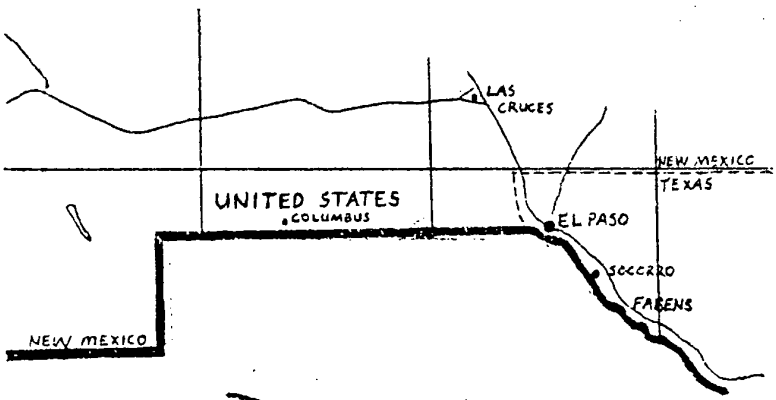
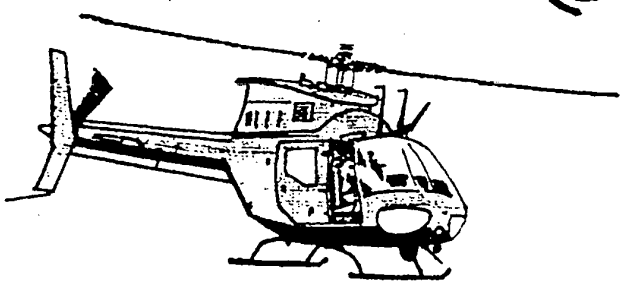
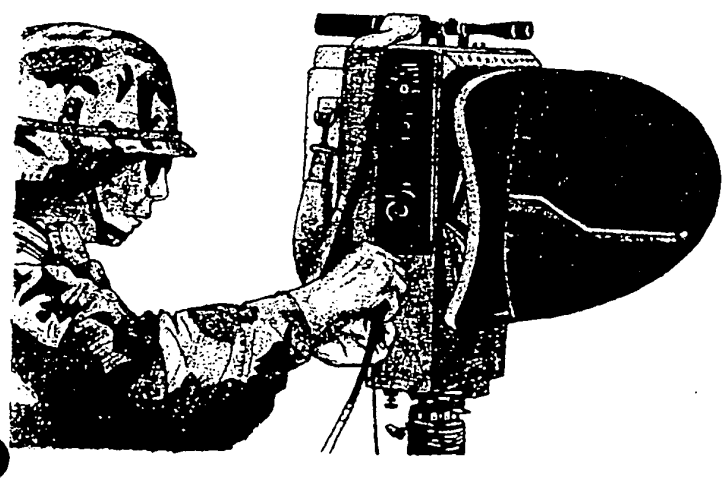
NATIONAL GUARD BUREAU
COUNTERDRUG TASK FORCE

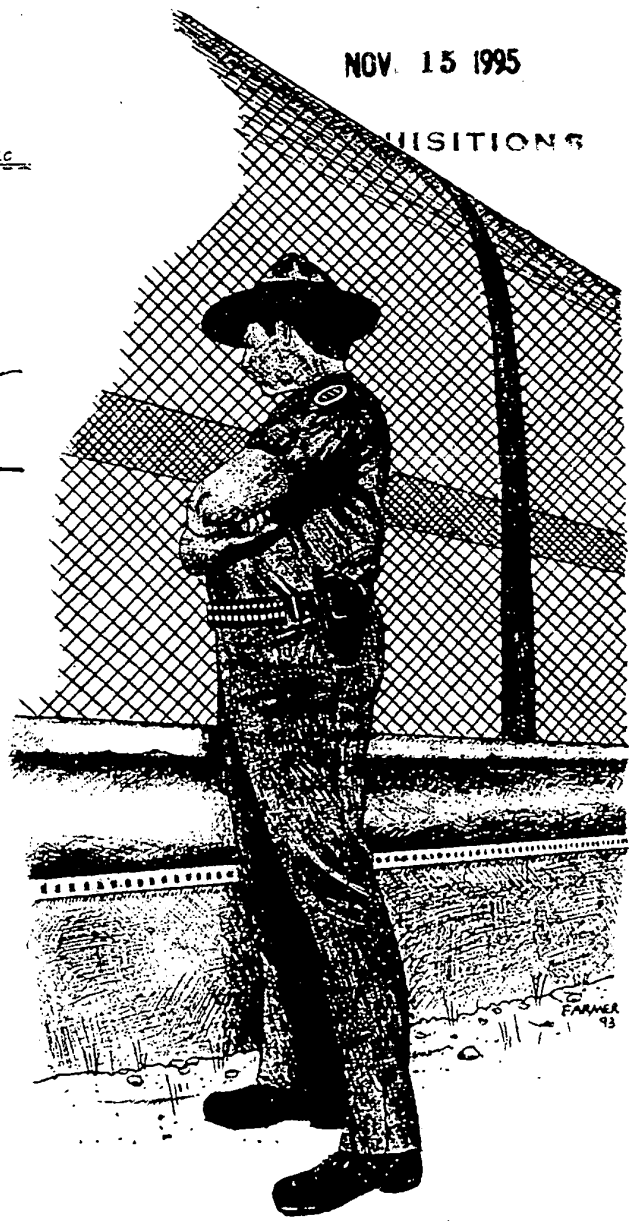
NATIONAL GUARD COUNTERDRUG LESSONS IV

1 March 1994









Compiled by: The National Interagency Counterdrug Institute

DEPARTMENTS OF THE ARMY AND THE AIR FORCE
NATIONAL GUARD BUREAU
WASHINGTON, D.C. 20310-2500

March 1, 1994

This is the fourth edition of *National Guard Counterdrug Lessons* compiled by the National Interagency Counterdrug Institute. More than 2,500 after action reports were reviewed to develop the lessons recorded in this document.

Budget constraints have made it more important than ever to ensure that counterdrug funds are wisely spent. Each state's National Guard must constantly review counterdrug support operations to improve their efficiency whenever possible. The development and dissemination of *National Guard Counterdrug Lessons* is one method of improving the quality and efficiency of our counterdrug support. These bulletins are intended to help units share successful techniques, tactics, and procedures as well as provide information on mistakes to be avoided.

While the majority of these lessons were developed from reports submitted by National Guard counterdrug support elements, I encourage other organizations to also provide input. Information from law enforcement organizations receiving counterdrug support and the active military and reserves are very welcome. Please feel free to send the National Interagency Counterdrug Institute information regarding your experiences (whether they were positive or showed that improvement is needed) with the use of military counterdrug support. Their address is listed at the back of this bulletin. The Institute will gladly facilitate this exchange of information within the counterdrug community.

I would particularly like to express my appreciation to the Interagency Operations Security Support Staff, the National Security Agency's Operations Security Education Division, and Joint Task Force Six for their contributions to this document. By helping to improve operations security, their efforts will increase the safety of counterdrug personnel and help make counterdrug support more effective.

FRANCIS J. BRAY
Director, Counterdrug
Task Force

TABLE OF CONTENTS

(*Note: The mission titles and numbers used in this document refer to the sixteen National Guard counterdrug support missions currently approved by the Secretary of Defense. For mission descriptions or further information, see National Guard Regulation (AR) 500-2/ Air National Guard Instruction 10-801 dated 30 September 1993. The mission descriptions are being reviewed for potential consolidation. New guidance may be issued for fiscal year 1995.*)

Mission #1, Surface Reconnaissance

Observation. A marijuana eradication mission covering a large area was planned using multiple helicopters to insert and extract reconnaissance and eradication teams and to sling load marijuana to destruction sites. The aircraft arrived several hours late. Although a refueler was scheduled during the initial planning conference to support the operation, it failed to show up and the aircraft were forced to fly to an airport to refuel. (Apparently, there was confusion between the various chains of command for the aircraft, the refueler, and eradication ground teams concerning mission requirements and times. Additionally, some elements made unilateral changes to the support agreed upon during the initial planning conference without informing the other units involved in the operation.)

These events caused the operation to begin a day late. Once operations did begin, the aircraft would leave the area to refuel without coordinating with ground elements. All aircraft left at the same time to refuel together, causing gaps in aerial lift support. Eradication teams would request to be inserted or extracted and discover the aircraft had left the area to refuel.

Lesson(s).

--As with any tactical operations, units, personnel, and/or equipment dedicated to a counterdrug support mission should be either attached or in direct support (DS) to the National Guard team or task force headquarters providing counterdrug support. Unity of command must be maintained. One operations order should be written for all National Guard elements providing counterdrug support during a mission in order to synchronize operations and ensure unity of command and effort. Meanwhile, the senior law enforcement agency (LEA) representative is in charge of the operation and directs supporting military elements through the senior military member present.

--Consider designating an Air Mission Commander and/or air liason officers to control/coordinate aviation operations.

--Synchronize aircraft refueling with ground team operations. Develop a refueling schedule to allow ground teams to plan for times aircraft will be out of the area. If possible, stagger aircraft refueling to provide continuous aerial lift coverage during an operation. Ensure LEAs and military personnel have continuous communications capability.

Observation. Reconnaissance (and surveillance) missions often require making detailed notes. Making such

notes using pen and paper can be difficult in a field environment.

Lesson(s). Consider the use of a small tape recorder for taking notes during reconnaissance (and surveillance) missions.

Observation. During reconnaissance prior to marijuana eradication, the terrain prevented LEA officers from communicating with their dispatch. This problem was solved by using hand-held radios in a UH-1 helicopter to provide retransmission on the LEA net between agents on the ground and their dispatch.

Lesson(s). With appropriate communications equipment, helicopters can provide effective retransmission platforms. RAID aircraft are particularly well-suited for such missions

Observation. During a large-scale, highly publicized marijuana eradication operation, local citizens patrolled the area using all-terrain vehicles and motorcycles to look for counterdrug forces. When counterdrug forces were spotted, the information was passed on to a local radio station which broadcast warnings to marijuana growers.

Lesson(s).
--Plan for operations security (OPSEC) during all counterdrug missions, including eradication. (Further information on OPSEC is located in the appendices.) If marijuana growers or their allies are broadcasting the locations of counterdrug elements, monitor the appropriate radio stations as a means to evaluate OPSEC and make adjustments in plans if necessary.
--Consider the use of reconnaissance patrols as a means of terrain denial to scare marijuana growers away from their growing areas until eradication can be accomplished. Also, consider "false insertions" to confuse growers about the counterdrug area of operations.

Observation. During an eradication operation, National Guard helicopters were used to slingload an LEA's all-terrain cycles (ATCs) into suspected growing areas. Use of the ATCs gave law enforcement officers greater range and mobility to locate and destroy marijuana growing sites.

Lesson(s). LEAs should consider the use of ATCs during eradication operations. National Guard aircraft have the capability to move a wide range of equipment into the vicinity of suspected marijuana growing sites or to support other types of counterdrug missions.

Observation. In support of an LEA marijuana eradication operation, a counterdrug support element used a reconnaissance team that had insufficient training and no prior experience in counterdrug operations. After the team

was unable to locate any marijuana, it was discovered that none of the team members knew how to recognize marijuana or the indications of a growing site.

Lesson(s). Ensure personnel are properly trained prior to deploying them on missions. The Drug Enforcement Administration has a training video for eradication operations. State National Guards should consider making this video part of mandatory training for personnel involved in eradication support.

Mission #2, Surface Surveillance

Observation. A listening post/observation post (LP/OP) deployed to a mission area with night vision goggles expecting to perform a mission only at night. Upon arrival, the team discovered the mission was actually to be performed during the day. Because they expected to operate only at night, the team didn't bring binoculars and weren't able to perform the mission at full effectiveness.

Lesson(s). Establish a standard equipment list for LP/OP missions. Since missions frequently change or may be extended, bring a standard equipment load to enable operations in all light conditions and likely weather.

Observation. During an LP/OP mission, suspected smugglers used what appeared to be scout vehicles to test for the presence of law enforcement forces before sending vehicles actually carrying drugs (load vehicles) across the border. The LP/OP team reported the vehicles crossing the border and the law enforcement response team acknowledged in the clear. When the LP/OP made their observation report over the radio, a vehicle following the two scout vehicles immediately turned around and re-crossed the border. Law enforcement officers stopped the scout vehicles and found each contained a two-way radio and a scanner tuned to the LEA's frequency.

Lesson(s).

--Communications security (COMSEC) should be a priority during counterdrug operations. Assume that any message transmitted in the clear will be monitored by drug traffickers. (See the appendices for further information on OPSEC planning.)

--Locate LP/OP positions and plan named areas of interest (NAIs) in depth to counteract the use of scout vehicles preceding load vehicles. Good counterdrug intelligence preparation of the battlefield (CDIPB) can help identify countermeasures for drug trafficker attempts to avoid law enforcement actions. (For more information on CDIPB, see *National Guard Counterdrug Lessons II*, dated 7 January 1993 and *National Guard Counterdrug Lessons III*, dated 11 July 1993.)

Observation. A military counterdrug support element conducting a mission was unable to communicate operational information to the headquarters of another counterdrug support unit. One of the counterdrug support elements had a STU-III phone with them, but not the "Secret" crypto key.

Lesson(s). Information concerning ongoing counterdrug operations should only be sent using secure transmission, to include the use of the telephone. (See the appendices.) Communications planning should include secure communications with the supported LEA as well as higher and adjacent military units.

Mission #4, Aerial Reconnaissance

Observation. At the last minute, an LEA receiving support reduced the number of law enforcement officers who were designated to fly on a mission. Due to the number of passengers in the original support request, a UH-1 had been scheduled to fly the mission with the crew in a counterdrug active duty special work (ADSW) status. Following the change in the number of passengers, an OH-6 would have been a more appropriate and more economical aircraft. An OH-6 and crew was available; however, the State Aviation Officer (SAO) could not be reached and the flight facility commander did not have authority to change the aircraft. Despite the higher operating costs, the mission had to be flown in a UH-1.

Lesson(s).

--When practical, a liaison officer should contact the supported LEA to confirm mission requirements in time to make any necessary changes.

--Consider delegating the approval authority for changes in counterdrug mission aircraft to facility commanders or other appropriate individuals when the SAO is absent or unavailable.

--Use of an Air Mission Commander or liaison officer can facilitate planning and eliminate many of the coordination problems that can affect counterdrug support.

Observation. An air reconnaissance mission was disrupted because a flight facility commander refused to refuel a RAID aircraft because of concern that his account would not be reimbursed by counterdrug funds.

Lesson(s). Refueling arrangements must be planned and coordinated in advance, even when using army aviation support facilities.

Observation. A crew that had never before flown counterdrug support was assigned to fly an air reconnaissance mission. The law enforcement officers on the mission had previously flown with a crew experienced in counterdrug support and felt the new crew "didn't know what they were doing and were

uncooperative, flying too high and too fast" to accomplish the mission.

During another mission (Surface Surveillance), an aircraft was used to insert a LP/OP team. In response to intelligence gathered by the supported LEA concerning a pending drug delivery, the team was to observe a clandestine airstrip. Despite the LP/OP team leader's instructions to the pilot, the aircraft flew over a nearby campground then placed the team directly on top of the planned LP/OP site in full view of the campground. No suspected drug activity was noted by LP/OP team.

Lesson(s). The pilot-in-command retains control over the aircraft and has final determination over the flight profile. However, counterdrug missions often entail special considerations that may differ from the training mission flights performed by most National Guard aviators. States should consider establishing counterdrug specific training, or at a minimum provide a counterdrug flight operations briefing before crews are assigned to fly counterdrug support missions.

Observation. A LEA requested two hours of flight time for an aerial reconnaissance mission. The mission would have actually required five hours to properly complete. Because of the two hour request, not enough blade time had been allotted to the mission to satisfy the LEA's requirements.

In another mission, an LEA requested "a Huey" to perform aerial recon-naissance for marijuana growing areas. Without performing a mission analysis, a UH-1 and crew was provided and used almost seven hours of blade time. An OH-58 would have been better suited for the mission and considerably cheaper to operate. However, it wasn't what the LEA asked for.

Lesson(s).

--Encourage LEAs to request a capability (i.e., "an aerial recon of fifty square kilometers between Mudville and Tinseltown to search for marijuana,") or mission type (aerial reconnaissance) rather than a specific piece of equipment or amount of blade time.

---If possible, use a liaison officer to assist LEAs in determining military support requirements and developing mission requests.

Observation. Prior to using aircraft for marijuana reconnaissance, the LEA observer performed a map reconnaissance to identify areas of likely cultivation and coordinated with other LEA agents assigned to those areas to develop air mission priorities. This procedure allowed the LEA observer and aircraft pilot to thoroughly plan the mission, pay extra attention to the areas of highest priority, and conserve blade time. Both the LEA and the National Guard aircrew providing support felt this mission was considerably more productive and efficient than previous air reconnaissance missions performed with little prior planning.

Lesson(s).

--LEAs and supporting National Guard counterdrug elements should conduct

intelligence preparation as part of the planning process for air reconnaissance missions. Pay particular attention to evaluating the area to be reconned and (if possible) use intelligence from law enforcement agents assigned to the area to help identify locations likely to contain illegal activity.
--Pre-mission coordination between aircraft pilots providing counterdrug support and supported LEA officers can make aerial reconnaissance more efficient and conserve blade time. An hour of pre-mission planning on the ground is well-spent if it results in saving even a few minutes of blade time.

Observation. During a marijuana eradication operation, a single UH-1 was used to identify marijuana, insert and extract eradication teams, and perform slingload operations. The time required to identify marijuana growing sites and then perform eradication enabled some growers to harvest their plants before eradication teams got to them.

Lesson(s).
--Consider using a separate, dedicated aircraft (an OH-58 is usually best) to scout for marijuana while a heavier aircraft (UH-1 or UH-60) performs eradication team insertion/extraction and sling loading. While requiring more aircraft, this technique may result in a lower total blade time requirement and/or lower total aircraft operating costs.
--Consider rappelling as a means to insert eradication teams.

Observation. Marijuana eradication operations were disrupted because the aircraft providing support was forced to leave for scheduled maintenance in the middle of the mission.

Lesson(s). When planning aerial lift support, check scheduled maintenance requirements when determining aircraft availability.

Observation. A military aircraft was assigned to support an LEA with aerial reconnaissance. By the time the aircraft departed its airfield, picked up the LEA observer at another airport, and arrived at the area to be reconned, half the blade time allotted to the mission had been consumed and the aircraft had to return without completing the reconnaissance.

Lesson(s). Consider ferry time (the travel to and from the mission site) when planning blade hours for counterdrug support missions. Also, it may be more cost effective to drive passengers to a central airfield rather than schedule several different pick-ups with aircraft.

Observation. An observer was assigned to an aerial reconnaissance mission for the first time. This mission was his first experience in aerial operations. Once the mission began, the

observer had difficulty navigating from the air but didn't say anything until he had been lost for a considerable period of time. The aircraft pilot, assuming the observer would handle navigation, didn't pay attention to the planned route prior to takeoff.

Lesson(s).
--In concert with the LEA observer, aircraft pilots should routinely perform a map reconnaissance of routes and areas prior to every flight.
--Prior to takeoff, pilots and LEA passengers should review the flight plan and mission profile together. At a minimum, they should agree on the area to be reconned, routes for getting there, and the altitude during the reconnaissance. Address special considerations, such as any concern that suspects will be aware that the area is being reconned. Planning time spent on the ground will pay off in the air.

Observation. A National Guard UH-1 was used to provide support to several LEA passengers during an aerial reconnaissance. Due to a limited number of intercom jacks, the aircrew could not provide all LEA passenger/observers with headphones.

Lesson(s). Consider using a removable aircraft intercom system to provide communications for all LEA passenger/observers.

Observation. A National Guard helicopter carried several LEA passengers to perform aerial reconnaissance of multiple areas. Because law enforcement officers interested in the same area sat on opposite sides of the aircraft, the pilot had to either directly overfly an area or make more than one pass to allow all LEA passengers to see each area of interest. Direct overflight and multiple aircraft passes increased the chance that suspects would be warned of future counterdrug operations and consumed additional blade time.

Lesson(s).
--Have law enforcement officers interested in a certain geographic area sit on the same side of an aircraft. Consider seating arrangements as part of pre-mission planning and coordination.
--When possible, observe areas targeted for aerial reconnaissance from a standoff distance, rather than flying directly overhead, to reduce the possibility of detection by persons engaged in illegal drug activity.

Mission #5, Aerial Surveillance

Observation. A National Guard RAID aircraft with a law enforcement observer provided support using LORAN to determine position while law enforcement officers in vehicles on the ground used a global positioning system (GPS). The aircraft was unable to effectively communicate positions to the LEA ground team because the location given by LORAN was several kilometers off from the position provided by the GPS.

In another mission, two RAID aircraft had difficulty determining the location of a suspected marijuana site because the locations given by LORAN in each of the aircraft differed by more than a kilometer.

Lesson(s). In many cases, LORAN navigation will not have the precision necessary for aerial surveillance operations. Consider the use of hand-held GPS in the aircraft or the use of street maps to communicate locations between aircraft and ground teams.

Mission #8, Cargo Inspection

Observation. Personnel from a military unit provided portable generators, light sets, and a command post (CP) van to support an LEA traffic checkpoint operation. One of the two generators wouldn't start at the beginning of the mission due to battery failure; a slave cable was not available. The generator that did work was not properly wired to run a light set. The majority of the personnel assigned to the mission did not know how to set up the CP van. The soldiers were billeted in a motel forty-five minutes away and worked twelve hour shifts. Most set-up and other physical labor requirements occurred when only one shift was on duty.

Lesson(s).
--Test equipment prior to deployment on counterdrug support operations and ensure all personnel are properly trained (and licensed if necessary) to operate it. Perform a train-up or practice exercise before conducting missions requiring a complex set-up or a large amount of equipment.
--Schedule shifts so that overlap occurs during periods when manual labor requirement are at their peak.
--Prior to deployment, ensure equipment is properly configured for the desired use. Plan for contingencies in case of equipment failure.

Mission #10, Aerial Photo Reconnaissance

Observation. A C-130 was used as a platform for aerial photography. Because of its operating altitude, the supported LEA felt the aircraft provided better OPSEC and drew less attention from suspects than previous missions using helicopters.

Lesson(s). The C-130 can be an effective platform for photo reconnaissance missions.

Observation. A LEA requested aerial photographs of a certain area. While processing the support request, the Air National Guard unit providing support discovered the area had been previously photographed at the request of another LEA. New prints were made from the results of the previous mission,

satisfying the LEA's requirements without the need for additional flights.

Lesson(s). Maintain the negatives from photo reconnaissance missions and develop a reference file. Refer to previous missions before committing resources to fly new missions.

Mission #12, Marijuana Greenhouse/ Drug Laboratory Detection

Observation. During a marijuana eradication operation, a two-man team was dedicated to identify areas for eradication of ditchweed prior to employment of the "main force." Once eradication teams reached the growing sites, the recon team left to find the next site. This procedure appeared to save time and make more efficient use of the eradication team.

Lesson(s). Consider the use of a dedicated reconnaissance element to identify marijuana growing areas and to guide eradication teams to their location.

Mission #14, Administration, Information, Logistics, and Maintenance Support

Observation. A National Guard element provided an expandable van, generators, and lighting to support an LEA traffic checkpoint. The individuals providing support wore civilian clothes, making it difficult for officers of the supported LEA to distinguish National Guard personnel from the general public. The inability to quickly identify National Guard support personnel made coordination more difficult and may have posed a safety hazard.

Lesson(s). Carefully review plans that call for the use of Guard members in civilian clothes. If the supported LEA requests that Guard members do not wear uniforms, consider other methods of identification such as raid jackets, distinctive baseball caps, etc. If the supported LEA is concerned about the combative appearance of BDUs, consider the use of Class B uniforms or coveralls.

Operations Security (OPSEC)

Observation. Most law enforcement officers and military personnel perform OPSEC as a normal part of their operations; however, many law enforcement organizations and military units providing counterdrug support do not have an effective OPSEC program. The lack of OPSEC can allow drug traffickers to discover and evade counterdrug efforts and may also result in increased risk to counterdrug personnel.

Lesson(s). (*Note: The following is not intended to provide a complete review of OPSEC planning and requirements. It focuses instead on only those aspects of OPSEC that may be pertinent to joint counterdrug*

operations, especially areas that may be of interest to law enforcement agencies receiving counterdrug support. For more information on OPSEC, see DOD Directive 5205.2, DOD Operations Security Program or Army Regulation 530-1, Operations Security (OPSEC).)

During counterdrug operations, OPSEC is a process used to prevent drug traffickers* from determining counterdrug force capabilities and intentions and thus evade law enforcement actions or present a risk to counterdrug personnel.

Prior to conducting a raid on a drug house, for example, law enforcement officers will want to prevent the suspects from being "tipped off" before the raid. The officers planning the raid will keep their details of their plans from personnel without a "need to know." Other OPSEC measures may include keeping regular uniformed patrol officers out of the area prior to the raid in order to avoid scaring the suspects off, using secure communications to prevent suspects with scanners from discovering the impending raid, and conducting pre-raid surveillance in a covert manner to prevent suspects from discovering they are being observed. Another example of OPSEC during law enforcement operations is keeping backup officers out of sight or in disguise during "sting" operations.

Each counter-drug organization or task force should assign a specific individual, preferably with both operations and intelligence analysis experience, to perform the functions of OPSEC planner.

The OPSEC process consists of three elements:

a) identification of counterdrug actions that drug traffickers can observe or detect by drug trafficker intelligence systems;

b) determination of indicators that might help traffickers identify counterdrug force capabilities and intentions in time to avoid drug seizures and arrests; and

c) selection and implementation of measures to eliminate or reduce the vulnerability of counterdrug forces.

Planning for OPSEC involves eight steps. Depending on the nature of the operation, these steps may be either brief or performed in detail:

1. Determine critical information.
2. Identify OPSEC indicators.
3. Determine OPSEC vulnerabilities.
4. Devise OPSEC measures.
5. Prepare OPSEC plans.
6. Brief participants.
7. Perform OPSEC measures and monitor the situation.
8. Perform OPSEC follow-up.

Determine Critical Information, which consists of specific facts that drug traffickers would find useful in evading or disrupting counterdrug actions. Most information pertaining to law enforcement and counterdrug operations is unclassified, but extremely sensitive. To determine critical information, the OPSEC planner must think like a drug trafficker and ask: "If I were a drug trafficker, what would I want to know about potential law enforcement activities?" Obvious examples include:

--"Am I under surveillance?"

*The term "traffickers" in this section includes personnel involved in the production and distribution of illegal drugs as well as smugglers.

--"Are the cops planning to raid my drug lab?"

--"Will any law enforcement personnel be in the area when I smuggle my drugs across the border?"

--"What profiles are the U.S. Customs Service using to select vehicles and cargo containers for secondary inspection?"

Critical information will be different for each counterdrug operation. The working aid in the Appendix A gives useful ideas for determining counterdrug critical information.

Identify OPSEC Indicators. They are counterdrug force actions that drug traffickers can observe, or gain knowledge of through open sources such as newspaper articles or public records, then piece together to discover critical information; they are clues to counterdrug force plans, capabilities, and vulnerabilities. Examples could include the appearance of "strangers" in town with military hair cuts and/or rental cars, a change in uniformed patrol patterns within an area, the emplacement of remote sensors, and the presence of military personnel and equipment at a law enforcement agency headquarters.

The OPSEC planner prepares a list of OPSEC indicators and estimates drug traffickers' capabilities to collect information and intelligence. Considerations include drug trafficker ability to monitor counterdrug force communications, ability to observe counterdrug force movements--particularly through the use of night vision devices and enhanced optics, and the ability to detect counterdrug force use of radar and remote sensing devices. The list of indicators, the determination of critical information, and the results of the estimate of traffickers' intelligence and information collection capabilities is provided to members of the counterdrug team for the upcoming operation as preliminary guidance for OPSEC planning.

Determine OPSEC Vulnerabilities. These are conditions in which drug traffickers may obtain indicators concerning counterdrug force actions in time to evade or disrupt the planned operation. After receiving the initial OPSEC planning guidance, all members of the counterdrug force should visualize the planned operations from beginning (including the planning and coordination stage) to end determine OPSEC vulnerabilities.

Devise OPSEC Measures. These are methods and actions taken to prevent drug traffickers from discovering critical information. Such measures include use of secure communications, limiting information to those individuals with a "need to know," and ensuring mission participants do not engage in "loose talk." One standard measure is to protect the identities of counterdrug support personnel from release to the public.

Prior to implementing OPSEC measures, the OPSEC planner should perform a risk analysis to compare the expected costs of a measure (e.g., lodging counterdrug support troops in a motel several miles away from the mission area, the purchase of secure communications equipment, etc.) with the risk of mission compromise if the measures are not taken (e.g., traffickers may discover the presence of soldiers or might monitor counterdrug communications).

An **OPSEC Plan** is prepared and used to **Brief Participants**. The plan should address the information determined to be critical, OPSEC indicators, the estimate of drug traffickers' intelligence collection capabilities, OPSEC vulnerabilities, and the selected OPSEC measures and responsibilities for implementing them.

Performance of OPSEC Measures takes place in accordance with the OPSEC plan. **Monitoring the Situation** is a continuous process of evaluating the effectiveness of OPSEC measures. Based upon the feedback obtained through OPSEC monitoring, counterdrug personnel may need to reinforce or adjust OPSEC measures to protect critical information.

OPSEC Follow-Up reviews the effectiveness of OPSEC plans. Key participants should be briefed on the success or failure of OPSEC efforts. After action reviews and reports should routinely address OPSEC effectiveness. Lessons learned concerning OPSEC are the basis for improvements in the counterdrug force OPSEC planning process, and should be shared.

It is especially important to use OPSEC lessons to validate OPSEC training programs. A force that is educated about OPSEC is less likely to inadvertently compromise their mission. Training and education is the most cost-effective security measure to implement.

Appendix A

WORKING AID FOR LAW ENFORCEMENT AGENCY CRITICAL INFORMATION

Overview. The following working aid was designed to prompt operation planners to identify and assess the critical information aspects of counterdrug operations during the planning stage. Its proponent is the Interagency OPSEC Support Staff, which includes representatives from several federal law enforcement agencies. The working aid is purposely non-specific because every operation is different, each organization and agency has unique concerns, and every location and target has a different operating environment. It is not intended to constitute official guidance--the supported law enforcement agency retains the lead for making decisions concerning counterdrug operations while National Guard personnel will remain in a support role.

The working aid approaches the overall concept of critical information at two levels that are not mutually exclusive: Basic Operations (typified by many DEA and task force operations), and National Level Operations (such as joint task forces that combine Department of Defense and federal law enforcement agency assets). Within each of these two levels are three subgroups of information that may be relevant to an operation: activity-specific information, people-specific information, and support activity-specific information.

The following charts are provided:

- Activity-Specific Information
- People-Specific Information
- Administration and Support Activity Information
- National Operations Vulnerabilities
- Example Drug Trafficker Intelligence Collection Strategy

WORKING AID FOR LAW ENFORCEMENT AGENCY (LEA) CRITICAL INFORMATION

Developed by

Anne Brooker-Grogan, OCP
National Security Agency
National Cryptologic School, OPSEC Education Division

Introduction

There is an on-going requirement in the law enforcement community for guidance as to what should be considered sensitive and critical information according to the OPSEC process. To help meet this need, this working aid provides information and ideas for counterdrug (CD) planners to use in the OPSEC process.

The main advantage of applying OPSEC to law enforcement and counterdrug activities is the unique insight provided through the use of the adversary point of view.

Encouraging operations and OPSEC planners to think like criminals, traffickers, and other prime targets should enhance overall effectiveness of law enforcement assets and increase the probability of operational success where maintaining essential security and achieving the factor of surprise often plays a crucial role.

Definitions

Operations Security (OPSEC) is the process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with the planning and conduct of friendly operations and other activities.

Critical Information consists of specific facts about friendly capabilities and intentions that may be used by an adversary to counter and defeat counterdrug operations.

Indicators are friendly observable actions and open source information that can be interpreted and pieced together by an adversary to derive critical information.

Guidelines

Most information pertaining to law enforcement and counterdrug activities is unclassified, but extremely sensitive. Such information in the hands of an adversary could easily compromise operations and result in loss of life or failed operations.

This working aid is UNCLASSIFIED.

Basic Operations

Examples Basic federal law enforcement operations are planned and executed utilizing known techniques for surveillance and information gathering. Areas that should be evaluated for critical information at this basic level of activity include:

* activity-specific information
* people-specific information
* support activity-specific information

ACTIVITY-SPECIFIC INFORMATION	EXAMPLES
CURRENT AND FUTURE INVESTIGATIONS	COVER NAMES ASSOCIATED WITH THE ACTIVITY PERSONS, PLACES, THINGS INVOLVED SCHEDULES, OBJECTIVES, GOALS IDENTIFYING LEADING ORGANIZATION ISSUE OF SEARCH/ARREST WARRANTS
SCOPE OF ACTIVITY OR OPERATION	INVOLVEMENT OF OTHER FEDERAL AGENCIES INVOLVEMENT OF MILITARY SERVICES STATE/LOCAL LEA INVOLVEMENT INTERNATIONAL LEA INVOLVEMENT
SPECIAL ASSETS OR EQUIPMENT IN USE	USE OF TRADITIONAL WIRETAPS USE OF ELECTRONIC SURVEILLANCE EQUIPMENT USE OF AIRBORNE ASSETS USE OF BUGS, TRACKING DEVICES USE OF HIDDEN CAMERAS USE OF WIRES ON CIs/OTHERS USE/IDENTITY OF COVERT VEHICLES MAINTENANCE SCHEDULES/REQUIREMENTS SPECIAL LOGISTICAL REQUIREMENTS AIRCRAFT PAINT SCHEMES/TAIL NUMBERS AIRCRAFT FLIGHT PLANS BOAT NAMES/HULL NUMBERS AUTHORIZATION TO USE SPECIAL EQUIPMENT FLIGHT PLANS ON FILE WITH THE FAA

Comment Planners should be aware of any special logistical requirements that are associated with an operation. Certain resources are unique to specific equipment or systems, or may even be associated with a specific agency.

Example When an agency has a skilled technician whose services are often in great demand to support "really important" high-visibility operations--that person becomes linked to that agency, and his/her presence is an indicator of agency involvement in a significant operation ("...when they care enough to send the very best...").

PEOPLE-SPECIFIC INFORMATION	EXAMPLES
PERSONAL INFORMATION	NAMES/COVER NAMES AGENCY/ORGANIZATIONAL ASSOCIATIONS ASSIGNED PARKING SPACES UNDERCOVER IDENTITIES PHONE/PAGER NUMBERS ADDRESSES/LOCATIONS VEHICLE DESCRIPTIONS/LICENSE NUMBERS PHYSICAL DESCRIPTIONS FAMILY INFORMATION ANY INFORMATION ABOUT CIs HISTORY OF OFFICIAL TRAVEL PASSPORT/VISA INFORMATION
SCHEDULE INFORMATION	DUTY ROSTERS BREAK SCHEDULES OVERTIME PAPERWORK TIMES/PLACES OF SCHEDULED MEETINGS TRAVEL PLANS/ITINERARIES TIMES/LOCATIONS OF OPERATIONS COMMUNICATIONS CHECK-IN SCHEDULES TIMES/PLACES OF ANY OTHER SPECIAL EVENTS
COMMUNICATIONS DATA	TYPES OF COMMS AVAILABLE RADIO CALLSIGNS PAGER INFORMATION CELLULAR PHONE NUMBERS 'COVER' TELEPHONE NUMBERS

Comments Although much of this information would seem to be well-protected, this is the type of miscellaneous information that is most likely to be disclosed inadvertently over telephone or radio and in casual conversation.

Analysis of COMSEC monitoring of various law enforcement agencies has yielded extensive information that produces a picture of people and activities.

Example 1 One case on record shows where a criminal compiled information on federal, state, and local law enforcement personnel through monitoring unprotected radio communications, and supplemented the dossiers that he compiled with photographs of residences, vehicles, and family members. Fortunately, these files were seized before they were made available to other members of the criminal element.

Example 2 Another area that is of great concern to LEAs is the protection of Confidential Informant (CI) sources--a compromise of information that reveals their identity can lead to reprisal against the CI, frequently resulting in a loss of cooperation from that CI, and therefore, loss of the intelligence source to the LEA.

SUPPORT ACTIVITY INFORMATION	EXAMPLES
ADMINISTRATIVE SUPPORT	SENSITIVE DOCUMENT PREPARATION PAYROLL INFORMATION OVERTIME RECORDS AND REQUESTS TRAVEL PLANS AND RECORDS PASSPORT/VISA INFORMATION SPECIAL BANK/CREDIT CARD ACCOUNTS TELEPHONE BILLS LICENSING OF COVERT VEHICLES PARKING FACILITIES FOR COVERT VEHICLES PARKING PERMITS/GARAGE PASSES LEASING SPACE FOR SPECIAL OPERATIONS PERSONNEL FILE INFORMATION ORGANIZATION CHARTS CONTRACT INFORMATION DEALINGS WITH D.A./U.S. ATTORNEY'S OFFICES EXTRADITION REQUESTS
COMMUNICATIONS SUPPORT	TYPES OF COMMUNICATIONS AVAILABLE CALLSIGN INFORMATION COMMUNICATIONS STRUCTURE/PROCEDURES COMMS ASSOCIATED WITH SPECIFIC AGENCY SPECIFIC PROBLEMS WITH COMMUNICATIONS KNOWN EQUIPMENT VULNERABILITIES OUTAGES RANGE LIMITATIONS LIMITED SECURE/PROTECTED ASSETS UNIQUE COMMUNICATIONS/SIGNALS
LOGISTICAL SUPPORT	MAINTENANCE SUPPORT FOR COVERT EQUIP AIRCRAFT/BOAT VEHICLE MAINTENANCE STORAGE FOR LARGE EQUIPMENT STORAGE/DISPOSITION OF SEIZED ASSETS RESERVED VEHICLES PARKING SPACES SERVICE ACCOUNTS FOR CELLULAR PHONES SERVICE ACCOUNTS FOR PAGERS CONTRACTS FOR LOGISTICAL ITEMS HOUSING FOR PERSONNEL IN TDY STATUS

Comments The potential for compromise among LEA (and military) administrative support activities is high. Many of these support personnel are in traditionally low-paid, low-profile jobs and are usually low on the priority list for training. These are the people that are key to a successful law enforcement OPSEC program, and should be a priority for OPSEC training and awareness programs.

Guidelines New legal rules, new technology, and new responsibilities cause constant change within the law enforcement community, especially at the street level. For this reason, each operation must consider OPSEC on a case-by-case basis, as there is no such thing as a standard LEA operation.

National Operations

Introduction This section addresses situations and challenges that would be found in a national, international, or Joint Task Force activity. The material in this section and that introduced in the Basic Operations section are NOT mutually exclusive.

Technology Specific technology applications that are in use or are planned for use in future operations. Also relevant to this category are types of technology that are in use, or are being considered for use, and their actual or potential applications.

Protecting LEA involvement with research and development efforts in these fields and procurement/acquisition data about such technologies should be a priority.

Example An example of this concern could be the use of Global Positioning System technology to track a shipment of contraband.

Resources The number, capabilities, dispositions, and availability of resources available for counterdrug detection and interdiction. An observable shortfall of support assets may tip off a limited capability and reduce the effectiveness of an activity's mission.

Example How many planes, boats, helicopters, personnel, etc. are available to look for and catch traffickers? How fast can they go? How far can they see? Where are they located (or based)? Are they functional, and if not, when might they become operational?

Communi-cations Communications are often the weakest link in an operation and should be examined closely. Planners should look at communications very closely, and spend extra time and effort in coordinating the communications equipment support for an operation. A good communications plan may be able to compensate for weaknesses in other areas, but deficient communications may compromise an otherwise well-planned operation.

Example

The scope of communications security concerns should include:

* the types of communications gear in use
* the disposition of those assets
* the capabilities of the particular communications equipment
* any inherent problems or limitations of the gear

Procedures for the use of all modes of communications should be examined. Patterns of use can be used as an indicator of impending activity by an adversary (e.g., "go secure just before...", "check in every hour on the hour," etc.). Patterns of radio silence may also be indicators.

The allocation of radio frequencies may be exploitable by an adversary and should be an item of concern to planners.

Comment

Planners seeking the factor of surprise should consider "borrowing" frequencies from other non-LEA agencies for brief periods to deceive those adversaries who have the known lists of assigned LEA frequencies programmed into scanners and receivers.

Organizations using protected/encrypted communications need to address interoperability concerns, as all participants should be able to communicate securely.

Secure Comms

The use of secure or protected communications can be a great benefit but also a potential liability. Planners need to track the dispositions, extent of use, types, and interoperability issues associated with secure communications.

The presence of encrypted communications on the air is an indicator of LEA and/or military activity. Encrypted communications on known LEA assigned frequencies have been used in the past as a barometer of LEA activity.

Encrypted signals from various equipment have very unique characteristics and can be identified and tied to specific organizations.

Encrypted communications can also be monitored for the volume of radio traffic--occasional transmissions would indicate a low level of activity, whereas a burst of activity would be a heads-up that something was happening or about to happen.

The use of low probability of intercept equipment along with encryption may decrease some of the above risks.

Comment

The most secure form of communication is no communication at all. However, the costs of reduced ability to coordinate and the reduction in tactical flexibility must be weighed against the benefits of restricting this potential indicator.

Task Force Makeup

Composition of special groups or task forces. Identification of the main participants of a joint task force or special operation makes the job of an adversary easier, as the adversary may already have personnel lists or have associated certain organizations or persons with specific activities or special operations.

Knowing details about the LEA (and supporting military) organizational structure and hierarchy would be useful to an adversary, as the presence or absence of known high-ranking personnel could easily be an indicator.

Sources and Methods

ANY details about our intelligence gathering/collection/analysis capabilities, and most importantly, HOW MUCH WE KNOW ABOUT A TARGET!

Divulging intelligence sources and methods can not only compromise national-level intelligence assets, but may also endanger personnel and upset delicate diplomatic arrangements. What we know and how we know it is the essence of intelligence, and as such, should be protected as extremely sensitive (or even classified) information.

Schedules

Places/dates/schedules/itineraries related to operations. Dates can be implied through a number of different information sources that are very effective indicators.

Travel and lodging arrangements can accurately reflect an operation's timetable.

Time sensitive procurement activities, required legal documents, and other logistical requirements such as rented spaces and vehicles can indicate schedules and agendas.

Casual references to personal schedules made via radio or telephone can provide tip-offs to activity schedules.

Known Vulner-abilities

Where and what are our **known** vulnerabilities. This is an extremely sensitive subject area, especially vulnerabilities that could result in single point failure of an operation.

Vulnerabilities include areas of limitations and weaknesses associated with other LEA resources, such as boats, aircraft, vehicles, communications, radar coverage, available intelligence, and other critical areas.

Support Elements

Specific links with support activities. Many federal LEA assets rely on non-LEA or non-federal support facilities to make their missions possible. These include military or civilian installations, military/civil airfields, commercial/official marinas, state and local LEA facilities, etc. Many of these facilities are not enthralled with the idea of being closely associated with a counterdrug or other LEA function and would like their association to be kept low-key.

Personnel at these support locations may also present an OPSEC threat by insisting on posted work schedules, including advance notification of overtime or late work hours, as well as other formalities that the LEA community has traditionally overlooked.

Warrants

As a legal document, the warrant is essential to the search, arrest, and prosecution of criminals. The warrant has a number of aspects of sensitive information that are unique to the law enforcement process.

The existence of a warrant is an indicator of an operation that is close to completion--the LEAs feel that they have sufficient evidence to take the case to court and are able to convince a judge or magistrate of this fact.

The warrant document contains what may be sensitive information:

* the full name of the person to be arrested
* the address of the property to be searched
* the nature of the crime committed or suspected
* the scope of the search
* a detailed account of the source of information
* why there is reasonable cause to take the case to court

The time constraints placed upon the warrant by the issuing authority are also considered sensitive (prior to serving the warrant). Warrants are handled by a large number of people during the course of preparation, granting and serving, so many people potentially have access to this information.

There is a real concern about protecting sources and methods of information, particularly in the case of a CI. The affidavit for the warrant details exact dates, times, and places that the CI observed the reported activities. This information is frequently detailed enough that the person who is the subject of the warrant can determine the identity of the CI and take measures to suppress or retaliate against the CI.

Cover and Deception

Details concerning cover and deception. If there are counterdrug personnel in a foreign country, their cover must be protected. This includes:

* identities
* affiliations
* locations
* associations with U.S. and other nations' agencies
* contacts with foreign national informants
* means of reporting
* schedules for reporting
* specific targets
* purpose for being in the country
* special assets and means available to them

Additional care and planning are mandated for an operation that involves some sort of deception activity. A deception must **not** have any detectable flaws.

Planners should also bear in mind that a deception that worked very well before may not work a second time, as an adversary may have figured out what we did and how we did it. Also remember that deceptions may not transplant well between different countries, cultural groups, and operational environments.

Note

If used with care and great caution, deceptions are a very effective tool but need to be planned exhaustively by <u>all</u> parties involved.

The use of military personnel for deception operations must receive careful legal review, preferably including a military attorney, prior to the operation. Military counterdrug support personnel are prohibited from working undercover. Deliberate release of misinformation by military personnel is also generally prohibited. An example of anacceptable use would be to have military personnel support a high visibility surveillanceor reconnaissance mission as terrain denial on one part of the border in order to channel potential drug traffickers into a different area where law enforcement interdiction is actually planned to take place.

Example of Hostile Collection Strategy

WHAT THE TRAFFICKER NEEDS TO KNOW...	HOW THEY CAN FIND OUT...
KNOW THAT THERE ARE DEDICATED INTERDICTION ASSETS	INFORMATION READILY AVAILABLE THROUGH OPEN SOURCE MATERIAL AND OBSERVATION
KNOW THE DETECTION AND MONITORING AREAS OF OPERATION	SOME INFORMATION FROM OPEN SOURCES HUMINT SOURCES COMMUNICATIONS MONITORING OF RADIOS VISUAL OBSERVATION OF SHIPS AND PLANES
KNOW THE CAPABILITIES OF THE DETECTION AND MONITORING RESOURCES	HUMINT SOURCES ANALYSIS OF COMMUNICATIONS PATTERNS ANALYSIS OF SCHEDULES OPEN SOURCE MATERIAL KNOWLEDGE OF PROFILES USED BY LEAs
KNOW WHEN CD RESOURCES ARE NOT AVAILABLE AND ROUTES ARE SAFE TO USE	HUMINT SOURCES COMMUNICATIONS MONITORING VISUAL OBSERVATION OF CD ASSETS

Other information that would be useful to traffickers would include:

Aircraft Details — Number of operational aircraft, pilots, types of aircraft, and locations. This can be learned through open source and human intelligence (HUMINT) methods such as observation, inquiries, getting access to flight schedules, duty rosters, maintenance schedule, etc.

SOPs — Flight procedures (SOP): roles of interceptor, tracker, and helicopter. They can find this through open source and communications monitoring of U.S. counterdrug frequencies as well as of air traffic control frequencies, visual observation, and insider knowledge obtained legally or otherwise.

Communications — Communications used by counterdrug participants (frequencies, callsigns, procedures, and networks). Much of this information is available through open source information from a wide variety of sources. Additional information can be acquired through continuous monitoring of counterdrug communications and becoming familiar with schedules, callsigns, and routine activities, even to the extent that the monitors acquire voice recognition of individual counterdrug personnel.

Radar Coverage	Fixed radar coverage/profile. Some information is available from open source. Additional information can be acquired by exploratory flights accompanied by devices such as the "Blue Box," or even a standard radar detector, to determine the operating parameters of the system. Insight can also be gained through communications monitoring, such as hearing remarks concerning the limits of radar assets made in conjunction with routine detection/intercept operations. HUMINT can observe whether aerostat radars are up and functioning, and established aerostat operating patterns based on weather conditions are well-known.
CD Capabilities	Counterdrug force ground and airborne capabilities and procedures. The concerns are the same as above, with additional input from visual sources regarding the operational status of aerostat radar (if it's up, then it's probably working--if there is a chance of high winds, it's down and that part of the coast is clear). Also, the visual observation of AWACS aircraft being prepared/taking off is significant information. FAA radar coverage is available through open source info, as all aeronautical navigation maps have FAA air traffic control radar zones marked as part of their standard information. AWACS and other radar information (operating frequencies, characteristics, etc.) can be obtained by checking through *Jane's* reference books.
Current Threat	Detecting counterdrug aircraft while airborne. This may be done by monitoring interdiction frequencies while airborne, use of radio frequency detection devices such as radar detectors or the Blue Box, and visual observation by the pilot of the target aircraft, by spotters on the ground, on ships, or in other aircraft.

For questions regarding this working aid, please contact Annette Brooker-Grogan, National Cryptologic School OPSEC Education Division, (410) 859-4594.

Appendix B

MILITARY COUNTERDRUG SUPPORT OPERATIONS SECURITY (OPSEC) GUIDE

Introduction. The following guide is intended to help military planners identify critical information and OPSEC vulnerabilities that may be associated with counterdrug support missions. The guide, however, is a generic example of OPSEC considerations. It may not cover every situation. The suggested countermeasures might not be appropriate in every instance. Use this document as a tool to help plan and execute OPSEC programs. Commanders must determine what OPSEC measures to implement based upon their own risk assessment.

CRITICAL INFORMATION	INDICATORS	ENEMY CAPABILITIES	COUNTERMEASURES
1. Dates/times of missions.	Unsecured telephonic coordination w/LEA. Increased phone traffic as start date approaches.	Telephone monitoring by Drug Trafficking Organizations (DTOs).	Use secure phones. Encourage LEA to practice good OPSEC procedures.
	Opening new radio nets with LEA at mission startup.	Radio monitoring with scanners by DTOs.	Use LEA terms/codes or use secure voice communications.
	Units receiving intel via unsecured FAX.	DTOs monitor telephone lines for a copy of intel FAX.	Do not FAX intel over unsecured line.
	Units receiving intel via US Mail or private carrier.	Observation by relatives, friends of DTOs working in postal work force.	Hand carry. Have intel mailed to LEA or sanitized post office box. Use DoD personnel to hand carry.
2. Identification of supporting unit.	Unit representatives visiting LEA & area of operations (AO) for counterdrug intelligence preparation of the battlefield (CDIPB) data.	Observation by relatives/ friends of DTOs (viewing personnel w/LEAs).	Meet LEAs outside area of operations.
3. Military support assets working CDIPB.	Providing copies of TDY orders for car rental/lodging.	Observation by relatives/ friends of DTOs at car rental agencies/hotels (viewing TDY orders).	Do not provide copies of TDY orders to anyone. If government rates are refused, pay premium cost.

CRITICAL INFORMATION	INDICATORS	ENEMY CAPABILITIES	COUNTERMEASURES
4. Supported LEA identification.	Use of DoD phrases, terms, jargon, and rank.	Relatives/friends of DTOs overhearing discussions.	Coordinate in closed door sessions only.
		Observation by relatives/friends of DTOs at car rental agencies/hotels.	Never discuss mission near administrative, custodial or non-mission essential personnel.
	Use of government tax exempt forms.		Do not use tax exempt forms.
	Having pre-op intel/info mailed to LEA.	Observation by relatives/friends of DTOs.	Have mail sent to a post office box number.
		Workers at Post Office.	Do not use military return address.
	The wear of unit headgear, t-shirts, crests and/or display of unit specific notebooks, letterhead, luggage, etc.	Observation by relatives/friends of DTOs in target area.	Visiting unit personnel sanitize travel profile when in mission AO.
	Congregation of DoD personnel & LEAs, e.g., at lunches, dinners, especially in public.	Observation by DTO relatives, friends, or associates.	Eliminate excessive, large, and/or unnecessary public gatherings w/LEAs.

CRITICAL INFORMATION	INDICATORS	ENEMY CAPABILITIES	COUNTERMEASURES
	Leaving mission related info & material in hotel room.	Observation by DTO relatives, friends, or associates working at hotel.	Take mission related info/ material with you, leave it at the site under DoD control, or store in field safe. Never leave mission information unattended.
	Requesting CD intelligence from LEAs not knowledgeable of SR.	Overhearing by DTO relatives, friends, or associates	Do not attempt to acquire intelligence from LEAs not associated with mission. Make requests for intel to LEA you are supporting.
5. Location of objective area.	Taking of video/photographs in Area of Operation. Talking w/LEA at his office.	Can observe something out of the ordinary or overhear conversations.	Recons should be kept to a minimum. Limit exposure to a select few in areas away from AO & LEA's workplace.
6. Military intent to support LEAs.	**Private Land Use** - Research in county court for land owner identification; Request to land owner to operate on their land; Land use request goes to area Corps of Engineer Office. Taking of video/photographs in Area of Operation.	HUMINT- - Direct observation	Have LEA get land use agreement. Obtain long term agreements. Recons should be kept to a minimum.

CRITICAL INFORMATION	INDICATORS	ENEMY CAPABILITIES	COUNTERMEASURES
7. Mission Parameters	**LEA submission of Support Request (SR) -** Support Request contains dates, location, mission intent.	HUMINT sources within the LEA have access to SR information.	LEAs should reduce the number of HQ reviewing the SR until operational requirements dictate that it be briefed to area and regional coordinators.
	SR routed through numerous LEA headquarters (area task force, regional coordinator, state coordinator, etc.)		LEAs should treat SR as LEA sensitive.
	SR not handled as a sensitive document.		SRs could be written so as to limit amount of info divulged, with specifics refined later.
	LEA verifies mission by phone.		
	Military support unit pre-mission liaison with LEA - (Upon receipt of the Support Request, action officers contact LEA to discuss mission).	Technology exists in the hands of the threat which allows their monitoring of both telephone and in-room conversations.	LEAs obtain secure telephone equipment.
	Use of unsecure telephone.		Military unit provides secure equipment to LEAs for operations.

CRITICAL INFORMATION	INDICATORS	ENEMY CAPABILITIES	COUNTERMEASURES
	Unusual amount of LEA presence in his HQ (agents are normally in field). Assembling of "key" LEAs for joint planning. Paperwork related to military support handled by others who don't have a need to know (secretaries, clerks, distribution personnel, etc.).		Planners should meet with LEAs in person to reduce uncovered phone line discussions.
	Solicitation of unit support ability - Mission is discussed and messages are sent to multiple HQs. Major HQs in turn disseminate info to subordinate units.	Threat access to this info is limited. However, open source documents may become available to the threat.	Use STU III to contact possible supporting HQs. Reinforce to commands that mission info is sensitive.
	Initial Site visit with requesting LEA - LEA and supporting unit personnel conduct activity in the mission AO prior to operation. Unit uses rank & military unit when contacting LEA.	HUMINT sources can observe activities of site recon.	Request LEA meet with military support unit outside the mission AO.

CRITICAL INFORMATION	INDICATORS	ENEMY CAPABILITIES	COUNTERMEASURES
	Use of rental vehicles Use of government credit cards. Use of government rates at hotels. Video and still photo equipment used in prep of mission.	Identification of size of rental vehicles associated with LEA. Rental agency used by military can be determined.	Limit number of people and rentals on site survey. Determine if it is wise to meet LEA in his HQs. Use LEA vehicles in AO. Conduct aerial recons in LEA A/C or in military A/C if common in AO. Avoid all private property until deemed essential to obtain land use agreement.
8. Mode by which the main body arrives and time of arrival.	Large group of personnel arriving at a small airport. Inquiries at airport about arrival data. Convoys of rental vehicles at airport to move personnel.	HUMINT- - Direct observation by populace.	Have small group arrivals. Stagger arrivals. Arrive out of AO or at military base.
9. Air staging location.	Mass of military people in area.	Obtains knowledge of military movement, organization, & intent via HUMINT.	Change site to military base or airport out of AO.

CRITICAL INFORMATION	INDICATORS	ENEMY CAPABILITIES	COUNTERMEASURES
10. Location of billeting & messing of the advance party.	Several young, short haired individuals arriving at the same time & obviously not from the local area.	Can observe something out of the ordinary or overhear a conversation that something is being planned or is in progress.	Use military base for support. Use a base of operations outside AO. Move/change locations occasionally.
11. How initial movement from arrival airfield to AO (base of operations) will be conducted.	Large number of DoD personnel traveling commercially or using military air. Mission numbers placed on travel orders.	HUMINT- - Direct observation by populace.	Travel in civilian clothes; use low visibility travel arrangements. Do not leave document laying around.
12. Selection of Staging Area.	High profile military/LEA operations signature (increase in personnel, vehicles, equipment). Large contracting activity. Unusual racial composition for locale. Operations/military information left in hotel rooms. Increase in transmissions on radio freq. used by LEAs	HUMINT- - Direct observation of Military and LEA Agents SIGINT- -scanner equipment smugglers. IMINT- - photographic surveillance of site.	Operate from secure sites or DoD facilities. Disperse personnel for messing, billeting. Operate well off-site location. Use cash transactions and multiple contracting. Control off-duty time. Relax grooming standards (if approved by Commander/TAG).

CRITICAL INFORMATION	INDICATORS	ENEMY CAPABILITIES	COUNTERMEASURES
13. Method of deployment of personnel.	Convoys of like-type vehicles arriving in AO. Military traveling in uniform. Military vehicles used to deploy troops and equipment.	HUMINT- - Direct observation by populace.	Contract different types of vehicles and support equipment from more than one source. Avoid use of military equipment. Stagger arrival of personnel over several days. Military vehicle support should only be used from one military installation to another (avoid MAC aircraft in small civilian municipal airport). Follow-on deployments should be done by civilian vehicles.
14. Mode and schedule of transportation of the advance party into & around the AO.	Several young short haired individuals arriving at the same time & obviously not from the local area.	Observe something out of the ordinary or overhear conversations.	Rent used vehicles. Use LEA-provided unmarked or forfeited vehicles.
15. Mission number, type mission, supporting unit, and supported LEA.	Orders - Mission specifics stated on orders. Taking of video/photographs in area of operations. Talking w/LEA at his office.	Can detect presence and mission of military personnel when orders are presented for billeting, renting cars, etc. This is especially true for reservists who must present orders with their ID to use base facilities.	Avoid terms such as counterdrug, eradication, law enforcement, etc. in the mission description. Use generic statements on orders such as "conducting military training."

CRITICAL INFORMATION	INDICATORS	ENEMY CAPABILITIES	COUNTERMEASURES
		Can observe something out of the ordinary or overhear conversations.	Control distribution of orders. Recons should be kept to a minimum. Limit exposure to a select few and in areas away from AO & LEA's workplace.
	Pre-mission training. Combined DoD/LEA training sessions.	HUMINT- -Direct observation by threat	Conduct training at a secure location/away from area of operations. Conceal special equipment.
16. Intent to provide military support to LEA & location of AO.	Scheduling of facilities/ training areas.		Work in small groups.
17. Transportation into and out of operation area.	Large group of obvious outsiders arriving. Several rental cars (in convoy). Military vehicles/equipment moving on roads. Military equipment visible in vehicles.	HUMINT--Direct observation of military and LEA agents.	Limit number of vehicles gathering or driving to area of operation. Have military vehicles/equipment travel during evening hours. Rent older vehicles or vehicles more indigenous to the area.

CRITICAL INFORMATION	INDICATORS	ENEMY CAPABILITIES	COUNTERMEASURES
17. Identity of mission/target area.	Wearing uniforms in mission area.	Observation by relatives, friends of DTO associates, and the local populace.	Unless visibility is desired, limit wearing of uniform to mission area.
	Visitors to mission sites.	Observation by DTO relatives, friends, or associates, and the local populace.	Restrict on-site visits to mission essential.
	Presence of support/mission preparation intel equipment.	Observation by DTO relatives, friends or associates, and the local populace.	Limit the use of intel prep equipment at mission AO, e.g., tape recorders, camcorders, cameras, etc.
	Group reservations at hotels/group travel, especially by van.	Observation by DTO relatives, friends or associates, and the local populace.	Use multiple hotels recommended by LEAs and stagger routes and times of travel to and from mission area of operation.
	Dismount points too close to mission site.	Surveillance of mission AO. Observation by relatives, friends of DTO associates, and the local populace.	Use brushy or rocky areas to conceal dismount points. Infiltrate during periods of limited visibility.
	Pre-op intelligence over flights of target areas.	Observation by relatives or DTO associates, and the local populace.	Don't conduct pre-op flights over target area unless high altitude intel packages are used.

CRITICAL INFORMATION	INDICATORS	ENEMY CAPABILITIES	COUNTERMEASURES
			If used, ensure immediate reporting to ground teams during operational flights. Avoid unsecured airfields.
	Releasing too many maps of target area.	Observation by DTO relatives, friends, or associates, and the local populace. Capability to access/exploit open source documents.	Restrict maps & target data to need to know basis.
	Requesting CD intelligence from LEAs not knowledgeable of SR.	Overhearing by DTO relatives, friends, or associates, and the local populace. Monitoring of unsecure phone traffic.	Do not attempt to acquire intelligence from LEAs not associated with mission. Make requests for intel to LEA you are supporting.
	Dissemination of intelligence products to non-mission essential personnel.	Observation/access by DTO relatives, friends, or associates.	Limit distribution of intelligence reports or products to DoD/LEA elements who are directly involved in operation.
18. Use of military vehicles in support of CD mission.	Military vehicles operating outside habitual training areas.	HUMINT--Direct observation by the local populace.	Use only civilian vehicles. Conceal vehicles during daytime.

CRITICAL INFORMATION	INDICATORS	ENEMY CAPABILITIES	COUNTERMEASURES
19. Movement of personnel in & out of base of operations.	People conjugating at same locale & time.	Knowledge of military movement.	Move only at night; Deception movement plan in and out of primary AO. No convoy movement in AO. Use infiltration tactics. Vary meeting sites and times. Keep to minimum.
20. Vehicular parking.	Late model & military vehicles in area.	Knowledge of military movement	Spread out the number of vehicles in area.
21. Billeting.	Reservations for large group of people during off-peak time frame. Army people at AF base, etc. ID signature of military units.	Knowledge of military movement.	Avoid contracting for billeting. When possible, billet at different locations out of AO.
22. Billeting/messing of the visitors.	Short-haired/military looking.	Observe something out of the ordinary or overhear a conversation that something is up.	Don't identify yourself as government employee if normal rate is less than per diem.

CRITICAL INFORMATION	INDICATORS	ENEMY CAPABILITIES	COUNTERMEASURES
23. Transportation of visitors in/around base of operations/AO.	Obviously not from the local area.	Observe something out of the ordinary or overhear a conversation that something is up.	Don't allow LEA to visit CP in marked vehicles. Eliminate mention of mission on TDY orders.
24. Activity around base of operations.	Communication gear (292/SATCOM) outside. Additional people/vehicles.	Observation. HUMINT.	Camouflage/hide location of communication gear. Avoid use of military communications equipment. Limit number of people in area. Use military base for CP.
25. Location of chain of command (COC).	Activity surrounding a command post.	Threat can detect presence and size of military unit.	Locate COC away from the area of operations; use civilian clothes; employ "blend-in" techniques such as renting RV trailers.
26. Visitors.	New faces, especially visitors of importance attract attention	Can determine presence of military unit.	Minimize visitors, especially to area of operation. Restrict chain of command visitors.
27. Press releases.	Local officials may release information regarding a mission to local papers for political or other reasons.	Can gather considerable information about the mission.	Good prior coordination by unit commander with supported LEA is the best preventative measure. Ensure unit adherence to PAO guidance.

CRITICAL INFORMATION	INDICATORS	ENEMY CAPABILITIES	COUNTERMEASURES
28. Casual conversations.	Any contact with locals can result in inadvertent release of information.	Possibility of gathering detailed information. Local smuggling organizations, if alerted to the presence of military personnel, will deliberately target bars, restaurants, and other likely spots to learn what they can. They will also gather information from local people who may come into contact with troops.	Minimize such contacts by restricting liberty, billeting personnel in military facilities, etc. Positive control of individuals through a healthy command structure is the key.
29. Military Radio Procedures.	Use of military jargon during unsecure radio transmissions	Can determine callsigns, number of recon teams, and areas of operation. This has been one of the most significant compromises to military support.	Military support teams should **use secure communications.** For uncovered nets (LEA frequencies) adopt LEA callsigns and procedures, i.e. avoid the use of military jargon such as "out here", grid coordinates, etc.
30. Unexpected encounters.	When operating in remote areas, military personnel may encounter local law enforcement personnel who are unaware of the operation; local residents also.	Publicity resulting from such an encounter would alert smugglers to a military presence. Smugglers or growers could even arrange for an "accidental" encounter to take place.	A letter of introduction or written paper prepared by the supported LEA explaining permission to conduct military training with a telephone number could resolve legitimate encounters with other LEAs.

CRITICAL INFORMATION	INDICATORS	ENEMY CAPABILITIES	COUNTERMEASURES
31. False responses.	Smugglers will be alerted to the fact that an area is being watched when a false LEA response occurs; or if a smuggler escapes if LEA responds to the wrong place.	Threat can determine presence of military personnel and area of operation by noting LEA responses.	False or erroneous reporting usually occurs when military personnel are unfamiliar with local terrain and normal local activities. Countermeasures include several days of pre-mission train-up with LEA, ride along, and good intel prep. Personnel manning LP/OP positions must give a good intel prep. Also, personnel manning LP/OP positions must give a good changeover brief to relief teams. Ensure military and LEA personnel use same maps and designations of critical locations (e.g., LP#1, Hill 502, etc.).
32. Errors and Miscommunication	When an operation does not go smoothly, the recovery process may involve clear-voice transmissions, sudden scrambling of personnel, and other reactions that can compromise the mission. Such events tend to be extensively (often angrily) discussed after-the-fact.	Threat can detect presence of military personnel and locations of LP/OP sites by picking up on the unusual activity or the resulting discussions.	Several days of pre-mission train-up is vital to minimizing errors and miscommunication, and will improve OPSEC. Team cohesion can be enhanced with Situational Training Exercises (STXs). Military can teach small-unit tactics to LEA: LEA teaches advanced tracking techniques to military at formal sessions or informal gatherings.

CRITICAL INFORMATION	INDICATORS	ENEMY CAPABILITIES	COUNTERMEASURES
33. Cellular telephones.	Unsecured transmissions.	SIGINT. Interception of transmissions. Cellular telephone calls can be intercepted with off-the-shelf radio scanners.	Use operational/brevity codes. Limit number and length of transmissions. Use secure cellular telephones.
	Overtly transporting cellular telephones.	HUMINT. Military personnel carrying cellular telephones in public may arouse suspicion or invite theft.	Keep cellular telephones concealed and protected. Note that vehicles with cellular telephones are targeted by thieves.
34. Military radios.	Unsecured transmissions.	SIGINT. Interception of transmissions. Military radio transmissions can be intercepted with off-the-shelf radio scanners.	Use NSA approved electronic (on-line) encryption devices. Use burst transmission devices. While technically not secured these devices offer a reasonable amount of security. Use Operational/Brevity codes when not using on-line encryption devices.
		SIGINT. Direction finding and jamming employed against radios appears to be minimal.	Limit number and length of transmissions. Use appropriate ECCM techniques.

CRITICAL INFORMATION	INDICATORS	ENEMY CAPABILITIES	COUNTERMEASURES
	Overt placement of military radios and antennas.	HUMINT. The profile of military radios and antennas in a non-military environment will arouse suspicion and compromise locations.	Use low profile antennas. Keep military radios out of sight. Use military facilities whenever possible to mark operations.
35. LEA radios.	Unsecured transmissions.	SIGINT. The majority of LEA radio systems are unsecured. Notable exceptions are USCS and some USBP systems. SIGINT. Traffic analysis.	Use DES/electronic (on-line) encryption whenever possible. Avoid using LEA radio systems except in an emergency or to coordinate with the LEA. Use operational/brevity codes when not using on-line encryption devices. Use LEA (not military) call signs and radio procedures. Attempt to blend in with normal LEA traffic. Limit number and length of transmissions.

CRITICAL INFORMATION	INDICATORS	ENEMY CAPABILITIES	COUNTERMEASURES
36. Pagers	Unsecured transmissions.	SIGINT. Signals to pagers are difficult to intercept.	Pagers are a valuable means of communications and may be employed in lieu of other less secure means. The pager can be used to transmit operational/brevity codes.
	Overtly carrying pagers.	HUMINT. Military personnel carrying pagers in public may arouse suspicion and invite theft.	Keep pagers concealed and protected.
37. Telephones.	Unsecured transmissions.	SIGINT/HUMINT. Personnel must assume that all unsecured telephone lines are being monitored.	Use STU-III telephone whenever sensitive information is being discussed or faxed. Use operational/brevity codes when not using on-line encryption devices.
38. FAX.	Unsecured	SIGINT. FAX transmissions can be intercepted.	Use secure FAX whenever sensitive/classified information is being transferred.

CRITICAL INFORMATION	INDICATORS	ENEMY CAPABILITIES	COUNTERMEASURES
39. COMSEC Material.	Protection of COMSEC material.	SIGINT. Counterdrug COMSEC material varies in classification from UNCLAS to TS. The UNCLAS material is designed to be used with LEA's that do not have a security clearance. All COMSEC material must be protected from compromise.	Adhere to DoD regulations when handling COMSEC material.
40. MREs/Tray Packs	Carrying around in plain sight on civilian rentals. Trash.	HUMINT. Can detect signs of military presence and activity by size of trash disposed of.	Hide packages/trash, police areas of operation.
41. Batteries (Civilian/Military)	Trash wrappers. Disposal. Purchase from local vendors.	Can determine types of communications gear.	Police trash. Dispose of expended batteries at military DRMOs. Purchase away from area.
42. Construction material for tactical positions (i.e., barbed wire, sand bags, etc.)	Carried in civilian rental vehicles. Left behind when changing position.	Can detect positions. Can detect presence of DoD personnel.	Recover all class IV. Conceal when transporting.

CRITICAL INFORMATION	INDICATORS	ENEMY CAPABILITIES	COUNTERMEASURES
43. Class V	Carried in plain sight in civilian vehicles.	Can detect presence of DoD forces.	Conceal Class V when transporting.
	Expended pyrotechnics, brass, packaging not policed up from AO.	Can detect types of weapons. Can detect LP/OP positions.	Police all expended brass.
44. LBE/TA-50/782 Gear.	Carried in plain sight in civilian rentals. Military type clothing, i.e., corfram shoes		Conceal during movement to AO.
45. Rental Vehicles	New vehicles.	Can detect DoD presence.	Contract at large cities away from the AO.
	Same types/makes. Contracted with local vendors.	Can glean number of personnel, dates of exercise, and key personnel off the contract.	Request varied types of rentals and ensure local license plates are on vehicles.
	Refuel/repair. Rental company markings. Rental license plates.	Local fuel/tire shops deal with military.	
46. Medical	Use of civilian facilities to treat DoD personnel.	Can detect DoD personnel.	Ensure medics/corpsmen are prepared for all emergencies. Use civilian hospitals only in emergencies.

CRITICAL INFORMATION	INDICATORS	ENEMY CAPABILITIES	COUNTERMEASURES
	Discarded medical trash with military markings.	Can detect positions.	Police AO.
47. Laundry.	Use of civilian vendors/cleaners.	Can glean presence of military units.	Do own laundry.
48. Port-A-Johns/Dumpsters.	Use of civilian vendors.	Location of units.	Use slit-trenches/cat holes.
	Obvious presence of military forces.	Number of personnel.	Place waste receptacles away from sensitive mission sites.
		Can glean presence of military forces.	Carry out.
49. Additional supplies.	Increase in volume for certain items.	ID equipment & supplies of unit.	Have unit order supplies or ship their supplies in advance.
		Arouse curiosity.	
50. Movement of military personnel from billeting or support base to AO.	Vehicle patterns, helicopters on horizon, landing zones, entry/exit routes.	Knowledge of AO, ingress/egress points.	Vary location, use deception routes.
		Patterns established.	Insert for longer duration.
51. Time.	Daily/or set pattern for time of day, every 3d/4th day, etc.	Patterns established.	Vary time & days of ingress/egress.
			Use helicopters only for necessity, not convenience.

For Further Information...

The National Interagency Counterdrug Institute (NICI), a federally funded activity of the National Guard Bureau, was established December 12, 1990 by the California National Guard with the approval of the Department of Defense. NICI supports the National Drug Control Strategy by training representatives of law enforcement, military organizations, and the drug demand reduction community; and by analyzing tactics and procedures, establishing a repository of lessons learned, and disseminating information on counterdrug- and drug demand reduction-related issues, seminars, and conferences.

The National Interagency Counterdrug Institute (NICI) provides management-level training in the planning and conduct of joint counterdrug operations to both military and law enforcement personnel. The Counterdrug Managers' Course (CMC) is a five-day course presented by NICI approximately ten times a year. This tuition-free course is designed to enhance the interoperability of military and drug law enforcement agencies. (Students pay only for transportation, lodging, and meals.) NICI also provides a Drug Prevention and Demand Reduction Course (DPDR) approximately four times a year. This five-day course trains military and law enforcement personnel, public officials, business and community leaders, educators, counselors, and military family support group members to develop effective counterdrug programs within their communities. There is no tuition charged to attend this course. (Students pay only for transportation, lodging, and meals.)

NICI classes are conducted at San Luis Obispo, California and various other sites across the United States. Individuals interested in attending NICI courses should contact NICI student services at (805) 549-3966 or DCTN 630-9966.

* * *

The Research and Analysis (R&A) Division of NICI publishes *National Guard Counterdrug Lessons* at least once per year. They also publish a bi-monthly *NICI Bulletin* to provide information to the counterdrug and drug prevention/demand reduction community on drug prevention/demand reduction- and counterdrug-related conferences and seminars. To be placed on the mailing list for *National Guard Counterdrug Lessons* and the *NICI Bulletin*, or to have information on your conference or seminar included in the bulletin, contact the NICI R&A Division at (805) 549-3968 or DCTN 630-9968.

The NICI Research and Analysis Division also maintains an extensive library of materials on joint counterdrug operations and general drug policy issues. The Division offers a Request for Information service free of charge to the counterdrug community. Contact them to obtain copies of publications or to ask questions concerning military support to counterdrug operations.