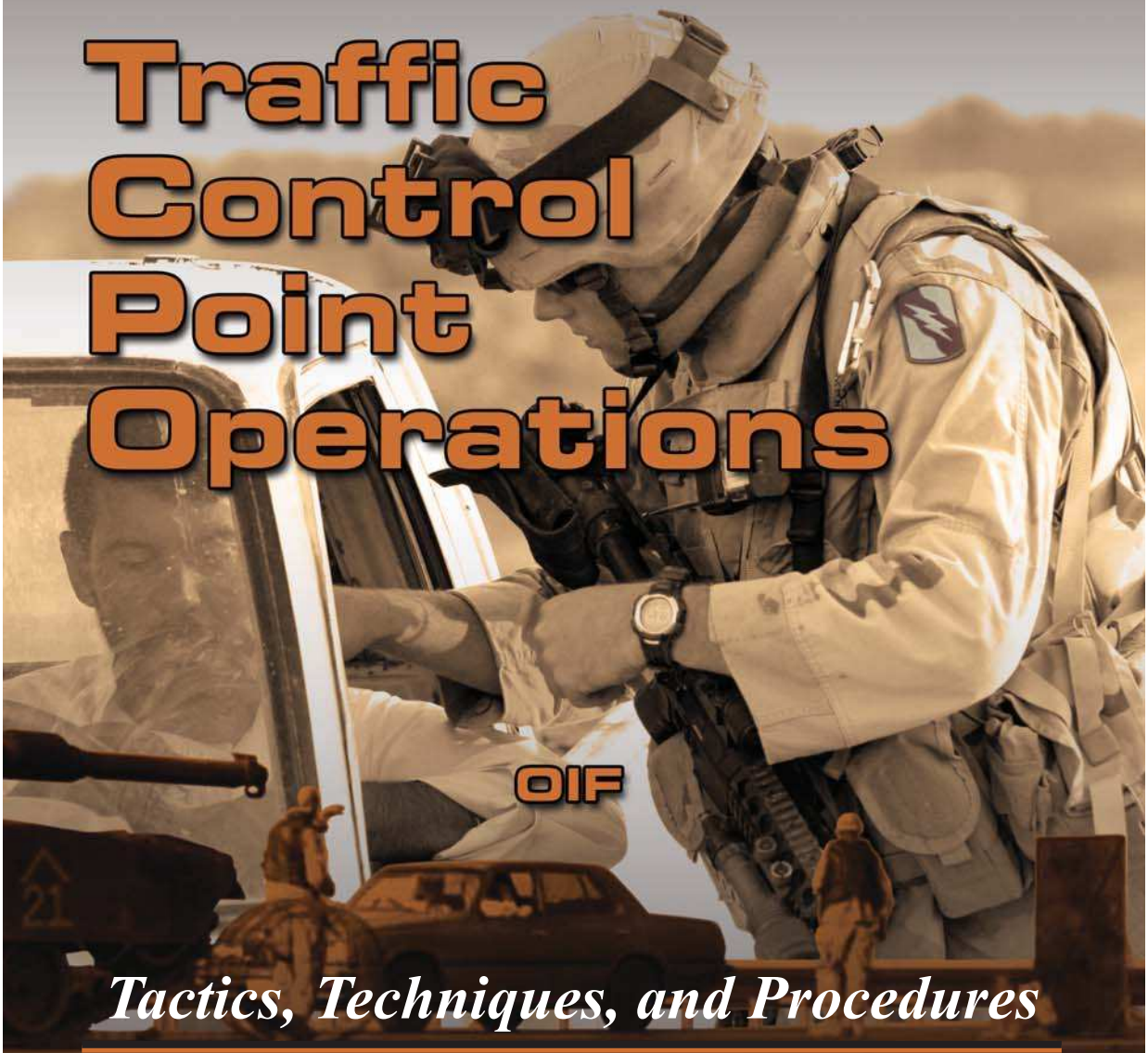
HANDBOOK

No. 06-15 Apr 06

Traffic Control Point Operations



Tactics, Techniques, and Procedures

Center for Army Lessons Learned (CALL)
Fort Leavenworth, KS 66027-1350

FOR OFFICIAL USE ONLY

Foreword

This handbook examines the essential role that traffic control points (TCPs) play in ongoing operations in Iraq today. TCPs are a critical control measure supporting a unit's overall force protection, movement control, and information operations. All established TCPs must meet stringent force protection requirements, accomplish the mission, and minimize chances for collateral damage against other coalition forces and friendly Iraqi citizens. Soldiers must balance these requirements, while simultaneously maintaining an ability to effectively communicate and interact with the sheer volume of traffic.

The Iraqi operational environment is complex and often ambiguous. Reports from theater clearly validate that leader decisions and Soldier actions at TCPs can have both short and long term effects. They may also have strategic and international repercussions. This handbook will discuss theater proven tactics, techniques, and procedures (TTP) to mitigate these challenges in order to conduct successful TCP operations and provides examples of current battle drills and recommended equipment checklists. These TTP, battle drills, and checklists are based on lessons learned by units in theater as they establish and equip TCPs and react to TCP incidents throughout Iraq.

The purpose of this handbook is to provide Soldiers and leaders a guide to employing effective and timely escalation of force policies within the rules of engagement, while limiting collateral damage and maintaining force protection.

Lawrence H Saul

LAWRENCE H. SAUL
COL, FA
Director, Center for Army Lessons Learned

Traffic Control Point Handbook

Table of Contents

Center for Army Lessons Learned

Director	**Colonel Lawrence H. Saul**
Managing Editor	**George J. Mordica II**
CALL Analysts	**Ralph Nichols** **Keith Warman** **Scott Blaney**
Editor	**Valerie Tystad**
Graphic Artist	**Mark Osterholm**

The Secretary of the Army has determined that the publication of this periodical is necessary in the transaction of the public business as required by law of the Department. Use of funds for printing this publication has been approved by Commander, U.S. Army Training and Doctrine Command, 1985, IAW AR 25-30.

Unless otherwise stated, whenever the masculine or feminine gender is used, both are intended.

Note: Any publications referenced in this newsletter (other than the CALL newsletters), such as ARs, FMs, and TMs, must be obtained through your pinpoint distribution system.

This information was deemed of immediate value to forces engaged in the Global War on Terrorism and should not be necessarily construed as approved Army policy or doctrine.

This information is furnished with the understanding that it is to be used for defense purposes only, that it is to be afforded essentially the same degree of security protection as such information is afforded by the United States, that it is not to be revealed to another country or international organization without the written consent of the Center for Army Lessons Learned.

Introduction

Traffic Control Point (TCP) Operations

"…In reference to conducting TCPs, you must shape situations to minimize the tough calls, and train our leaders on how to react…this will reduce the number of Iraqi civilian injuries and deaths."

LTG Petraeus, Commanding General, Combined Arms Center, *December, 2005*

In the Iraqi theater of operations, a TCP is defined as any position established to control movements into and out of an area where coalition forces (CF) will be in direct contact with vehicles and passengers to include the local populace. (For the purposes of this article, the terms traffic control point and vehicle checkpoint will be used interchangeably). TCP effects are synchronized across the lines of operations with a unit's higher headquarters and are differentiated by both placement techniques and duration. TCPs are normally part of an inner and/or outer security ring and are established to facilitate conducting vehicle searches (focusing on weapons, explosives, and other contraband). Personnel manning TCPs make positive identification (PID) checks to discover, apprehend, and kill, as necessary, targeted insurgents. TCPs also serve as an information collection gathering post for CF and the civilian population.

Soldiers conducting TCP operations in Iraq today are routinely required to make split-second, life-and-death decisions. TCP personnel must decide whether vehicles or pedestrians pose a significant force protection threat. Soldiers, manning numerous TCPs across Iraq, face a tough and dangerous mission and perform their duties admirably, 24/7. Commanders, at all levels, know they must provide the required resources to empower Soldiers to do their best and make the appropriate decisions.

Reports from the field verify that Iraqi responses vary widely at TCPs. The circumstances on the ground can initially appear ambiguous and confusing. Vehicles may approach a TCP at a high rate of speed or drive in an erratic or unpredictable manner. To conduct an effective TCP in Iraq today, Soldiers must understand the person they are attempting to control.

Most Iraqis entering a TCP have no hostile intent and will be compliant, but they may also be confused and in a hurry. Iraqis fitting this category usually recognize that security is important for their future and acknowledge that Soldiers simply have a job to do. Properly trained and patient Soldiers can keep interactions with the local populace calm and eliminate confusion at the TCP with clear, consistent, and repeated instructions.

Some Iraqis may approach your location with no hostile intent but will be defiant. They simply may not want to pull over for a variety of reasons. They may not

respond well to directions from non-Muslims and, in particular, to CF, who they may perceive as occupiers in their country. Iraqis fitting this category see this stop as an unreasonable request and a waste of time because they have no hostile intent and only want to proceed with their business. They may initially be compliant, but they may also grow angry, and that anger can quickly escalate to evasiveness or hostility. They may decide not to stop or may attempt to bypass or even turn around to avoid a TCP. They may not understand or may pretend to not understand posted and verbal instructions and warnings. This type of driver is the most difficult to assess when determining potential hostile intent and the corresponding escalation of force (EOF) response. Properly trained and patient Soldiers can normally diffuse defiant, but non-hostile vehicle occupants with clear, consistent, and repeated instructions. However, if the driver refuses to obey instructions and warnings but has not yet displayed overt hostile intent, Soldiers must begin to consider appropriate EOF measures. Leaders at all levels should teach and reinforce the use of this tactical pause to all Soldiers operating a TCP.

A driver approaching a TCP with hostile intent creates a serious and dangerous situation. This event usually develops rapidly, and CF have limited reaction time. This scenario often develops into actions on contact. A smart and inventive enemy will use a myriad of personnel, vehicle borne improvised explosive devices (VBIEDs), and small arms fire in an attempt to inflict casualties at TCPs. Properly trained and equipped Soldiers manning TCPs constructed to standard that provide maximum force protection and response times are the keys to success.

Establish TCPs to control traffic where and when you want it in order to shape the conditions for success. You must make it the Iraqis' decision to comply or not comply, and give the Soldier more time to react. You must put the decision to comply squarely on the shoulders of the driver of the vehicle through a series of control measures. Patterns picked up from theater clearly indicate that successful TCP designs accomplish the following:

- Provide Iraqis with an earlier warning.
- Slow down traffic at the earliest opportunity.
- Firmly control the traffic flow.
- Establish a distinct vehicle search area with blast protection.
- Establish a clear warning line where Soldiers have an opportunity to regain compliance from vehicles and assess EOF actions.
- Integrate latest available EOD capability.
- Have combat life savers and be able to quickly conduct medical evacuation, if required.
- Prepare for detainee operations.

- Employ a defendable engagement area if lethal force is required.
- Effectively position TCP personnel.
- Leverage available barrier equipment
- Have capability to disseminate TCP operations intent/procedures to educate the local population, mitigate problems, and secure local populace support/compliance.

Commanders in Operation Iraqi Freedom (OIF) standardized operations by designing a naming convention for the different types of TCPs. TCPs are categorized by task, purpose, and employment duration and are either static or mobile.

- Permanent TCPs are deliberately established static positions determined to be an ongoing fixed site requirement to control or monitor a specified location for a long duration. They are normally established along main supply routes or at critical intersections and are large, man-power intensive, hardened, well equipped, and advertised to the local population.
- Snap (also referred to as flash or hasty) TCPs can be part of a predetermined plan or established as an impact operation. They are often hastily erected and require less manpower. Because of the quick set up time, they are not as hardened or well-equipped as a permanent TCP. Depending on mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC) they may or may not be advertised in advance to the local population. Snap TCPs are designed to control movements for a short duration (normally 30 minutes or less) and are established in reaction to actionable intelligence or as part of displaying an impact security presence in an area. Staying too long at a given location tends to draw the enemy to the snap TCP; therefore, their effectiveness degrades over time.
- Rolling TCPs are set up in response to conditions on the roadway and/or enemy activity or to facilitate unimpeded CF movements. Duration is METT-TC dependent.
- Temporary halt TCPs are established due to exigent circumstances and collapse as soon as the problem is fixed (e.g., combat logistics patrol maintenance stop).

All control movements have the potential to interact with the local population. Personnel conducting reconnaissance for potential TCPs must pick locations which best balance force protection and traffic circulation control. Always anticipate second and third order effects of the site location. When establishing TCPs, leverage available road space with available resources to include non-lethal weapon/ammunition and barrier equipment sets. TCPs are always employed with the inherent capability to conduct lethal fire and should be oriented to defend in depth if penetrated. All TCPs operate under the same rules of engagement (ROE)

and EOF, but the application of graduated response must be tailored to the physical environment, volume of traffic, and crowd control. Training and rehearsals must be tailored for different TCP operations.

EOF Considerations

Graduated response measures are used to protect both CF and Iraqi citizens. EOF procedures are fundamental considerations during any TCP incident. EOF must be an integral part of all training scenarios and cannot be treated as a stand alone event. EOF vignettes addressing ambiguous conditions are a powerful teaching tool (see Chapter 3). Lessons learned from OIF reveal that the more control measures and barrier equipment at a TCP, the more time a Soldier has to make an EOF decision. More time often results in enhanced situational awareness, which may lessen the requirement to escalate to higher levels of force. Applying the right response, at the right time, is vital to all operations in Iraq. Remember, the unnecessary use of deadly force by CF on Iraqi civilians diminishes Iraqi support for the coalition and its objectives. Inappropriate use of lethal force destroys the lives of innocent Iraqis and their families, who could otherwise have played a vital role in the future of Iraq. Lethal force incident at TCPs also potentially fuel future insurgent activity and provide a negative propaganda message the anti-Iraqi forces can use to delay progress in Iraq.

Chapter 1

Leadership Challenges of Preparing Soldiers for Traffic Control Point (TCP) Operations

This chapter addresses the significant leadership challenges of preparing Soldiers for TCP operations, as recognized by experienced commanders currently serving in Iraq. The information in this chapter is intended to help Soldiers properly execute their duties by providing them with the tools they need for success including TCP tactics, techniques, and procedures (TTP), recommended equipment lists, and escalation of force (EOF) procedures within defined rules of engagement (ROE).

Reports from commanders in Operation Iraqi Freedom (OIF) verify that there are too many deadly force incidents at TCPs, both static and rolling, that could be prevented or handled with less than lethal force. Reducing the number of deadly force incidents at TCPs is both a leadership challenge and a training issue. Leaders naturally and rightfully tell their Soldiers to use caution and assess each and every situation; however, successful leaders in OIF today realize they must shape the situation at a TCP by using control measures and preparing Soldiers to respond.

Leaders understand that successful TCP operations begin with the Soldiers' ability to better communicate and more effectively interact with the Iraqi people. They know if Soldiers do this, they are in a better position to respond with a measured EOF to control the situation and execute their mission.

Leaders, at all levels, understand that Soldiers must use a combination of techniques to communicate and control Iraqi drivers including verbal commands, hand and arm signals, signs, light sets, and barriers. They also know these techniques are not an inherent ability, but trained skills the Soldier must develop as he attains situational awareness (SA). Positive control at TCPs is difficult to obtain and must be both planned and trained. Standard battle drill rehearsals must transform behavior into instinct. Trained Soldiers can more easily differentiate between a vehicle that is simply ignoring their warning and a vehicle that is displaying willful disobedience or hostile intent. Trained units who rehearse their anticipated responses are better prepared to deal with all types of TCP incidents. Trained leaders and Soldiers know they must exhaust all measures before using deadly force.

TCP operations are a team effort. Soldiers monitoring vehicle traffic at a TCP must quickly establish SA and effectively communicate with one another. Soldiers must be aware of the current situation and be able to predict future events based on their battle drill training. A rushed and inappropriate response of a single Soldier cannot become the team's response. Setting the conditions and controlling the situation remain a chain of command issue and a leadership challenge in a situation where events can happen or develop quickly. Rehearsed battle drills, early warning, and

barrier placement help to shape the environment for both optimum force protection and traffic control.

Leaders must be clear on how to train, conduct, and equip Soldiers to properly set up and execute TCP operations. The consequences of a Soldier making the wrong decision and incorrectly applying EOF procedures within the defined ROE, could be death or injury to non-combatants/civilians on the battlefield, coalition forces (CF), Iraqi Army (IA)/Iraqi Police Services (IPS), and/or fellow Soldiers.

Collectively, a wrong tactical decision (or at least a public perception of wrongdoing) can also have potentially long-term, strategic consequences, as evidenced by the recent shooting of a bodyguard for a reporter at a U.S. Army checkpoint. This type of unnecessary application of force endangers our efforts to win the hearts and minds of the Iraqi people and sustain the coalition. Leaders are challenged to have their units always at the ready, yet able to practice tactical patience in order to let the situation develop before acting decisively. At the other end of the spectrum, the failure or refusal of a Soldier to shoot at enemy targets could result in death or injury to the Soldier and others manning the checkpoint.

Leaders know that battle drill training requires their personal involvement and that training must be tailored to a specific TCP incident. OIF after action reviews (AARs) and checkpoint operations and battle stress-related information extracted from CALL Initial Impression Report No. 05-35, *Cultural Awareness Impact upon Battle Command,* provide the following training tips:

- Soldiers must know that there is a complex and, often, ambiguous environment out there.
- When establishing and conducting TCP operations:
    - Give yourself early warning.
    - Balance force protection and movement control.
    - Do not “telegraph” your position unless that is your intent.
    - Know how to employ hand and arm signals; signs; flares; lasers; and other control measures, such as TCP equipment sets and non-lethal weapons and ammunition.
- Human intelligence (HUMINT) collection remains the largest producer of actionable intelligence. More local Iraqi engagement normally leads to more preventable TCP interdiction.
- Cultural awareness is not merely customs training. You must know how Iraqi honor shapes behavior.
- Deploy with a baseline of Iraqi command and control phrases and be able to communicate with or without an interpreter.

- Know how to influence the person you are dealing with.
- Using an interpreter is a deliberate process and must be rehearsed. Soldiers and interpreters must be a team. Effective interpreter teams are better able to diffuse potential problems at TCPs.
- Apply the right response at the right time. Both ROE and EOF protect you and others, while minimizing collateral damage.
- Know and quickly use the explosive ordnance disposal (EOD) "9-line" report.
- Leverage Iraqi Security Forces (ISF) (both the IA and IPS) knowledge of the area to mitigate potential threats to TCP location, to communicate your message to other Iraqis, and to make positive identifications (PIDs) of insurgents. Lack of PID and inadequate evidence collection procedures can lead to the release of a potential insurgent from an Iraqi court.
- Leverage HUMINT, TTP, barrier equipment sets, and available technology to counter the improvised explosive devise threat.
- Maintain operational security. Leaks about any operation help the enemy.
- When permitted, let the local Iraqis know you are conducting TCPs for their security and safety. Getting them to buy into and support the process is fundamental to winning the "perceptions war."
- You must be able to treat your own casualties and call for help if care is beyond your capability.
- At many checkpoints, Iraqis failed to understand the hand signals commonly used by U.S. military personnel, and Soldiers must draw their weapons to force a driver to stop.
- People at checkpoints, roadblocks, and entry control points react differently to a pistol than they do to a rifle. In the Saddam regime the pistol was the preferred method of execution. Whenever a Soldier drew his/her pistol in a situation, the Iraqis would react in a very obedient or cowering manner. The pistol represented authority, and Iraqis treated the bearer accordingly.
- Remove sunglasses, when appropriate. Iraqis feel that the "eyes are the windows into the soul," and they do not really trust someone if they cannot see their eyes.
- To decrease the possible loss of life at checkpoints and vehicular contact locations, be familiar with Iraqi body language and commonly used Iraq-specific hand signals.
- Cultural awareness is a force protection issue.
- Leaders must be aware of the potentially adverse effect that stress might have on their Soldiers' internalization and application of cultural awareness values during a long and violent deployment.

- Soldiers in units participating in heavy fighting and suffering many casualties may tend to become culturally insensitive at higher rates than other Soldiers. Soldiers who have participated in multiple OIF deployments may share the same tendencies.

TCPs on the asymmetrical battlefield are combat operations. Leaders, at all levels, understand that TCPs are critical missions. Reactions from the local populace at TCPs are often confrontational and potentially hostile and can be militarily and politically sensitive operations. Although only a limited number of Soldiers conduct TCP operations, they are often the most exposed to hostile fire outside the unit's forward operating base. TCP personnel are the ones responsible for controlling the congested traffic; interacting with the local population; assessing potential threats; and defeating an often faceless enemy, all while applying the appropriate measured response.

Leaders have learned and are stressing to young Soldiers that they will often operate checkpoints in congested areas under ambiguous circumstances. Numerous unit AARs state that nothing should be treated as routine when conducting checkpoint operations. Soldiers and junior leaders manning TCPs must remain vigilant and suspicious. Treat each vehicle as if it were the most important one coming through the checkpoint. Soldiers are at the "tip of the spear" during these operations, and their actions support shaping the overall tactical situation. Use the following guidelines during TCP operations:

- Bring vehicles into your area when and where you want them.
- Balance telegraphing location with surprise and force protection.
- When you must defend, defend in depth.
- Design well equipped, erected, and positioned checkpoints to make the vehicle going through the barrier plan display non-hostile or hostile intent; well-designed checkpoints facilitate early warning and enable Soldiers to be more active than reactive, and, consequently, they have more time to make EOF decisions.
- Anticipate consequence management of all decisions against the information operations and media (public affairs) campaign.
- Synchronize TCPs as part of the overall security and movement control plans.

See Chapter 3, "Escalation of Force," Figure 3-2: Example Checkpoint with U.S. EOF Procedures.

OIF Observations

The following TCP operation observations, comments, and vignettes from Soldiers and junior leaders in the field offer TTP to help mitigate risks associated with setting up and engaging enemy targets at TCPs.

TCP Observations from OIF:

Observation #1: The "set-up" time for a TCP often alerts individuals of an impending TCP diminishing its effectiveness.

Discussion: Setting up the TCP is, unfortunately, one of the indicators of an impending TCP, and hostile individuals have learned many different techniques to avoid CF TCPs. As soon as cars start seeing the set-up, they begin to warn on-coming traffic of the TCP. A technique to counter this problem is the "rolling" or "traffic jam" TCP. The sequence is as follows: The patrol picks a location for the TCP that is on a well-traveled road. Instead of traveling to that location immediately and establishing the TCP, the patrol drives towards the TCP location and has the trail vehicle pull off to the side of the road approximately 500 meters prior to the inspection area. The lead three vehicles travel in a staggered column formation in order to block traffic from passing them and begin to slow as they approach the inspection area. The intent is to have local vehicles trailing the three CF vehicles until the TCP is set. When the lead vehicles get to the inspection area, they are already in TCP formation and immediately begin TCP operations. The trail vehicle that had pulled off the side of the road moves to the rear of the column of vehicles and blocks them in. The TCP subsequently inspects the vehicles caught in the traffic jam. The patrol then has the option of allowing additional vehicles into the TCP or moving to an alternate location.

Lesson: Units include this variation of the TCP in their patrols. This technique is intended for a very short duration to surprise cars following behind military vehicles. It will not substitute for the more deliberate TCP techniques that patrols use but can add an extra measure of unpredictability that will limit the enemy's ability to counter TCPs.

Observation #2: The unit conducted a map reconnaissance for possible vehicle checkpoint (VCP)/TCP locations based on the template from the battalion order.

Discussion: The technique used for selecting a VCP/TCP was to find a wadi or other terrain feature in the templated area and use it for cover and concealment for support vehicles. The hide site was close to the checkpoint. The unit wanted to use this TTP because of increased observation in a desert environment and wanted to increase survivability for vehicles not used in the VCP/TCP. The unit also placed OPs, manned by the scout platoon, at higher elevations to provide overwatch prior to establishing a VCP/TCP. The unit modified the TTP based on the terrain available. They were not always able to use the terrain to hide the vehicles.

Lesson: A map reconnaissance is invaluable in selecting likely positions for conducting VCPs/TCPs. Once at the location, leaders must make adjustments based on mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC).

Observer/Controller Observations from Combat Training Centers (CTCs):

Rotational units do not conduct enough checkpoint operations. This situation may stem from the rotational training unit not getting a good intelligence read to drive initiation of TCP operations. The amount of focus on checkpoint operations is dependent on the rotational unit's training objectives. Most units will train this task during cordon and searches or snap checkpoints; however, execution of this task is dependent on the rotational training unit's plan. Over the past year, many fixed site and checkpoint security requirements have transitioned to host nation forces. As a result, less of these types of missions are incorporated into current rotational scenarios. The search and attack and combat patrol lanes create an excellent opportunity for units to train this task. Still it depends on the unit's read to incorporate TCPs into the plan. When TCPs are conducted, O/Cs provide on-going coaching and feedback during AAR discussions.

Units are coached to employ snap TCPs that are driven by the intelligence, surveillance, and reconnaissance (ISR) process. Two benefits from this approach are that the snap TCP is active and does not inherently create a pattern, Units are also coached to continue their analysis to ensure that they are not establishing patterns. (See Chapter 4 for information on establishing a snap TCP).

Risk-Mitigation TTP Recommendations

The following analysis/recommendations for training and leader development are intended to reduce risk, enhance force protection, limit collateral damage, assist leaders and Soldiers in applying EOF at TCPs, and enhance combat to training integration:

Training

- Units must conduct checkpoint operations at home station, CTCs, and mobilization training centers and integrate into reception, staging, onward movement and integration (RSOI) prior to deployment to a combat theater.

- Checkpoint operations standing operating procedures (SOP) vary widely from unit to unit. Consider development and implementation of command-directed mission essential task list (METL)/SOP for checkpoint operations to standardize procedures. The below list is not all inclusive, but represents some of the essential elements required for checkpoints:

- º Number of personnel required (based on intelligence preparation of the battlefield, area of operations, and METT-TC) for different type of checkpoints.
- º Snap TCP equipment list and pre-configured sets and vehicle load plans incorporated into unit SOP.
- º Required training that includes current, OIF based TTP and interrogation procedures.
- º ROE/EOF.
- º Local/English language signs (to include sign dimensions, distance intervals before checkpoint, etc.).
- º Interpreters/Linguists interface.
- º Detainee processing checklist
- º Properly developed checklists are codified in SOP; standards via plans (include branches and sequels) and orders (operations orders and fragmentary orders) are enforced.

- Junior leaders (noncommissioned officers [NCO] and company grade commissioned officers) must conduct rigorous, routine pre-combat checks, pre-combat inspections, and rehearsals (troop leading procedures [TLP]).
- Once the checkpoint rehearsal is completed, conduct a thorough AAR to discuss what went right (sustain) and areas that need improvement. Rehearse again; repetition increases proficiency in the tasks that must be completed. If Soldiers are well rehearsed on the required METL associated with checkpoint operations, it increases the likelihood for successful mission accomplishment in combat operations.
- Recommend that a snap TCP team be designated for every platoon. Use the snap TCP team to train the rest of the company to enhance operational capabilities. (See Chapter 4: Snap TCP Operations.)
- If an EOF incident occurs resulting in discharge of weapon, integrate the following steps into scenario lane training/rehearsals:
  - º Determine if death, injury, or property damage has occurred.
  - º Secure the site.
  - º Render first aid.
  - º Request civilian ambulance or conduct medical evacuation.
- Integrate follow-up reporting into scenario lane training; report to higher headquarters. (See Chapter 3, "Escalation of Force," Figure 3-1: Incident Occurs Resulting in Discharge of Weapon.)

- Incorporate threat identification into reflexive fire training; include EOF discriminatory fire during individual marksmanship training.
- Conduct transition training from optics to signaling devices to weapon systems. Ensure Soldiers are confident with the transition process to prevent application of EOF too quickly.
- Train EOF during basic combat training.
- Incorporate EOF into annual individual training requirements.
- Continue to incorporate all aspects of EOF scenarios into collective training at home-station training (field training exercises), mobilization centers, CTCs, mission rehearsal exercises, and RSOI (opportunity training) prior to deploying to a combat theater and during the unit's relief in place/transfer of authority validation program.

Leader Development

- Incorporate EOF and EOF consequence management training into Basic Officer Leader Course and NCO leadership courses.
- Leaders must recognize the signs of combat stress and how it affects Soldiers at EOF incidents. Leaders must take pro-active measures such as counseling; appropriate medical consultation; and relief (rest period), when possible, to help alleviate the pressures of combat. Soldiers must strive to maintain their reasoning faculties when under extreme duress in often ambiguous combat situations.

Summary

Soldiers and junior leaders at TCPs face multiple, potentially violent situations with every vehicle encountered. They must simultaneously orchestrate the important issues of ensuring force protection; interdicting, disrupting, and detecting possible insurgents and contraband; and protecting civilians from harm, without unnecessarily impeding traffic movement. Senior leaders in OIF report that more must be done to train all Soldiers and leaders on how to shape the situation and react to complex situations. These skills require all Soldiers and leaders to be ever vigilant and apply TLP and well rehearsed TTP. Everyone assigned to a TCP must maintain SA, know the ROE/EOF procedures, maintain an aggressive but controlled combat posture, and know how to report or to bring additional forces and support to bear if required.

Chapter 2

Rules of Engagement (ROE)

The following standing operating procedure (SOP) examples were adapted from a unit in Operation Iraqi Freedom (OIF) and are an expansion of Multi-National Coalition Forces-Iraq (MNC-I) rules of engagement (ROE) developed by a commander for Soldiers in his command.

This SOP establishes standard ROE for all elements of the command. These rules are for initial planning. These rules may be changed or modified for a specific operation or phase of an operation. Commanders and leaders at all echelons are responsible for keeping all Soldiers aware of the current ROE.

Self defense

Nothing limits the right of individuals and units or a commander's inherent authority and obligation to use all necessary means to defend themselves, their units, and others in the vicinity. Use of force proportional to a threat, to include deadly force, is authorized in defense of yourself, your unit, other U.S. Soldiers, and other persons in your vicinity and in defense of property specifically designated by your commander. Use only necessary and proportional force. Minimize collateral damage.

Definitions

- Collateral damage is the unintended loss of civilian or noncombatant life, injury to civilians, or damage to civilian property incident to the legitimate use of military force. Do not use force reasonably expected to cause collateral damage disproportionate to the concrete and direct military advantage expected to be gained.

- Dual-use facilities are infrastructures, facilities, structures, or systems used by or reasonably expected to be used by both hostile forces and the local civilian populace. Examples include public works such as power stations, water systems and storage, and major roads and bridges.

- Hostile acts are attacks or other use of force against the U.S., U.S. forces, or friendly forces. It is also force used directly to preclude or impede the mission and/or duties of U.S. forces.

- Hostile intent is the threat of imminent use of force against the U.S., U.S. forces, or friendly forces. It includes threats against civilians or property specifically designated as under U.S. protection.

- Military necessity requires attacks on legitimate military targets using only that force necessary to achieve U.S. goals, unless such force is prohibited by the Law of War.

- Observed fire is fire for which the point of impact or burst can be seen by an observer or clearly identified by imagery, including live feed unmanned aerial vehicle imagery. The imagery must be less than eight hours old or within a period of time during which the target could not reasonably have moved. The fire can be controlled and adjusted on the basis of observation. An acquisition by radar (Q36/37) is considered observed fire; however, target area analysis (map/imagery/reconnaissance) must be done to ensure the target is not in a populated area.

- Populated areas are cities, towns, villages, built-up areas, and/or those areas designated on operational overlays as populated areas.

- Proportional force is force that is reasonable in intensity, duration, and magnitude to the perceived or demonstrated threat based on all facts known to the commander at the time.

- Self defense is the minimum amount of force necessary to decisively counter hostile acts or demonstrated hostile intent and ensure the continued safety of U.S. forces or other protected persons and property.

Lawful targets

The following types of targets may be engaged with all lawful means subject to the restrictions contained in these ROE.

- **Hostile forces.** A hostile force includes all conventional and unconventional units declared hostile within the unit's area of operations (AO). Hostile forces may be engaged with all lawful means, up to and including deadly force, subject to the following restriction: **Do not engage anyone who has surrendered or is out of battle due to sickness or wounds**.

- **Hostile aircraft/vessels**. Declared hostile forces' military aircraft/vessels will be considered hostile and may be engaged with all lawful means, up to and including deadly force, subject to the following restriction: **Do not engage aircrew personnel descending by parachute from a disabled aircraft or shipwrecked personnel**.

- **Military objectives**. All military objectives may be engaged, including those in cities and populated areas, subject to the limitations in these ROE. Apply proportionality and minimize collateral damage.

Protection of civilians and civilian property

- Civilians are protected persons entitled to respect of both their person and property. Do not target civilians unless in self-defense, defense of others, or defense of designated property in response to a hostile act or demonstrated hostile intent. Report engagements of protected persons to the staff judge advocate.

- When attacking military forces, military targets, or returning fire inside populated areas, the loss of life and damage to property must not be out of

proportion to the military advantage to be gained. Use reasonable force that is proportionate to the threat.

- Do not seize civilian property without approval of a company level commander and only for stated military purposes. If the property is occupied when seized, provide the owner with a receipt describing the condition of the property. Keep a copy.

- Except as authorized above, do not seize, commandeer, appropriate, or liberate private or public property unless authorized or directed by a battalion/task force commander.

- Protect livestock, crops, trees, wells, and water sources from unnecessary harm.

Civilian restraint and movement restriction

- Civilians may be restrained (arrest, detention, interrogation, disarmed, etc.) only when required to protect lives, property, or the security of operational facilities and areas and when all other means have failed.

- Civilian movement may be restricted when required by military necessity. Civilians failing to comply with movement restrictions in areas under unit control may be stopped and required to show identification and/or apprehended and detained (including their means of transportation) using the minimum amount of force necessary.

- Generally, civilians are denied access to secure areas/facilities (airfields, tactical operation centers, support areas, communication centers, etc.). Those attempting unauthorized access will be challenged, identified, and informed of access restrictions. Those gaining unauthorized access will be apprehended using the minimum force necessary and detained until it is determined if further action is warranted.

- Follow published rules for the search and treatment of detained personnel.

Protected places/properties

Hospitals; churches; shrines; schools; temples; museums; national monuments; and other historical, cultural, or religious sites are protected places. You may not engage a protected place unless it is being used for a military purpose and your mission or defense requires its engagement.

Dangerous public utilities

Do not engage installations that present potential dangerous conditions (nuclear power plants, dams, dikes, levees) or sites that when damaged/destroyed are likely to cause weapons of mass destruction [WMD]-like effects without prior approval of the brigade commander.

Search and seizure

As a force protection measure, battalion/task force-level commanders may authorize probable cause searches of any persons, vehicles, and/or places when there are reasonable grounds to suspect the presence of weapons or ordnance and may seize those weapons or ordnance. When possible, coordinate searches with local civilian authorities. Absent any hostile or criminal acts, persons relinquishing weapons or ordnance to U.S. forces will be released. Others should be turned over to local civilian authorities as soon as possible.

Fire support

- Nothing in this paragraph is intended to limit the inherent right to take all necessary and proportionate action in self-defense/defense of others.
- All fire missions directed against known or suspected targets in populated areas must minimize collateral damage.
- The tactical commander (battalion task force and/or company/team) controlling fires may approve observed fire into populated areas within his AO.
- Only the commander may authorize unobserved fire into populated areas within the AO. Approval is not required if the unit is in contact or at risk of being overrun or destroyed and uses only the necessary and proportional amount of force to neutralize or destroy the hostile act/intent.
- The next higher level commander is the approval authority for targeting suspected dual-use facilities and protected properties. As always, this does not limit the right of self-defense/defense of others. If the enemy misuses a protected property, it is no longer protected and may be targeted, applying the principles of necessity and proportionality in order to minimize collateral damage.

POPULATED AREA AUTHORITY MATRIX			
TYPE OF FIRE	**OBSERVED**	**UNOBSERVED**	**EXCEPTION**
Direct Fires	**Authorized**	**N/A**	
Indirect Fires	**Authorized** **Tactical Commander is Approval Authority**	**Authorized** **Brigade Commander is Approval Authority**	**Self Defense**
Large Caliber Incendiary	**Authorized** **Brigade Commander is Approval Authority**	**Authorized** **Brigade Commander is Approval Authority**	**Self Defense** **+** **Brigade Commander Approval**

Mines

Conventional anti-personnel mines are prohibited.

Riot control agents (RCA)

Riot control agents (RCA) may only be used upon receipt of the brigade commander's authorization. (Cayenne pepper spray is an RCA.) If approved, RCA may only be employed in defensive modes to save lives in areas under direct military control. Examples include:

- Rioting by enemy prisoners of war/detainees.
- Dispersing civilians who are obstructing roadways or otherwise impeding distribution operations after lesser means have failed to result in dispersal.
- Rear echelon areas outside the zone of immediate combat to protect convoys from civil disturbances or terrorists' attacks.
- In combat search and rescue missions in remote areas outside the zone of immediate combat.
- RCA may not be employed in the following situations:
    - º As a method of warfare.
    - º When civilians are used to mask or screen hostile forces.

- Rescue missions in combat areas for downed aircrews and passengers and escaping prisoners.

Other chemical agents

- Use of herbicides is not authorized except for the control of vegetation within U.S. bases and installations or around their immediate defensive perimeters.
- Use of lethal or incapacitating chemical weapons/agents is not authorized.

International and joint operating area boundaries

No ground/air operations, including "hot pursuit" of enemy forces in contact or fires/air strikes will be conducted outside of the air, land, or sea space of unit's AO without authorization from the brigade commander.

Chapter 3

Escalation of Force (EOF)

"All MNC-I troopers and leaders at all levels understand and apply the identified EOF procedures in order to prevent unnecessary deadly force engagements toward Iraqi citizens…"

Commanding General, Multinational Corps-Iraq (MNC-I)*, *December, 2005

This chapter focuses on information disseminated in a current MNC-I operations briefing, "MNC-I Escalation of Force Training Package" (5 December 2005), and an MNC-I fragmentary order (FRAGO) (25 February 2006) regarding escalation of force (EOF) policies and guidance.

In Operation Iraqi Freedom (OIF), current pressing issues include the application of appropriate rules of interaction/rules of engagement and using escalation of force (EOF) commensurate with the level of threat the Soldier faces, while limiting collateral damage to civilians on the battlefield. Iraqis perceive that coalition forces (CF) engage in indiscriminate killing at traffic control points (TCPs). Soldier actions outside the authorized EOF procedures undermine the unit's mission and have potential to negatively affect CF information operations and public affairs operations campaigns. MNC-I reports that incidents outside the authorized EOF procedures have occurred and are presently occurring at TCPs.

Most Iraqi vehicles enter and exit TCP without incident. Throughout the Iraqi theater of operation (ITO), there are many varied elements (vehicular traffic, dismounted personnel, contracted workers, personal security detachments) that must be quickly identified at TCPs. Without positive identification, these vehicles present a perceived threat to CF force protection. EOF procedures provide alternatives to the use of lethal force for forces conducting ground operations in the Iraqi theater of operation.

Definitions:

- EOF is defined as sequential actions which begin with non-lethal force measures (visual signals to include flags, spot lights, lasers, and pyrotechnics) and graduate to lethal measures (direct action) to include warning, disabling, or deadly shots in order to defeat a threat and protect the force.

- Defensive actions are defined as EOF procedures that terminate with successful employment of non-lethal means (hand/arm signals, colored flags, spot-lights, pyrotechnics, or any other available resource).

- An EOF incident is defined as the employment of lethal force that results in weapons discharge, where the purpose or intent of the weapons discharge was to warn or employ in self-defense of an individual or unit.

Procedures to employ during EOF incidents:

- Use audible warning to warn (horn, air horn, loudspeaker, flash/bang device, siren).
- Use visual aids (lights, laser pointers, flares, colored flags, signs).
- Show weapon and demonstrate intent to use it.
- Attempt non-lethal means (stop strips, physical barrier, vehicle, visual/audio signal, signs).
- Fire warning shots (in vicinity of threat).
- Use disabling fire (tires, engine block, windows).
- Use deadly force (proportional to threat).

Contributing factors which may lead to unnecessary deadly force engagements toward Iraq citizens:

- Predeployment training did not use current in theater EOF policy and procedures.
- Training scenarios did not replicate the complex and often ambiguous environment in Iraq.
- Training did not include "what if" vignette drills to train best and worst case scenarios.
- Higher headquarters did not provide detailed EOF guidance to lower units.
- Leaders are not enforcing EOF standards.
- Leaders are not talking to Soldiers; Soldiers are not talking to each other.
- Units are not making EOF part of mission analysis before establishing TCP.
- Units are not adjusting their standing operating procedures (SOPs) or battle drills to prevent excessive use of force incidents.
- Units are not integrating EOF into pre-combat inspections/checks, actions on contact, battle drills, and after action reviews.
- Units are not meeting local Iraqi leaders to make them aware of EOF procedures resulting in a lack of local community understanding of TCP operations.
- Units are not interacting with the Iraqi population.
- Soldiers are not aware of Iraqi significant calendar events (religious holidays, etc.) that may significantly increase vehicle traffic.

- Soldiers are not aware of local business locations and operating hours in the vicinity of their TCP area of operations.
- Soldiers are not exercising positive control or "muzzle awareness" on weapon systems.
- Units are not consistently reporting EOF incidents in a timely manner.
- Units are not conducting constant reviews of EOF procedures.

Soldiers must have the following information in order to prevent potential fratricide incidents:

- Location of adjacent units/TCPs.
- CF movement control plan (including CF scheduled movement credits; planned Iraqi Army (IA)/Iraqi Police Services (IPS) movements; and interagency/non-governmental movements, if known).
- Aviation reconnaissance plan.
- Quick reaction force (QRF) plan.
- IA/IPS support at TCP and/or their patrol patterns.
- Medical evacuation support (air and ground; military [Iraqi and coalition] and civilian).
- Vehicle recovery plan.
- Detainee transportation assets supporting evacuation plan.
- Explosive ordnance disposal support.

EOF Vignettes

The following vignettes illustrate recent EOF incident experience in OIF and are suitable for incorporation into predeployment training.

Example 1: Outer Cordon:

Unit was on the outer cordon for a cordon and search when a civilian vehicle approached and ignored shouts, vehicle horn, and flashing lights. The unit fired one shotgun round as a warning shot. The vehicle ignored the warning and continued. The unit fired 13-15 rounds of 7.62-mm into the vehicle, resulting in two civilians killed and two civilians injured. No CF were injured or killed.

Example 2: Screen Mission:

The patrol, while posted at an intersection, observed a vehicle traveling at an unusually slow speed coming toward the cordon from the north. Because of

sustained enemy contact over the preceding 30 minutes and the unusually slow speed of the vehicle, the unit suspected it to be a possible vehicle borne improvised explosive device (VBIED). At 327 meters, Marines shouted and used hand and arm signals in an attempt to stop the vehicle. At 260 meters, the gunner fired three .50 caliber rounds at the deck (Marine term for "ground") in front of the vehicle. At 175 meters, the gunner fired ten .50 caliber round disabling shots into the vehicle. The vehicle was struck, collided into parked vehicles, and came to a stop. The driver jumped out of the vehicle and ran to the west, out of sight. Within seconds of this engagement, a second vehicle heading from the same direction approached the cordon in the same manner as the first vehicle. Again the unit believed it to be a possible VBIED and initiated verbal commands, as well as hand and arm signals, to stop the vehicle. At 250 meters, the vehicle did not stop, and the gunner fired three disabling shots into the vehicle. When the second round impacted the vehicle, it immediately ignited, and the vehicle was almost instantly consumed by flames from the ensuing fire. The driver exited prior to the vehicle being completely engulfed by flames and ran away from the vehicle and out of sight. This incident resulted in two civilians (insurgents) killed and no CF casualties.

Example 3: Convoy #1:

The unit reported an EOF incident on a supply route. The patrol reported that while moving south on the route, a vehicle approached their patrol at a high rate of speed from the rear. The patrol began using hand and arm signals to wave the vehicle off, but the vehicle kept approaching the patrol. The patrol fired a warning shot into the ground, but the vehicle did not stop or slow. The patrol then fired into the vehicle's engine compartment, and the vehicle stopped. The patrol reported that the two civilians in the vehicle suffered no life threatening wounds. The civilians were transported to a medical hospital by local emergency services.

Example 4: Convoy #2:

The unit reported an EOF incident while securing an intersection. A vehicle was approaching eastbound on the road. The vehicle ignored a spotlight. The unit fired a 5.56-mm round when the vehicle was approximately 100 meters away. The vehicle continued to approach and another shot was fired from approximately 50 meters away. The vehicle then stopped, and the convoy continued on its mission without further incident. No injuries or damage to civilians or CF resulted from this incident.

The following figures provide an example of a traffic control point and guidance for training the EOF process, consequence management, and reporting procedures.

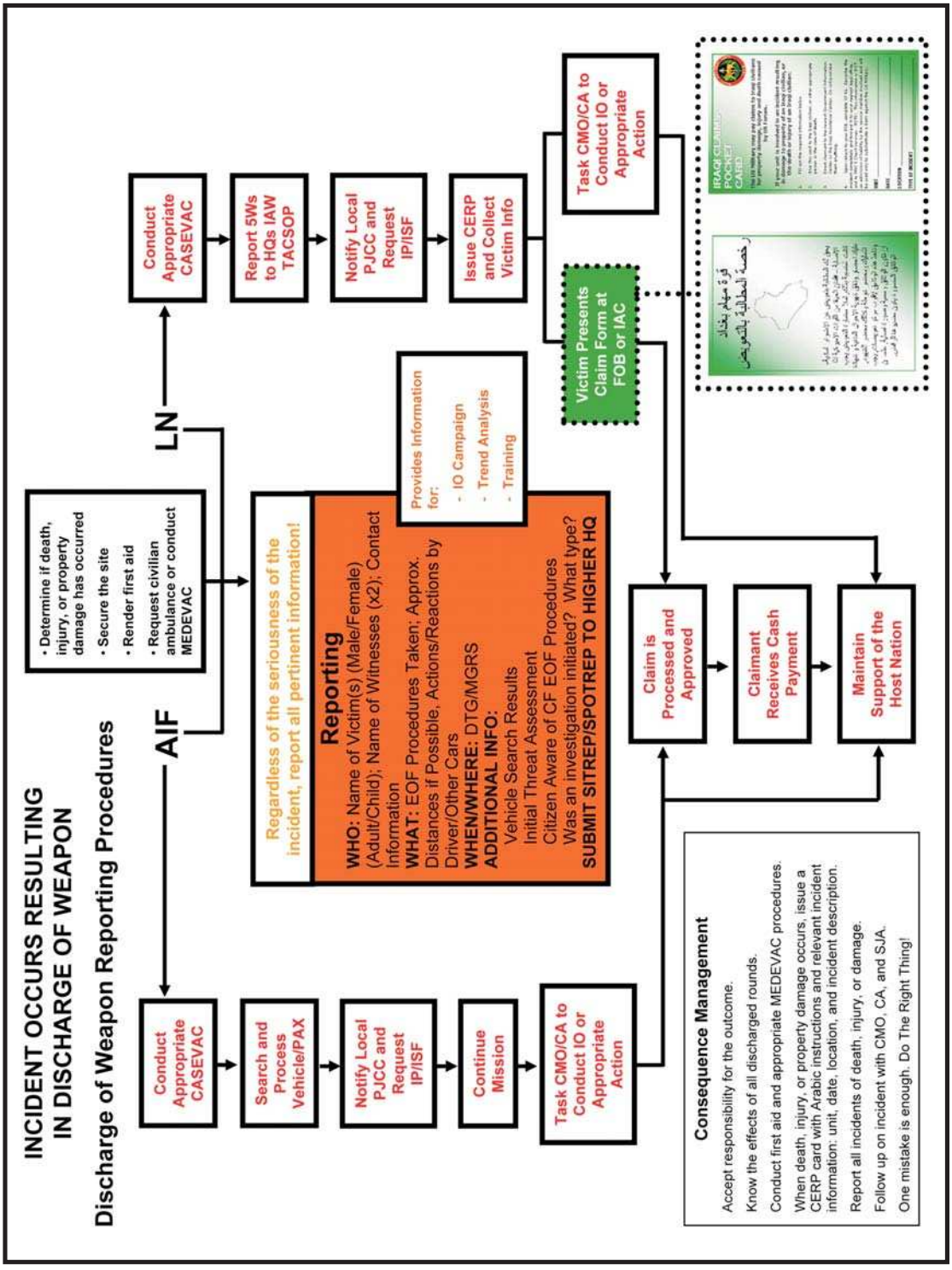

INCIDENT OCCURS RESULTING IN DISCHARGE OF WEAPON
Discharge of Weapon Reporting Procedures
AIF
LN
• Determine if death, injury, or property damage has occurred
• Secure the site
• Render first aid
• Request civilian ambulance or conduct MEDEVAC
Regardless of the seriousness of the incident, report all pertinent information!
Reporting
WHO: Name of Victim(s) (Male/Female) (Adult/Child); Name of Witnesses (x2); Contact Information
WHAT: EOF Procedures Taken; Approx. Distances if Possible; Actions/Reactions by Driver/Other Cars
WHEN/WHERE: DTG/MGRS
ADDITIONAL INFO:
Vehicle Search Results
Initial Threat Assessment
Citizen Aware of CF EOF Procedures
Was an investigation initiated? What type?
SUBMIT SITREP/SPOTREP TO HIGHER HQ
Provides Information for:
- IO Campaign
- Trend Analysis
- Training
Conduct Appropriate CASEVAC
Search and Process Vehicle/PAX
Notify Local PJCC and Request IP/ISF
Continue Mission
Task CMO/CA to Conduct IO or Appropriate Action
Conduct Appropriate CASEVAC
Report 5Ws to HQs IAW TACSOP
Notify Local PJCC and Request IP/ISF
Issue CERP and Collect Victim Info
Task CMO/CA to Conduct IO or Appropriate Action
Victim Presents Claim Form at FOB or IAC
Claim is Processed and Approved
Claimant Receives Cash Payment
Maintain Support of the Host Nation
IRAQI CLAIMS POCKET CARD
Consequence Management
Accept responsibility for the outcome.
Know the effects of all discharged rounds.
Conduct first aid and appropriate MEDEVAC procedures.
When death, injury, or property damage occurs, issue a CERP card with Arabic instructions and relevant incident information: unit, date, location, and incident description.
Report all incidents of death, injury, or damage.
Follow up on incident with CMO, CA, and SJA.
One mistake is enough. Do The Right Thing!

Figure 3-1

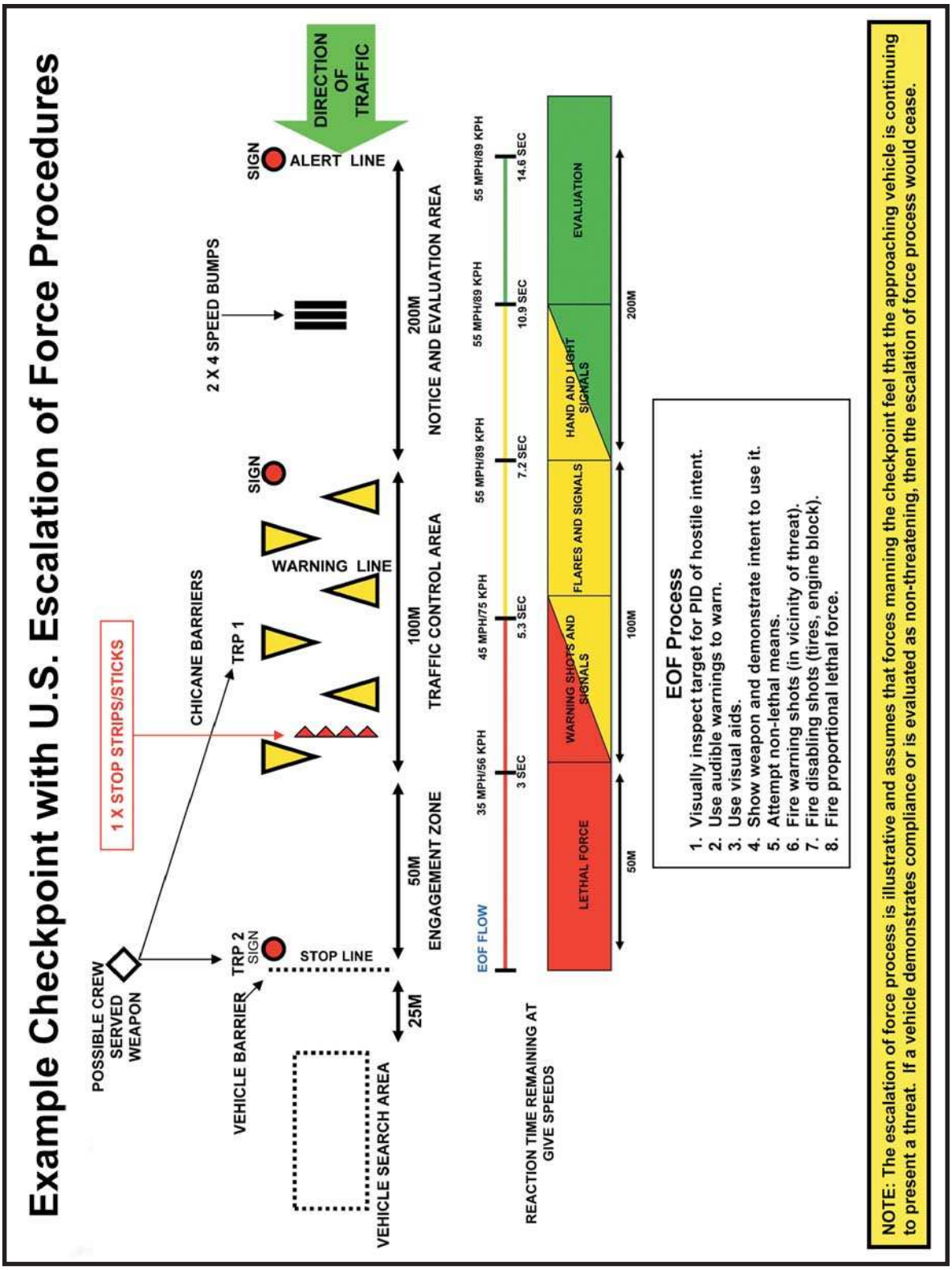

Example Checkpoint with U.S. Escalation of Force Procedures
DIRECTION OF TRAFFIC
SIGN
ALERT LINE
2 X 4 SPEED BUMPS
SIGN
WARNING LINE
200M
NOTICE AND EVALUATION AREA
100M
TRAFFIC CONTROL AREA
1 X STOP STRIPS/STICKS
CHICANE BARRIERS
TRP 1
POSSIBLE CREW SERVED WEAPON
TRP 2
SIGN
STOP LINE
VEHICLE BARRIER
50M
ENGAGEMENT ZONE
25M
VEHICLE SEARCH AREA
EOF FLOW
35 MPH/56 KPH
45 MPH/75 KPH
55 MPH/89 KPH
55 MPH/89 KPH
55 MPH/89 KPH
3 SEC
5.3 SEC
7.2 SEC
10.9 SEC
14.6 SEC
REACTION TIME REMAINING AT GIVE SPEEDS
LETHAL FORCE
WARNING SHOTS AND SIGNALS
FLARES AND SIGNALS
HAND AND LIGHT SIGNALS
EVALUATION
50M
100M
200M
EOF Process
1. Visually inspect target for PID of hostile intent.
2. Use audible warnings to warn.
3. Use visual aids.
4. Show weapon and demonstrate intent to use it.
5. Attempt non-lethal means.
6. Fire warning shots (in vicinity of threat).
7. Fire disabling shots (tires, engine block).
8. Fire proportional lethal force.
NOTE: The escalation of force process is illustrative and assumes that forces manning the checkpoint feel that the approaching vehicle is continuing to present a threat. If a vehicle demonstrates compliance or is evaluated as non-threatening, then the escalation of force process would cease.

Figure 3-2

Chapter 4

Snap Traffic Control Point (TCP) Operations

Planners must assume that TCPs will encounter enemy attempts to inflict casualties and battle damage and disrupt movement. These insurgent tactics are used both for their immediate destructive effects and for long-term anti-coalition force propaganda efforts. TCPs should never be established without the capability of being immediately reinforced.

TCP personnel screen, clear, document, and detain pedestrians and vehicles and their passengers. After vehicles are validated, drivers are allowed to continue down the roadway.

Snap TCPs are quickly erected, operate for a short duration, and achieve a specific purpose. Snap TCPs are often conducted under a time-compressed military decision-making process (MDMP) and serve as both a security and a movement control check. Because of their mobility, snap TCPs can cover multiple locations in a relatively short amount of time. Units have learned to position snap TCPs, leveraging the natural/man-made terrain and existing roadway features to canalize traffic and prevent the ability of insurgents to seek bypass. Coalition forces (CF) also integrate observation posts for overwatch and sniper positions for both added security and to defeat anticipated targets attempting to interdict TCPs along the main supply routes. More stringent force protection measures may be required for checkpoint operations of longer duration.

Purpose of a snap TCP:

- Quickly controls traffic and maintains the ability to search for enemy contraband or individuals (insurgents).
- Provides commanders with an ability to immediately have a security presence and influence an area of operations.
- Enhances force protection and establishes an engagement area for the application of graduated response measures if required.
- Deters, disrupts, and interdicts enemy freedom of movement; denies terrain; and facilitates capture of individuals (insurgents)/equipment based on actionable intelligence.
- Employs vehicle control measures to allow Soldiers more time to determine hostile intent of drivers negotiating a snap TCP.
- Emplaces obstacles which will stop vehicle-borne improvised explosive devices (VBIED) or suicide VBIEDs outside a 50-meter minimum safe distance of friendly troops (mission, enemy, terrain and weather, troops and support available, time available, and civilian considerations [METT-TC] dependent).
- Shows Iraqi people that their security is important enough to commit Soldiers to these positions.

Recommended escalation of force (EOF) procedures at snap TCPs.

If time and circumstances permit, use graduated response measures ("5 S"):

1. **SHOUT** warnings to stop (Arabic: "Kiff-Armik)
2. **SHOW** weapon
3. **SHOVE**, restrain, or detain
4. **SHOOT** warning shot*
5. **SHOOT** to eliminate threat

Note: You do not have to go through each step if the situation does not safely allow for it.

Use these steps to develop a better understanding of threatening situations. If the threat level becomes imminent and deadly, apply lethal force to neutralize the threat. *Warning shots should be used in situations where force, up to and including deadly (lethal) force, would be authorized in accordance with standing rules of engagement (ROE)/EOF. The above "5 S" principles for graduated EOF are not just applicable when responding to threats to persons, but also to threats to certain property.

The following snap TCP checklist was adapted from a checklist employed by a unit in OIF. This checklist provides guidelines ("a way") to help shape the situation at snap TCPs, facilitating an appropriate EOF response.

Reference: FM 5-0, *Army Planning and Orders Productio*n, Chapter 4, "Troop Leading Procedures."

Snap TCP Checklist	
Receive the Mission	**Status**
Receive an operations order (OPORD), fragmentary order (FRAGO), or warning order (WARNO).	
Issue initial WARNO to subordinates and include: • Type (mobile or static) • Duration • Follow-on location • Commander's critical information requirements • Initial intelligence, surveillance, and reconnaissance (ISR) tasks • Confirmation back-brief	
Perform an initial assessment: Gain/maintain situational understanding, analyze the mission based on mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC).	
Allocate time available for preparation, to include rehearsals and movement.	
Issue Warning Order	
Issue a WARNO outlining the mission including ROE and EOF and follow the five paragraph OPORD format: • Mission or nature of the operation • Time and place for issuing the order • Units or elements participating in the operation • Specific tasks not addressed by unit tactical standing operating procedures (TACSOP) • Timeline for operation	

Make a Tentative Plan	
Combine military decision-making process (MDMP) Steps 2 through 6: **Mission analysis (Follow METT-TC format)** • Mission º Commander's intent º Concept of operation º Specified, implied, and essential tasks • Enemy º Composition, disposition, strength, recent activities, ability to reinforce, and possible enemy courses of action (COAs) • Terrain and weather º Observation and fields of fire º Avenues of approach º Key terrain/road intersections º Obstacles º Cover and concealment • Troops and support available º Confirm purpose/duration º Plan and coordinate direct and indirect fire support º Coordinate explosive ordnance disposal (EOD); use 9-line EOD report format º Coordinate air reconnaissance support (if available) º Coordinate medical support; casualty evacuation º If a joint snap TCP, integrate Iraqi Army and Iraqi Police (IP) • Time available º Time required to move to, establish, search, breakdown, and move to follow-on location.	
Snap TCP Checklist (continued)	

- Civil considerations
  - Areas: urban or rural
  - Structures: built up, battle damaged, mosques, etc.
  - Capabilities: local services, fire, police, medical
  - Local population: friendly, neutral, and hostile
  - Local leaders: tribal, religious, and civic

COA development

- Analyze combat power
- Brainstorm ways to accomplish mission
- Identify snap TCP location
- Control measures (array snap TCP forces/assign responsibilities):
  - Review ROE/EOF guidance
  - Establish notice and evaluation area, traffic control area, and engagement zone
  - Establish barrier plan
  - Designate vehicle lanes
  - Assign/position search teams and search area
  - Assign/position observation posts
  - Designate 360-degree security
  - Designate overwatch positions (front and rear locations)
  - Assign sniper team(s)
  - Establish crew-served weapon locations
  - Identify detainee handling/evidence collection teams
  - Designate unit vehicle positions
  - Establish key leader position
- Develop a concept of the operation (how leader envisions mission from start to finish)
- Prepare COA statement and sketch

Snap TCP Checklist (continued)

COA analysis • Identify enemy most probable COA (example: VBIED) • Leader visualizes set of actions and reactions to enemy most probable COA **COA comparison and decision making** • Mission accomplishment • Time to execute operation • Results from unit reconnaissance • Posture force for future operations	
Initiate Movement	
Conduct convoy briefing	
Move to snap TCP location	
Conduct Reconnaissance	
Conduct digital or analog (conventional) map reconnaissance	
Incorporate intelligence products from higher	
Conduct ISR	
Disseminate updated digital reports to subordinates	
Complete the Plan	
Adjust the plan based on updated ISR effort	
Make final coordination with adjacent units/TCPs and higher headquarters prior to issuing the order	
Snap TCP Checklist (continued)	

Issue the Order	
Small unit orders normally issued verbally and may be supplemented by graphics and/or other control measures (Blue Force Tracker, Force XXI battle command, brigade and below, etc.)	
Follow 5 paragraph OPORD format	
Snap TCP Checklist (continued)	
Reinforce intent of next higher commander	
Conduct combined mission, safety, ROE/EOF briefing	
Supervise and Refine	
Conduct pre-combat checks, pre-combat inspections, and rehearsals with designated snap TCP team prior to mission execution (if possible)	
Back-brief commander or designated representative	
Execute Mission	
Search area procedures: • Establish notice and evaluation area, traffic control area, and engagement zone • Establish standoff from neighborhood structures • Establish vehicle lanes and position search teams • Post warning signs in English and local language with sufficient distance to allow drivers to react, such as: "Slow, U.S. Checkpoint" and "Stop, Take Orders From Soldiers" • Emplace physical barriers to force vehicles to slow down (spike strips, concertina wire, etc.); prepare barriers, such as tire poppers or a vehicle to block movement of vehicles attempting to continue through search area • Position interpreters with search teams	
Snap TCP Checklist (continued)	

Process detainees • In case of search refusal or demonstrated hostile intent, separate, restrain and detain individual(s) • Maintain separate area for detainees • Maintain evidence collection/property accountability (includes weapons, ammunition, explosives, and other contraband) • Secure detainee vehicles at the scene • Take statements/photo/video of scene • Process captured documents and/or equipment **Treat and process Iraqi casualties:** • Treat and evacuate casualties (medical evacuation) • Know location of nearest Iraqi/coalition hospital/clinic • Know location of nearest IP/coalition military police station • Report to higher headquarters, and continue operations as directed or move snap TCP	
EOF Procedures	
Conduct visual inspection of target for positive identification of hostile intent: use binoculars, sights, and optics	
Use audible warning signs to warn (horn, air horn, loudspeaker, flash/bang device, siren)	
Use visual aids (lights, laser pointers, flares, signs, colored flags, multi-lingual signs)	
Show weapon and demonstrate intent to use it	
Attempt non-lethal means (stop strips, physical barrier, vehicle, visual/audio signal, signs, hand and arm signals, etc.)	
Fire aimed warning shots; consider weapons caliber and effect you are attempting to achieve and strive to avoid/limit collateral damage	
Aim disabling fire at tires, engine block, etc.	
Snap TCP Checklist (continued)	

React to hostile elements and/or actions in accordance with ROE and EOF: • **SHOUT** warning to stop (Arabic: "Kiff-Armik") • **SHOW** weapon • **SHOVE**, restrain, or detain • **SHOOT** warning shot* • **SHOOT** to eliminate threat *Warning shots should be used in situations where force, up to and including deadly (lethal) force, would be authorized in accordance with standing rules of engagement (ROE)/EOF.	
Report EOF incidents to higher headquarters.	
Equipment	
Signs: (2X) Alert signs, (1X) warning sign, (1X) stop sign, (1X) stop paddle	
(5X) Sawhorses (folding) or (10X) traffic cones or (7X) warning triangles	
(5X) Bean-bag lights or similar flashing/warning lights	
(3X) Spike strips (to disable a vehicle), rolls of concertina wire, or similar vehicle disabling device	
(1X) Portable speed bump or field expedient substitute (sandbags, etc.)	
Flashlights (2 per screening team and search team)	
Search mirrors/optics, binoculars, infrared illuminators, night vision devices, telescopic thermal sights, high-power spotlights	
Signaling devices: Whistles, visible laser pointers, air horn, public-address system (megaphone), sirens, signal pyrotechnics (star clusters), colored flags	
Snap TCP Checklist (continued)	

Laminated search instructions, curfew violation warnings, contraband list, weapons policy guidelines, vapor trace/X-spray, and female search instructions	
Personnel search wands (hand-held metal detector), crowbar/tanker bar/Halligan tool	
Civilian jumper cables, tow chains, fire extinguisher	
Pre-printed instructions in local language, leaflets to explain local actions	
(20X) Detainee forms and (20X) evidence forms	
Digital camera	
(20X) Zip ties/handcuffs/flex cuffs	
(20 pair) Rubber gloves	
Landing zone (LZ)/pick-up zone (PZ) panels	
(5X) Body bags	

Table 4-1

Snap TCP Example

- **Identify** and **stop** the target vehicle
- **Cover** vehicle and occupants with direct-fire weapons (watch following vehicles for indication of remote detonation of target vehicle).
- **Maintain** standoff and use a bullhorn or public address (PA) system to **direct occupants out** of the vehicle.
- **Direct driver to open** all doors, trunk, and hood
- **Use optics to inspect** the vehicle from standoff position; maneuver, as required, to get the best angles
- **Move** occupants away from vehicle; watch for suicide bomber (vest) indicators
- **Search/apprehend** the occupants, if required. Refer to "look out" list and use vapor trace/X-spray, leaflets to explain actions, and detainee/evidence kits
- **Inspect** vehicle per TACSOP, if required, after optics inspection

Counter Vehicle-borne Improvised Explosive Device

Principles:

- **Maintain Standoff**: 50 meter minimum
- **Maintain 360-Degree Security**: You must be able to deal with approaching threats from all directions
- **Use Tactical Dispersion**: Whether mounted or dismounted, do not bunch up
- **Employ Blast Protection**: Use your vehicles, terrain, and man-made features to your advantage
- **Use EOF procedures to ID threats: ("5 S") SHOUT warning to stop (in local language and English); SHOW weapon; SHOW restraint or detain; SHOOT warning shot; and SHOOT to eliminate threat**
- **Maintain communication** with higher headquarters

TCP Drill:

- **Security:** Ensure you maintain the right balance of inward and outward focus
- **Separation**: Use loudspeakers to instruct occupants to exit their vehicles and move away.
- **Search**: Clear the vehicle from a safe distance using optics. Only approach if necessary and with minimal force
- **Set-up:** Use speed and surprise to eliminate the enemy's ability to react

Conduct IED Check ("5-25") at Every Stop

5-meter checks: Identify a halt position. Conduct a visual/physical check for a 5-meter radius around your position. Check for disturbed earth and suspicious objects, such as loose bricks, etc. Start at ground level and scan upward. Be systematic; take your time and show curiosity.

25-meter checks: Patrol leader decides to occupy an area for more than 5 minutes. Once 5-meter checks are conducted, continue scanning out to 25 meters and then move forward in teams for a 25-meter radius around your position, checking for potential improvised explosive device indicators and anything out of the ordinary.

Figure 4-1

Appendix

Traffic Control Point Smart Card

See Smart Card included with this publication.

CALL PUBLICATIONS INFORMATION PAGE

In an effort to make access to our information easier and faster, we have put all of our publications, along with numerous other useful products, on our World Wide Web site. The CALL Web site is restricted to Department of Defense personnel. The URL is http://call2.army.mil.

If you have any comments, suggestions, or requests for information, you may contact CALL by using the Web site "Request for Information" or "Comment" link. We also encourage Soldiers and leaders to send in any tactics, techniques, and procedures (TTP) that have been effective for you or your unit. You may send them to us in draft form or fully formatted and ready to print. Our publications receive wide distribution throughout the Army, and CALL would like to include your ideas. Your name will appear in the byline.

If your unit has identified lessons learned or tactics, techniques, and procedures, please contact CALL using the following information:

Telephone: DSN 552-9569/9533; Commercial 913-684-9569/9533

Fax: DSN 552-4387; Commercial 913-684-4387

NIPR Email address: call.rfimanager@leavenworth.army.mil

SIPR Email address: call.rfiagent@leavenworth.army.smil.mil

Message: CDRUSACAC FT LEAVENWORTH KS//ATZL-CTL/

Mailing Address: Center for Army Lessons Learned, ATTN: OCC, 10 Meade Ave., Bldg 50, Fort Leavenworth, KS 66027-1350.

If you would like copies of this manual or have a request for information (RFI), please submit your request at NIPR: http://call.army.mil **or SIPR:** http://call.army.smil.mil. Use the “Request Information or a CALL Product” link. Please fill in all the information to include unit name and official military address. Please include building number and street for military posts.

Additionally, we have developed a repository, the CALL Archives, that contains a collection of operational records (OPORDS and FRAGOS) from recent and past military operations. Much of the information in the CALL Archives is password-protected. You may obtain your own password by accessing our Web site and visiting the CALL Archives page. Click on "Restricted Access" and "CALL Archives Access Request." After you have filled in the information and submitted the request form, we will mail you a password. You may also request a password via STU III telephone or a SIPRNET e-mail account.

CENTER FOR ARMY LESSONS LEARNED

CALL's products are produced at Fort Leavenworth, KS, and are not distributed through publication channels. Due to limited resources, CALL selectively provides its products for distribution to units, organizations, agencies, and individuals and relies on them to disseminate initial distribution of each publication to their subordinates. Contact your appropriate higher element if your unit or office is not receiving initial distribution of CALL publications.

Installation Distribution Centers
Corps, divisions, and brigades
Special forces groups and battalions
Ranger battalions
Staff adjutant generals
TRADOC Schools
ROTC headquarters
Combat training centers
Regional support commands

CALL PRODUCTS "ON-LINE"

Access information from CALL via the World Wide Web (www). CALL also offers Web-based access to the CALL Archives. The CALL Home Page address is

http://call.army.mil

CALL produces the following publications:

BCTP Bulletins, CTC Bulletins, Newsletters, and Trends Products: These products are periodic publications that provide current lessons learned/TTP and information from the training centers.

Special Editions: Special Editions are newsletters related to a specific operation or exercise. Special Editions are normally available prior to a deployment and targeted for only those units deploying to a particular theater or preparing to deploy to the theater.

News From the Front: This product contains information and lessons on exercises, real-world events, and subjects that inform and educate Soldiers and leaders. It provides an opportunity for units and Soldiers to learn from each other by sharing information and lessons. *News From the Front* can be accessed from the CALL Web site.

Training Techniques: Accessed from the CALL products page, this on-line publication focuses on articles that primarily provide tactics, techniques, and procedures (TTP) at the brigade and below level of warfare.

Handbooks: Handbooks are "how to" manuals on specific subjects such as rehearsals, inactivation, and convoy operations.

Initial Impressions Reports: Initial Impressions Reports are developed during and immediately after a real-world operation and disseminated in the shortest time possible for the follow-on units to use in educating personnel and supporting training prior to deployment to a theater. Products that focus on training activities may also be provided to support the follow-on unit.

Support CALL in the exchange of information by telling us about your successes so they may be shared and become Army successes.

Center for Army Lessons Learned

10 Meade Avenue, Building 50
Fort Leavenworth, KS 66027-1350

FOR OFFICIAL USE ONLY