation of the critical AT/FP tasks promulgated here, it might be useful if commanders were provided a clear understanding of how these fit into the larger picture of AT/FP. Chart 1 depicts the Goal of AT/FP and the four major objectives of the U. S. Armed Forces with respect to terrorism. Chart 1 also depicts the spectrum of terrorist activities from pre-incident to post-incident. Most importantly, however, this chart provides a framework for understanding two major points. First, it portrays the relationship between AT/FP objectives and installation critical AT/FP tasks. Secondly, it vividly makes the point that AT/FP critical tasks are operative across the entire spectrum of terrorism, from pre-incident to post-incident. Nevertheless, notice how much effect the accomplishment of these tasks could have on deterrence alone. The next portion of this guide will focus upon these critical AT/FP tasks and how they relate to the Army's AT/FP Program.

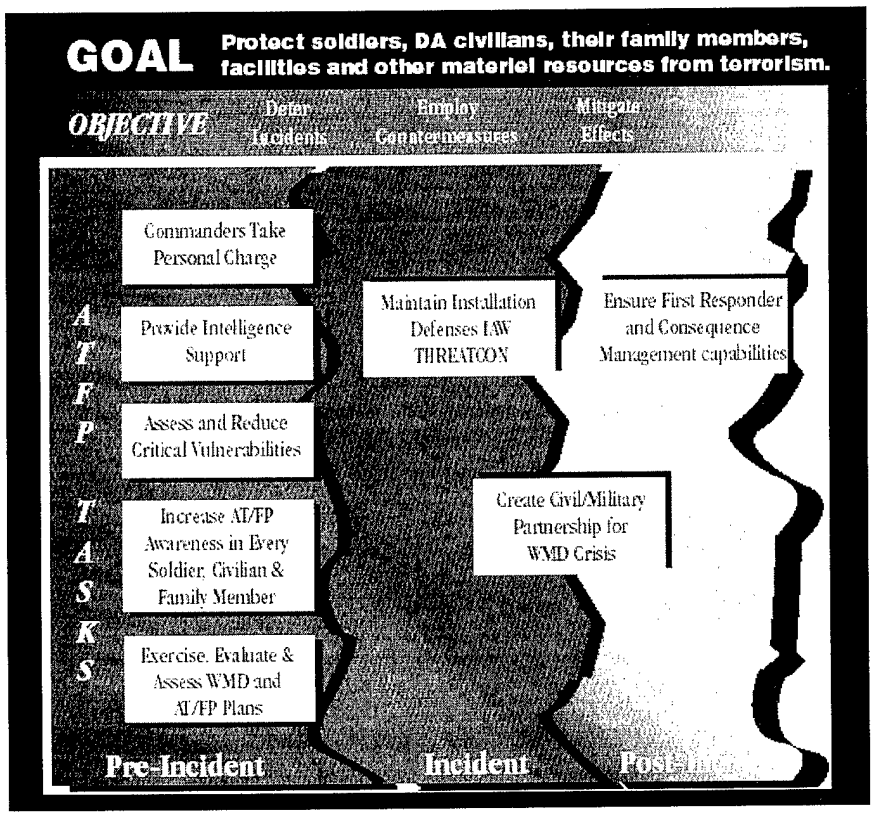


CHART 1

OVERVIEW

Chart 2 portrays the critical AT/FP tasks in relationship to the AT/FP Program as a whole. Near the center of the diagram, are the objects of the AT/FP security plan – personnel, critical resources, and information. Encircling these are programmatic elements of AT/FP (i.e. Personal Security, Physical Security, Information Operations, and Law Enforcement). The outer ring of boxes contains those critical tasks that Installation Commanders need to accomplish in order to enhance their AT/FP Programs. If these tasks are performed, the centerpiece of Chart 2 will contain AT/FP Plans that will be significantly more capable of protecting personnel, information and critical resources from attack; and if a terrorist incident should occur, these Plans would also better prepare our installations to respond to its consequences. Now let us focus on these very important tasks.

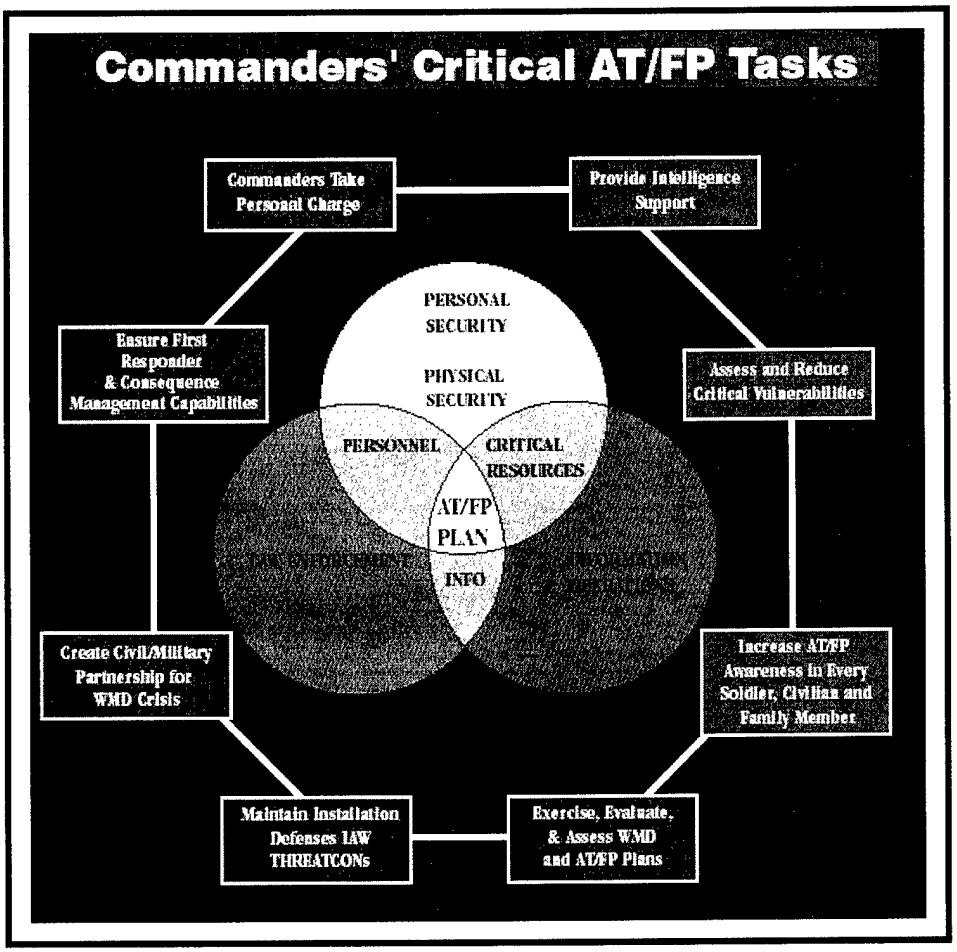


CHART 2

Commanders need to take personal charge of their antiterrorism force protection (AT/FP) program

As we all know, subordinates view as important what their leaders view as important. The major point that needs to be driven home here is that AT/FP is such an important responsibility that the commander should give the program his/her personal time and attention in order that the remainder of the command follow suit. Therefore, any actions the commander takes that reflect personal involvement in the AT/FP Program will send a clear message throughout the command. Specifically, there are a number of key actions that Installation Commanders should take to ensure that AT/FP becomes a commanders' program.

The Khobar Towers Bombing in Dhahran, Saudi Arabia on June 25, 1996 killed 19 Americans and injured over 500 other Americans.

- **GARRISON COMMANDERS CHAIR AT/FP COMMITTEE**

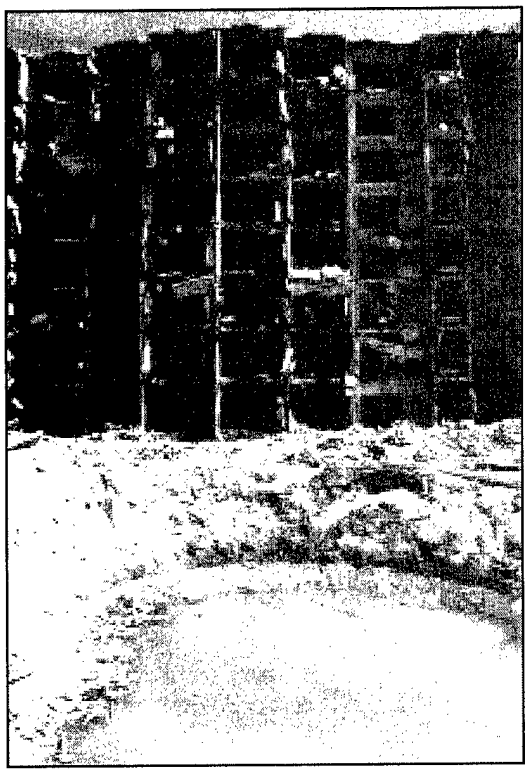
Garrison Commanders should personally chair the Installation AT/FP Committee. This will help accomplish a number of things. It will provide this body the high level attention, support, and direction that it requires to make it a viable entity. The AT/FP Committee must be the focal point for AT/FP planning on the installation and its importance cannot be exaggerated. This Committee should hold regularly scheduled meetings with an agenda focused on issues set by the commander or proposed by Committee members. On a regular basis, the AT/FP Committee should break into Working Groups with appropriate members and leadership to address specific projects assigned by the Committee, such as evaluating planned or programmed countermeasures. Given the number of times the full Committee will normally meet and its proper composition, discussed below, chairing the Committee should not be an onerous task for an already busy Garrison Commander.

• KEY INSTALLATION STAFF OFFICERS SERVE ON AT/FP COMMITTEE

There are two important actions, however, that must occur to ensure that Installation AT/FP Committees function as intended. First, key installation staff officers also must serve personally on the Committee. By this, we mean those officers who play a primary role in AT/FP planning and execution. Having key staff officers serve on the AT/FP Committee reinforces the high priority that the commander places on this Program. The Provost Marshal, Director of Logistics, Installation Resource Manager, Staff Judge Advocate, Director of Information Management, Installation Engineer, Medical Officer and Public Affairs Officer, at a minimum, should serve on an Installation AT/FP Committee. Commanders also should consider assigning other key personnel when present and appropriate, such as the installation Fire Chief to the Committee.

• IMPORTANCE OF FULL-TIME AT/FP OFFICER

A second critical component of the Installation AT/FP Committee, indeed of the AT/FP Program as a whole, concerns the existence and responsibilities of the Installation AT/FP Officer. Installation Commanders must designate an officer to serve as the Installation AT/FP Officer as his/her primary duty. This is necessary due to the scope and magnitude of the duties this officer must perform. An officer working AT/FP as a part-time duty will not be able to devote the time and effort needed for this important Program. This officer's responsibilities and required training are outlined in AR 525-13. Every effort should be made to provide as much continuity as possible in this critical position. The AT/FP officer should monitor the THREATCON status, receive the daily AT/FP Update from HQDA, and conduct the day to day operations and planning of the Installation AT/FP Committee. In this capacity, he/she should have ready access to the commander. In brief, the installation AT/FP Program is serious business and the role of the AT/FP Officer must be treated as a critical component of that Program.



On June 25, 1996, a terrorist truck bomb estimated to contain the equivalent of 3,000 to 8,000 pounds of TNT exploded outside the northern perimeter of Khobar Towers, Dhahran, Saudi Arabia. The water-filled crater shows the tremendous force of this size bomb.

• DEVELOP PLANS AND TRAIN FOR ALL ASPECTS OF AT/FP AND WMD INCIDENTS

Installation AT/FP plans must be updated regularly, based upon current threat and vulnerability assessments and should contain the basic physical security requirements IAW AR 190-13 (e.g., bomb threat, installation closure, WMD, etc.). As one can recall from Chart 1, the objectives of the AT/FP Program span the spectrum of terrorist attack. Therefore, commanders must ensure that installations develop plans and train for all aspects of Weapons of Mass Destruction (WMD) incidents and AT/FP, from pre-incident to post-incident phases. In developing and reviewing their AT/FP Programs, commanders should be certain that critical resources are identified, requested, reallocated, and provided. In cases where risks cannot be managed to acceptable levels, this situation should be raised to the next level in the chain of command for resolution.

Commanders provide intelligence support

• COLLECTION AND ANALYSIS OF THREAT INFORMATION

The first requirement that must be met in this critical task is the collection and analysis of threat information. For this to occur in a seamless manner, installations must have connectivity to all available intelligence sources. These should include support provided by military assets (CIDC and MI), and civilian intelligence and law enforcement authorities (local, state, and federal).

The bombing of the Alfred P. Murrah Federal Building in Oklahoma City on April 19, 1995 killed 168 Americans and injured hundreds more.

For example, INSCOM conducts foreign intelligence collection and counterintelligence (CI) activities for the Army and is responsible for notifying any affected installation upon receipt of time-sensitive threat information. The USACIDC collects, analyzes, and disseminates criminal information pertaining to threat activities and also has the responsibility to notify affected installations upon receipt of time-sensitive threat information. In addition, the Army Counterintelligence Center (ACIC) conducts liaison with national level analytical intelligence organizations to exchange information on all aspects of international terrorism and the threat it poses to the U.S. Army. Both the USACIDC and the ACIC provide threat information to the Antiterrorism Operations and Intelligence Cell (ATOIC) located at HQDA— (see Annex A for reference). Installation Commanders can derive maximum benefit from the ATOIC through the use of the daily ATOIC intelligence update. This message is widely distributed to all Army installations.

• DOMESTIC INTELLIGENCE COLLECTION

With respect to domestic intelligence, the FBI can be the most important conduit for installations in the development of local threat assessments and receipt of timely threat information. In late 1997, HQDA coordinated with the FBI to ensure that the latter's field offices share U.S. and foreign terrorist threat information with Army installations within their jurisdictions. Installation Commanders should make certain that this cooperative effort exists and is encouraged.

At the same time, commanders must be certain that any domestic intelligence activities are conducted IAW applicable Army regulations and DoD directives (i.e., AR 381-10, AR 380-13 and DoDD 5200.27). Use of MI assets is severely restricted in CONUS. If a commander has a question in this area he/she may refer to the HQDA DCSINT home page and review intelligence oversight (see Annex A). The Staff Judge Advocate is the commander's expert adviser in this extremely sensitive area. The Provost Marshal, who is the installation's liaison with outside law enforcement officials, must also be fully aware of these regulations and directives. As members of the AT/FP Committee, both of these officers, among others, will be contributing to the integration of an AT/FP system (Intelligence) on the installation's organization that can serve to synchronize its AT/FP efforts.

- **DISSEMINATION OF INTELLIGENCE**

The last point to be made on the subject of intelligence support is as important as the first. Some recent assessments of our intelligence efforts on installations indicate that we must improve our performance in disseminating intelligence products.

We can do a superb job of collecting and analyzing threat information; however, if we do not get that information into the hands of those who need it most, we have only accomplished half the task. Intelligence products should be disseminated to higher and lower headquarters, installation staff elements, contractors and tenant units continuously. Timely intelligence and useful analyses can contribute significantly to an installation's AT/FP Program.

"We must improve our performance in disseminating intelligence products."

On August 7, 1998, terrorist bombings of the U.S. Embassies in Nairobi, Kenya and Dar Es Salaam, Tanzania resulted in the deaths of over 220 persons and injured more than 4,000 people. 12 Americans and 40 Kenyan and Tanzanian USG employees were among those killed.

Commanders assess and reduce critical vulnerabilities

There is no doubt the Information Age and the world of high technology have significantly affected the tools and supporting systems of warfare. At no small expense, the Army has benefited greatly from this explosion in technology; and the future force will continue to take advantage of all that technology has to offer. In the fight against terrorism, however, we cannot always rely upon technology alone. Indeed, some of the Army's most important warfighting support systems are themselves terrorist targets. Our vulnerabilities, however, do not all fall into the categories of information systems and new technologies. Today we are an Army based upon a force projection strategy. Recognizing that we are not immune to terrorist attack at home, Installation Commanders must focus upon each of those critical vulnerabilities that can have a serious effect upon mission accomplishment.

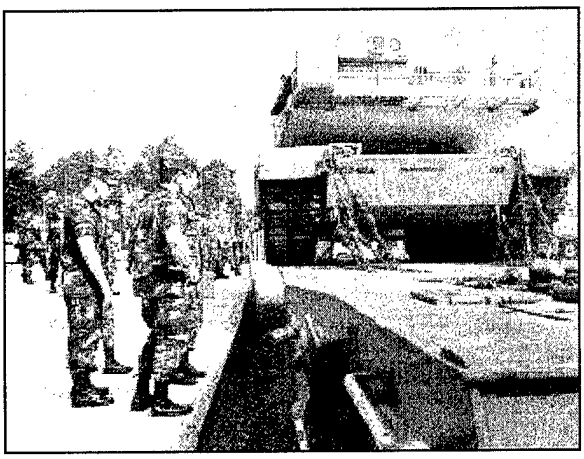
"60% of our network vulnerabilities are the result of human error"

• DEFEND COMPUTER NETWORKS

It is absolutely critical that we defend our computer networks from both internal and external threats. Unfortunately, 60% of our network vulnerabilities are the result of human error. We often find missing or weak passwords and personnel not properly trained. In addition, countermeasures are not installed and at times there is a lack of net discipline and operations security. This means that commanders need to emphasize their computer security awareness programs. We must do everything possible to provide the resources for computer network defense requirements. Make certain that security protection of software and hardware is installed and properly configured on our systems. Also, installations should respond to the Army's Computer Emergency Response Team (ACERT)—(see Annex A) when it issues countermeasure advisories. We also must eliminate unauthorized or excess computer connections. Entirely too many of the Army's computer-related problems in recent years have occurred as a result of such connections. In these cases, we are our own worst enemy. Lastly, in this highly technical field, commanders must make certain that personnel are properly trained and qualified for their positions. Take advantage of training courses for technical and administrative staffs offered through the Army's Directorate of Information Systems for Command, Control, Communications and Computers (DISC4)—(see Annex A).

• ASSESS VULNERABILITY OF INSTALLATION'S INFRASTRUCTURE

Returning to the subject of installations, when one considers possible terrorist capabilities, it is only prudent that commanders should assess the vulnerability of their installations' infrastructure systems. Water, electricity and/or gas supplies can be prime targets for terrorists. Each installation presents a unique situation and challenge when it comes to protecting these resources. Often the source of supply may not come under the control of the commander. It's possible, perhaps even likely, that the resource is provided by a local civilian entity. In such cases, the commander must assess vulnerabilities by coordinating with civilian proprietors, local officials and law enforcement personnel. This can be a difficult process and the Commander should use the expertise of his staff (e.g., PM, SJA, ENGR, PAO, etc.) to assist in evaluating specific conditions. Important questions will need to be addressed with these key civilians, as mutual concerns are discussed. For example, legitimate questions that might be raised in the case of a local civilian nuclear power plant may be what type of security exists at the facility and are there plans to increase that security should intelligence indicate a higher level threat than normal? If a truly effective civil/military partnership exists between the installation and the local communities, as the one prescribed later in this handbook, it will facilitate the commander's ability to address his concerns over the vulnerability of these critical life support resources.



• VULNERABILITY ASSESSMENT OF TRANSPORTATION SYSTEMS

Given the Army's mission to be prepared to project the force when required, Installation Commanders must also assess the vulnerability of transportation systems. This is no small task, since these include rail systems, roads (including bridges), airfields and seaports. Every installation with a requirement to deploy units must contend with at least one or more of these systems. Any of these can be a prime target for terrorists. The Army simply cannot allow their disruption to interfere with its mission. Reducing these critical vulnerabilities is an AT/FP responsibility.

Fortunately, there is an organization available to Installation Commanders that can assist in accomplishing the above tasks. The Joint Program Office for Special Technology Countermeasures (JPO-STC) is responsible for the oversight, management and execution of the DoD's Infrastructure Assurance Program (IAP). The mission of the IAP is to provide CINCs, military services, and DoD mission planners with a comprehensive infrastructure analysis capability to assess their dependencies and the potential impact on military operations, resulting from disruption of key infrastructure components. Specifically, the JPO-STC will focus upon energy, telecommunications and transportation systems. The JPO-STC's IAP process is based on site assessments and includes military installations, commercial ports, industrial facilities, and metropolitan areas. An IAP team can perform operational impact assessments across a wide variety of mission areas relative to an installation, to include force protection, installation readiness, force projection/mission planning, sustainment and mobilization. For more information on the JPO-STC see the reference at Annex A. Installation Commanders need to take advantage of this type of support.

• REQUIREMENTS IDENTIFICATION AND RESOURCING

In conducting the above assessments, commanders should ensure that critical requirements are identified, validated, prioritized and accomplished within their given resource levels. Having accomplished that, in those instances where commanders have identified requirements that cannot be met due to resource constraints, ensure the high priority unresourced requirements are identified, prioritized and prudently submitted to headquarters. The combination of command emphasis and staff involvement, to include functional experts with resource managers, provides a means to facilitate the funding of requirements. This is a serious and important responsibility. Among the many competing requirements leaders are faced with, there is no more important responsibility than the Force Protection Program. Ensure the priority given to force protection requirements is commensurate with the task. It is, however, a reality that everything cannot be funded immediately. Commanders must maintain the focus long term. By prioritizing all known requirements and developing objectives to achieve those requirements over a reasonable period of time (program years), a process is set in place that is feasible and safeguards our personnel, information and critical resources. At a minimum, requirements will be reviewed and updated during the periodic program review (AR 525-13, Standard 7). Commanders should use the available tools to assist in the articulation of requirements. The Joint Staff Integrated Vulnerability Assessments (JSIVA) conducted by the Defense Threat Reduction Agency (DTRA), DAIG Inspections, MACOM and installation assessments are all designed to support this effort.

"This is a serious and important responsibility... Commanders must maintain the focus long term."

Timely identification and submission of valid requirements during the Program Objective Memorandum (POM) build is essential to adequately and systematically resourcing your AT/FP needs.

In addition, the Army Staff is working on the development and implementation of an AT/FP Model that will allow installations to measure AT/FP posture in all associated AT/FP Tasks. This model will also be used to report the costs of AT/FP. The model is anticipated to be an AT/FP community asset, available on a classified web site and accessible throughout the year for management of resources and assessment of AT/FP strengths and weaknesses. Additionally, select information will be extracted for automatically updating Installation Status Report information on installations. Such cost/benefit measurements will have great utility at the installation, MACOM and DA levels. Some obvious applications for this information are: comparison and selection of acquisition alternatives, programming and budgeting of resources, development and refinement of AT/FP doctrine and risk management.

Combating terrorism is a DoD-wide effort. Specific requirements may also be funded through the Combating Terrorism Readiness Initiative Fund (CbT RIF). This fund is covered in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5261.01A. The purpose of the CbT RIF is to fund emergency or other unforeseen high-priority combating terrorism requirements. The fund provides a means for Army component commands via CINCs to react to unanticipated requirements from changes in terrorist threat levels or force protection doctrine/standards. It is not intended to subsidize ongoing projects or supplement budget shortfalls. CINCs may submit initiative requests from non-CINC aligned commands if the CINC has force protection responsibility or is enforcing additional force protection standards upon the non-CINC aligned commands.

Commanders increase AT/FP awareness in every person– soldier, DA civilian, and family member

• AT/FP AWARENESS TRAINING

AT/FP awareness is one of the most important elements of any AT/FP Program. We have seen evidence of how an alert and aware individual can thwart a terrorist incident; and unfortunately we have also seen the results of the failure of people to notice or report sightings of suspicious persons conducting surveillance of a future target. The lesson learned is clear. The more we can inculcate AT/FP awareness in all personnel, the stronger AT/FP Programs will become. The Department of Defense has mandated AT/FP training requirements for all military personnel, DoD civilians, and their family members under specific circumstances. The Army has provided implementing guidance to support these requirements in AR 525-13. Chart 3 provides an excellent summary of these requirements by noting who is to be trained, under what conditions and prescribes the minimum training standards.

The Regional CINCs' require that all DOD personnel–military, civilian, contractors, and family members–receive AT/FP awareness training prior to overseas travel. Commanders at all levels must coordinate their efforts in ensuring that all personnel receive the required training and that this training is properly documented. These pre-deployment and travel training requirements are an essential element of a viable AT/FP Program.

At a minimum, Installation Commanders should establish a three step procedure–TDY, leave and passes. These steps are as follows:

- Identify, conduct and document the training requirement;
- Use the documentation when initiating a request for travel;
- Ensure all documentation is verified prior to travel at current unit and repeat the procedure again upon travel completion at the gaining unit.

The 1986 terrorist bombing of the La Belle Disco in Germany killed 5 people, one of whom was an American soldier.

LEVEL	TARGET AUDIENCE	MINIMUM TRAINING STANDARD
LEVEL I– Individuals	(For All Threat Levels) Military and DoD Civilians prior to all travel and deployments outside the 50 United States, its territories, and possessions (to include Leave, Pass, or Temporary Duty). Family members prior to all travel outside the 50 United States, its territories, and possessions on official government orders and Permanent Change of Station travel.	Conducted within six months prior to travel: **Instruction by certified Level II instructor** using an approved USAMPS lesson plan, containing a minimum of the following subjects: • Individual & Unit Protective Measures • Hostage Survival Techniques • Terrorist Surveillance Detection • THREATCON Measures **Recent AOR update for area of travel** **View AT/FP Awareness Videos on:** • Individual Protective Measures • Terrorist Surveillance Detection • Hostage Survival Techniques **Receive AT/FP Awareness Handouts:** • JS Guide 5260, July 96 and DoD wallet card; or, a) GTA 19-4-3 (Individual Protective Measures), July 97 and GTA 21-3-11 (Army wallet card); or, b) CINC/HQDA approved equivalent
LEVEL II– AT/FP Officer	E-6 to 0-4 Military personnel or GS-5 and above DoD civilian employees certified to serve as the commander's AT/FP advisor and provide Level I instruction.	Attend TRADOC's designated training at the "Force Protection Unit Advisor Course" which contains a minimum of the following subjects: **Module A:** Conducting Level I Training: • Intro to Terrorism • Terrorism Operations • Individual & Unit Protective Measures • Hostage Survival Techniques • Terrorist Surveillance Detection **Module B:** AT/FP Unit Advisor Training: • Physical Security • Command Control Protect (C2P) • THREATCON Measures • Risk Analysis • Improvised Explosive Devices (IED)/CONPLANs • Threat Assessment
LEVEL III– Bn/Bde PCC students	0-5/0-6 commanders/selectees	"Implement the Army's Force Protection Program" • Taught in all branch PCCs, the Garrison Cdr Course and the General Officer Installation Cdr Course: Policy/Responsibilities/MOS Applications • View Sec Def/CJCS AT Awareness Video: TVT: "You May Be the Target"
LEVEL IV– Installation Cdrs: COL/Above	0-6 to 0-8 commanders/personnel and Senior Executive Service civilians responsible for AT/FP programs, policy, planning, and execution.	Executive level seminar providing pertinent briefings, current updates and panel discussions topics. Seminar concludes with a tabletop AT/FP wargame that facilitates interaction and discussion on power projection, WMD, THREATCON management, and implementation of AT/FP actions among participants.

Additionally, the documentation of the AT/FP training should be done on a Memorandum for Record (MFR) that would simply record the individual's name, rank (for soldiers), grade (for DA civilians), relationship (for family members), SSAN, specific training and country area briefing provided, and date training was conducted. The unit commander or the instructor who administered the training could sign this MFR, which would then be maintained in the unit/office training files. A copy of this MFR should accompany any subsequent requests for OCONUS leaves, passes, or TDY in conjunction with PCS orders. Supervisors and approval authorities should neither recommend nor approve such requests without this proper MFR documentation. Implementation of the above procedures would mean a marked improvement in the Army's AT/FP awareness posture.

"Leader training for the command's AT/FP Program requires particular attention."

- **LEADER AT/FP TRAINING**

Leader training for the command's AT/FP Program requires particular attention. Recent experiences indicate that a number of installation AT/FP Officers have not received certified training or a limited exception IAW AR 525-13. As a start, the AT/FP Officer must attend certified training IAW AR 525-13. Our standard must be that he/she is properly trained for the job! Requirements for this training need to be forecasted to MACOMs. The U.S. Army Military Police School conducts resident training for AT/FP Officers in "The Force Protection Unit Advisor's Course." In the past, Mobile Training Teams (MTTs) have also been utilized to meet this requirement. Installation Commanders should contact their MACOMs and the Military Police School for further information on this specific training. (see Annex A)

"Commanders should take every opportunity to reinforce AT/FP awareness as a means of inculcating a force protection mentality throughout their installations."

Attendance at the AT/FP Executive Seminars for O-6 to O-8 commanders/personnel is based upon a nominative process. These two and a half-day seminars consist of 70 to 90 personnel collectively from all of the Services and the CINCs. Each Service (CONUS) and CINC normally receive seven allocations per seminar. The AT/FP Branch in DAMO-ODL, HQDA, ODCSOPS is responsible for soliciting, scheduling and tracking CONUS Army attendees. Requests for nominations are transmitted to the field using the Army Message Handling System and are addressed to all Army activities. CONUS MACOM AT/FP offices should review, approve and consolidate all requests for their respective MACOMs. OCONUS Army units will submit their requests through the appropriate MACOM to their unified command IAW the CINC's policy.

- **USE OF COMMAND INFORMATION PROGRAM TO ADDRESS AT/FP AWARENESS**

In addition to formal training requirements, commanders should utilize their Command Information Programs through their Public Affairs Offices to the maximum extent possible to address AT/FP awareness issues. Commanders can use television programs, post electronic bulletin boards, newspaper articles and posters placed in high pedestrian traffic areas such as Post Exchanges and Commissaries, to get the AT/FP message across to as many people as possible. In order to be most effective, the AT/FP Information Program should be appropriately tailored to the audience, i.e. soldiers, family members, DA civilians and contractors. For example, AT/FP information provided to contractors should caution them to be personally knowledgeable and aware of any vehicles that may be supplying them with sub-contracted materials. These often-overlooked programs provide excellent opportunities to remind personnel of the need for continuous vigilance of suspicious activities and to explain the important roles they must play in the AT/FP effort. In short, commanders should take every opportunity to reinforce AT/FP awareness as a means of inculcating a force protection mentality throughout their installations.

Commanders must exercise and evaluate their AT/FP plans to include WMD planning

• ANNUAL AT/FP EXERCISE PROGRAM

Commanders must institute an annual AT/FP exercise program that tests the installation's capability to respond to the entire spectrum of AT/FP threats, including WMD incidents. This will help ensure that the installation Emergency Operations Center (EOC) can serve as the command, control and communications center for response to WMD incidents. In their AT/FP Plans, Installation Commanders should plan for various WMD scenarios, to include mass casualty decontamination procedures. These latter scenarios perhaps represent the most serious threat, since they will likely stretch an installation's resources and response capabilities to their maximum. If AT/FP exercises are to be truly realistic, they must include the participation of local, state and federal agencies to the greatest extent possible. Just as our Army "trains as we would fight," in this case, it is important that we exercise our AT/FP Plans as they would be executed in an actual terrorist incident. More guidance on this subject will follow in a subsequent critical AT/FP task.

Commanders should establish an effective evaluation process for their AT/FP exercises. In addition, AARs need to be conducted upon completion of exercises and feedback should be provided to the Installation AT/FP Committee. This will allow the latter to set about revising plans and procedures wherever necessary.

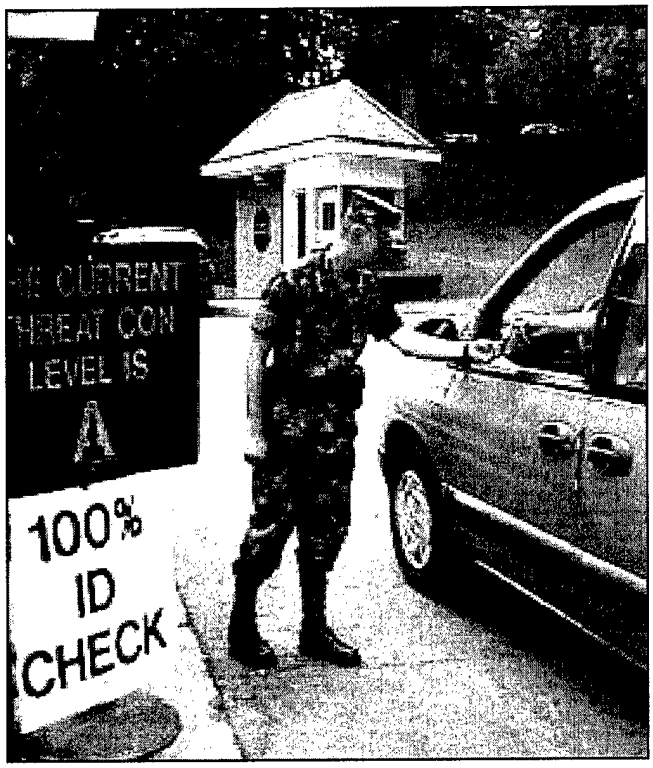
• PRE-EXERCISE TRAINING

While it is absolutely necessary to exercise all aspects of an installation's plans, there are techniques that can be used to "train-up," so to speak, to the level of complete, installation-wide exercises. For example, conducting a Table Top Exercise (TTX) with key personnel can serve as an excellent way to build towards an exercise including all participants in the AT/FP Plan. One way to view such a TTX is similar to a CPX with a WMD scenario. A minimum number of controllers would be necessary to input the scenario's moves. Participants would be the commander, his key staff and leaders who play a primary role in the installation's AT/FP Plans and their civilian partnership counterparts. The conduct of the exercise mainly consists of the various staffs, agencies and organizations coordinating their actions and reactions to each move of the scenario, face to face with one another. The TTX can be easily set up in a gymnasium or officer/NCO club ballroom, for example. The major purpose of the exercise is to gather the key AT/FP players together and identify any problem areas that require attention before AT/FP Plans must be executed as a reaction to an actual WMD incident. This latter technique has been used as part of the National Domestic Preparedness Program, initiated in 1996, with the Army as the executive agent conducting train-the-trainer programs for 120 cities in the United States. Installation Commanders can get more information on these types of exercises, as they relate to WMD incidents, by contacting HQDA, DAMO-ODS (see Annex A).

Commanders maintain installation defenses IAW threat conditions

- **THREATCON AND RANDOM ANTITERRORISM MEASURES PROGRAM (RAMP)**

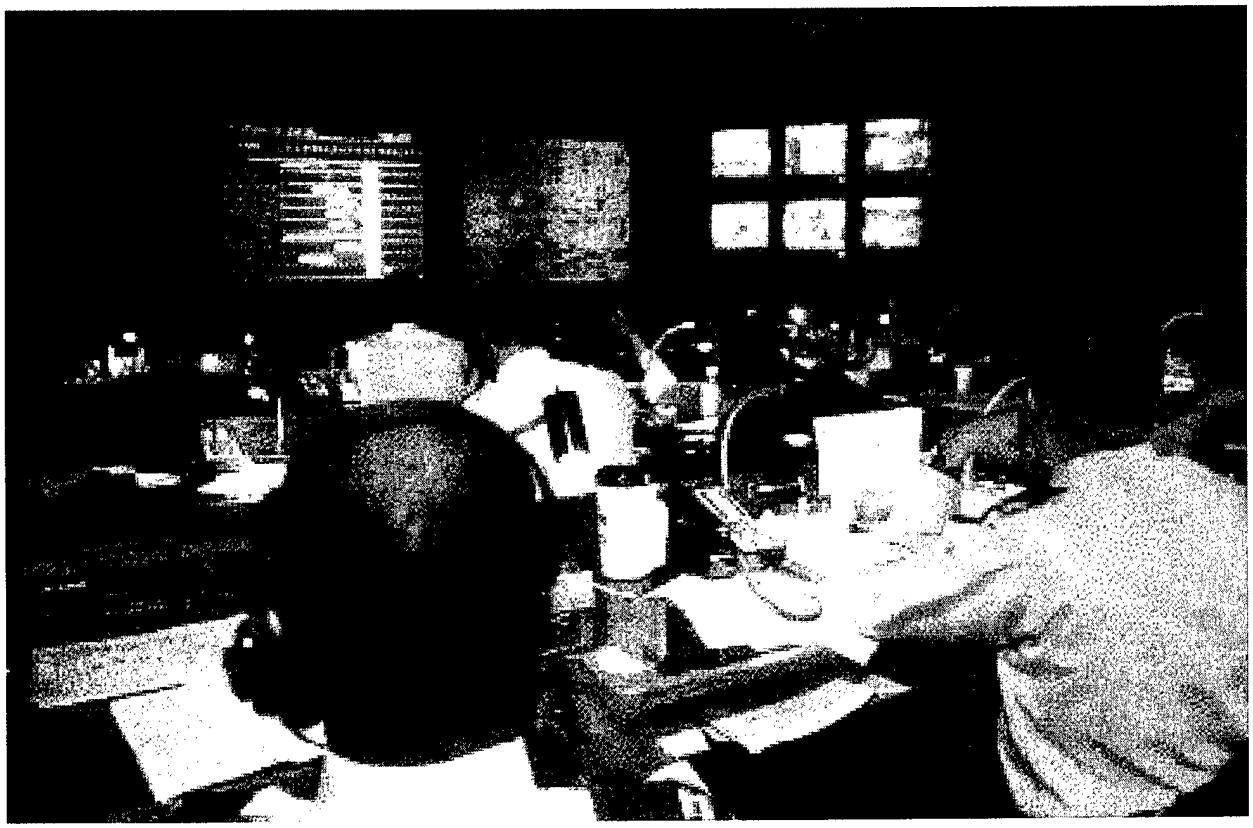
It is imperative that installations be prepared to increase their force protection posture IAW higher headquarters' directives or local threat information. In conjunction with the existing Threat Condition (THREATCON), commanders must implement a Random Antiterrorism Measures Program (RAMP) to help thwart terrorists from gathering intelligence on an installation. By implementing multiple security measures in a random manner and changing the appearance of an installation's security program, the commander can introduce a valuable element of unpredictability that will complicate terrorists' surveillance attempts. DoD Handbook O-2000.12-H, Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence, contains an excellent illustrative matrix on RAMP Implementation that commanders will find very useful as a planning tool (see Annex A). In addition, commanders' AT/FP Programs should plan to sustain THREATCON BRAVO, as detailed in AR 525-13, for a period of several weeks.



" RAMP introduces an element of unpredictability in security programs and deters terrorist attacks by varying routine and being sensitive to changes in the security atmosphere."

• INFORMATION OPERATIONS CONDITION PROCEDURES (INFOCON)

In an effort to employ additional countermeasures and further protect information resources, DoD has mandated the development of worldwide Information Operations Conditions (INFOCON) procedures. INFOCON recommends actions to uniformly heighten or reduce defensive posture, defend against computer networks attacks and to mitigate sustained damage to information and information infrastructure, including computer and telecommunication networks and systems. The INFOCON system presents a structured, coordinated approach to react to and defend against adversarial attacks on Army computers and telecommunications. The system applies DoD-wide in peacetime, conflict and war. Commanders are authorized to heighten or reduce INFOCON levels based on INFOCON security criteria, established by the program. INFOCON are based on three broad categories: operational, technical and intelligence (foreign and law enforcement). INFOCON levels should be commensurate with the risk. Over-aggressive INFOCON changes may impact system performance and communication abilities which could contribute to an adversary's objectives. MACOMs will provide INFOCON implementing instructions for their installations. Commanders should devote the kind of attention to INFOCON procedures as they do to THREATCON. For more information on this initiative, commanders can contact HQDA, DAMO-ODI (see Annex A).



Commanders Create a civil/military partnership for WMD crisis response

Presidential Decision Directives #39 and #62 assign responsibilities for terrorism response. As depicted in Chart 4, the FBI has the overall lead and is responsible for crisis management (capturing the terrorists, prosecuting them, and rendering safe any material.) FEMA is responsible for coordinating federal consequence management support for the state and local government (taking care of the people and facilities threatened or damaged by the attack.) DoD supports both the FBI and FEMA. Military commanders must be prepared to work with civilian responders to meet critical needs of the people affected by the attack. This concept of mutual aid is essential to meet potentially overwhelming requirements.

"Military commanders must be prepared to work with civilian responders to meet critical needs of the people affected by the attack"

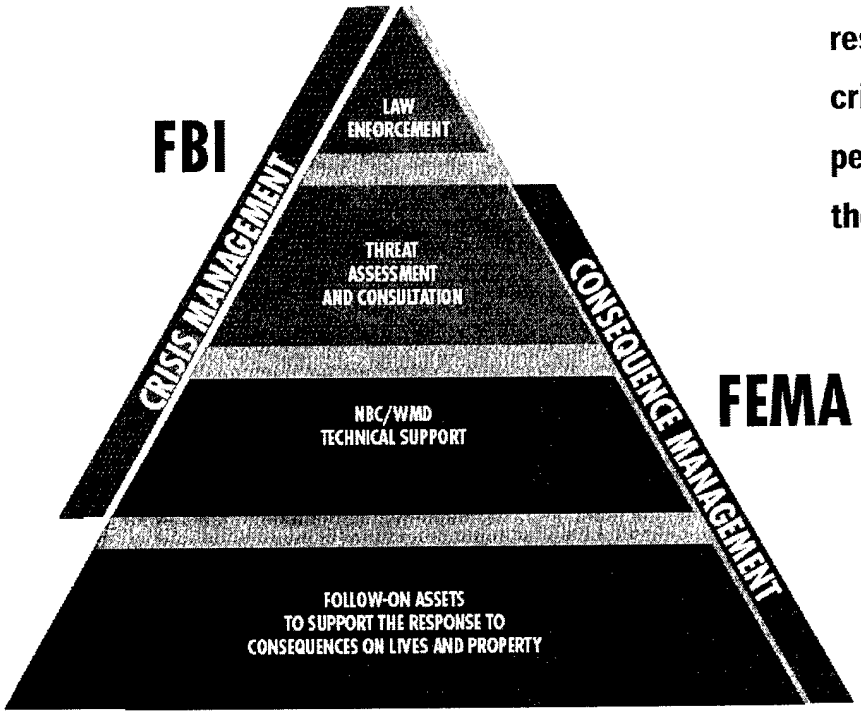


CHART 4

• THE NEED FOR CIVIL/MILITARY PARTNERSHIP AND THE BASIS FOR ITS CREATION

Some aspects of this topic have been alluded to previously; however, this task is of such importance to our AT/FP Programs that it is absolutely critical. Installation Commanders must get serious about this mission immediately. It is a fact that, depending upon their sizes, our CONUS Army installations are very similar to towns and cities. All of them have similar WMD vulnerabilities and all have similar WMD response capabilities. In addition, they all contain the primary target of WMD terrorism–people. It is also a fact that no single town or city, nor any single military installation possesses sufficient resources of its own to respond adequately to a WMD incident. This is why it is absolutely necessary for Installation Commanders to develop a civil/military partnership with their surrounding communities for WMD crisis response. J-34 has developed an AT/FP Installation Planning Template that contains a detailed WMD Appendix. This WMD Appendix addresses installation level planning and response for terrorist WMD incidents and commanders will find it a very useful tool. A copy of both documents can be found on the J-34 unclassified homepage (see Annex A).

An effective civil/military partnership will allow installations and communities to coordinate in advance both shared and exclusive resources, such as fire and rescue, law enforcement and medical capabilities. Creating the legal basis for such cooperation is achieved by negotiating and implementing memoranda of agreement (implying financial obligations) or memoranda of understanding (implying non-financial obligations). The senior leaders of both sides should negotiate the specific terms of a civil/military partnership. The Installation or Garrison Commander should represent the military, accompanied by the Staff Judge Advocate. The City Attorney will normally accompany local civilian leadership. There are good reasons for having this partnership committed to memoranda, not the least of which is that it will help to survive the test of time due to personnel turnover. In addition, such written documents facilitate the preparation and execution of plans much better than oral agreements or understandings could possibly hope to achieve.

"It is absolutely necessary for Installation Commanders to develop a civil/military partnership with their surrounding communities for WMD crisis response."

It makes sense, whenever possible, to include key counterparts of the civilian community in the work of the Installation AT/FP Committee. This may help facilitate coordination of a multitude of activities and foster a true spirit of partnership in the common defense against terrorism. For example, inclusion of local fire chiefs and senior law enforcement officials, not to mention hospital administrators, could be of immense benefit to the Committee's planning.

• CRITICAL IMPORTANCE OF INCLUDING CIVILIAN ENTITIES IN AT/FP EXERCISES

Earlier, in discussing installation AT/FP exercises, the importance of local, state and federal participation was mentioned. This needs to be stated even more emphatically and the rationale explained more fully. It is not just important that these entities participate in installation exercises; it is absolutely critical. Federal law mandates certain aspects of responses to WMD incidents and the civil/military partnership described above must be exercised if it is to be successful. While fire, rescue, law enforcement and medical personnel regularly train in their respective areas of expertise that could be relevant to a WMD crisis, joint civil/military exercises would greatly assist in ensuring that other important activities are coordinated effectively, such as public affairs. In addition, exercises will help senior leaders to learn how to manage more efficiently limited resources, by eliminating duplication of equipment and by multiplying response effectiveness through cooperation and communication.

Commanders must clearly understand the Incident Command System (ICS) which is mandated by Federal law for WMD response. If this is not done, some critical misunderstandings may exist even before a crisis occurs. Therefore commanders should familiarize themselves with the concept and the terminology of the ICS to fulfill their partnership obligations, while preserving military command responsibilities. Commanders are encouraged to read the materials on the Incident Command System that have been made available by the Federal Emergency Management Administration (FEMA) on the Internet. (see Annex A)

"Commanders must clearly understand the Incident Command System (ICS) which is mandated by Federal law for WMD response."

Commanders ensure WMD first responder and consequence management capabilities

• ENSURE EXTERNAL INTEROPERABLE PROCEDURES AND ESTABLISH INTERAGENCY COMMUNICATIONS

Recognizing that response to a WMD incident and consequence management will become a joint military and civilian effort, commanders must ensure that prior to any such occurrence, externally interoperable procedures are understood and have been exercised; secondly there must an ability to establish interagency communications. This latter point does not mean that installations must purchase an expensive array of communication systems in an attempt to match the variety of systems that their civilian counterparts and other federal agencies may possess. In some cases, the solution to establishing interagency communications may be found in the exchange of Liaison Officers with vehicles and radios. Perhaps communications through computer links will be the answer. Nevertheless, time is of the essence in such a crisis; and communication plans must be made and exercised in advance.

• ASSESS FIRST RESPONDER TRAINING

One of the most important concerns facing Installation Commanders today should be the status of their First Responders' capabilities. These fire and rescue, police and emergency medical personnel are the individuals we must rely upon to react immediately in a WMD incident to perform casualty triage, decontamination, emergency medical treatment, evacuation and tracking, site security, evidence preservation and contamination control measures. Therefore, commanders do need to assess the current status of their installations' First Responders' capabilities, in terms of equipment and training. One possible way to do this would be to take advantage of any partnership program with civilian communities by identifying civilian expertise that could be of assistance in assessing/training installation First Responders. Conducting exercises, even on a limited scale, is another excellent self-assessment tool. At this point, however, the most important question that Installation Commanders undoubtedly ask is, "How can I best access training for First Responders?"

"Commanders do need to assess the current status of their installations' First Responders' capabilities in terms of equipment and training."

• FIRST RESPONDER TRAINING

One source of First Responder training is to take advantage of opportunities provided by participating in the nation's Domestic Preparedness Program (DPP). The Defense Against Weapons of Mass Destruction (WMD) Act of 1996 authorized Federal resources to provide training and technical assistance to enhance state and local preparedness for terrorist incidents involving WMD. The Department of Defense became the initial lead Federal agency for the DPP. As such, DoD designated the Department of the Army as the Executive Agency to conduct train-the-trainer training for civilian First Responders in 120 cities in the United States. Training materials subsequently available through this program are an excellent resource for military installation's train-the-trainer training in WMD. Commanders and First Responders from military installations have been welcome to attend this training when it is near their installations and arrangements have been made through proper channels. This program is expected to continue for the foreseeable future and installations seeking more information should contact HQDA, (DAMO-ODS)—(see Annex A).

Other sources for First Responder training are also available. FEMA has set up an excellent program for First Responder training that is available free through the Internet (see Annex A). FEMA will work with commander's First Responders to create WMD training scenarios for installations. A portion of the FEMA program provides tested courses that can be taken individually or by a group via the Internet. Those who pass receive a certificate. In addition, the U.S. Army Soldier Biological and Chemical Command (SBCCOM) maintains an exhaustive list of WMD courses for Commanders, First Responders and other technical personnel. Detailed information on these courses, to include course descriptions can be found on the SBCCOM website (see Annex A). Commanders need to take advantage of the training opportunities noted above to make certain that First Responders are prepared to deal with the unthinkable.

It is not a matter of IF, rather, it is a question of WHEN...

The importance of accomplishing the tasks set forth in this guide cannot be overstated. Their accomplishment will not be easy and it will require the combined efforts of the entire Army Team. The stakes are high, however, and we must not fail to meet the challenge posed by terrorism. No doubt there are many demands placed on commanders' time and resources. As always, commanders will be required to make difficult decisions on priorities in their AT/FP Programs, based upon the threat and vulnerability analyses on their installations. Undoubtedly there are many things that can be done to improve installations' AT/FP posture. However, the guidance provided in this document represents the most important things that commanders must do to enhance AT/FP Programs on their installations. Doing less would put our personnel, critical resources and vital warfighting information assets at greater risk to terrorists' attacks.

"The guidance provided in this document represents the most important things that commanders must do to enhance AT/FP Programs on their installations."

Army Operations Center, June 8, 1999

"ANTITERRORISM FORCE PROTECTION IS CLEARLY EVERY COMMANDERS CHARGE.

THIS INSTALLATION COMMANDERS' GUIDE PROVIDES A SUPERB FOUNDATION FOR COMMANDERS TO BUILD ROBUST, VIABLE, AND REALISTIC AT/FP PROGRAMS THAT CAN PROTECT OUR FORCES, INFORMATION, AND INFRASTRUCTURE."

WAYNE DOWNING
GENERAL, USA (RET)

AR 525-13 — Antiterrorism Force Protection (AT/FP: Security of Personnel, Information and Critical Resources

This regulation prescribes Army policy and procedures and assigns responsibilities for the AT/FP Program. It contains a detailed list of other Army regulations and publications relevant to AT/FP. Additionally, it cites applicable DoD and JCS publications. The Army proponent for this regulation is DAMO-ODL-FP.

- Tel Com: (703) 695-8491/92
- DSN: 225-8491/92
- AT/FP Homepage: http://www.hqda-aoc.army.pentagon.mil/Odl/ATFP.html

AR 190-13 – The Army Physical Security Program

AR 381-10 – U S Army Intelligence Activities

AR 380-13 – Acquisition and Storage of Information Concerning Nonaffiliated Persons and Organizations

DoD Handbook 0-2000.12-H – Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence

DoDD 5200.27 – Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense

INTELLIGENCE SYSTEMS

Antiterrorism Operations & Intelligence Cell (ATOIC)
Tel Com: (703) 695-5300
DSN: 225-5300

Federal Bureau of Investigation: http://www.fbi.gov/

Intelligence Community Link: www.odci.gov/ic/icagen2.htm

ODCSINT- Office of the Deputy Chief of Staff for Intelligence: www.dami.army.pentagon.mil

INFORMATION SYSTEMS

Army Computer Emergency Response Team (ACERT)
http://www.acert.belvoir.army.mil/

DISC4 Training
Tel Com: (703) 607-5890

INFOCON Procedures
HQDA, DAMO-ODI
Tel Com: (703) 697-1119
DSN: 227-1119

CRITICAL INFRASTRUCTURE ASSETS

Joint Program Office for Special Technology Countermeasures (JPO-STC)
Tel Com: (540) 653-8730

AT/FP AWARENESS TRAINING

U.S. Army Military Police School
Tel Com: (573) 596-0131 ext. 62036

DOMESTIC PREPAREDNESS BRANCH

HQDA, DAMO-ODS (Nunn Lugar Branch)
Tel Com: (703) 695-4110 or (703) 614-1488/9458
DSN: 225-4110

CIVIL/MILITARY PARTNERSHIP FOR WMD CRISES RESPONSE

FEMA–Incident Command System: http://www.fema.gov/EMI
J-34 WMD Appendix
J-34 Homepage: www.dtic.mil/jcs/force_protection

FIRST RESPONDER TRAINING

HQDA, DAMO-ODS
Tel Com: (703) 695-4110
DSN: 225-4110

FEMA: http://www.fema.gov/EMI

U. S. Army Soldier Biological and Chemical Defense Command (SBCCOM):
http://www.sbccom.apgea.army.mil/

DEPARTMENT OF THE ARMY
UNITED STATES OF AMERICA
1775

INTERNET DOCUMENT INFORMATION FORM

A . Report Title : United States Army Antiterrorism and Force Protection : Installation Commanders Guide

Downloaded From the Internet 16 October 2001

C. Report's Point of Contact: Department of the Army Deputy Chief of Staff for Operations and Plans Pentagon Wash DC 20301

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials:__JC_ ____**Preparation Date**: 2001/10/17

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.