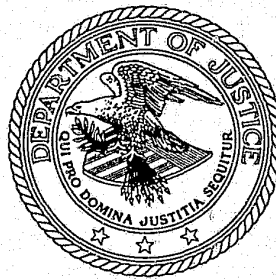


# BASIC ELEMENTS OF INTELLIGENCE

A Manual of Theory, Structure and Procedures  
for Use by Law Enforcement Agencies  
Against Organized Crime

143136



Technical Assistance Division  
Office of Criminal Justice Assistance  
Law Enforcement Assistance Administration  
Department of Justice

143136

**U.S. Department of Justice  
National Institute of Justice**

This document has been reproduced exactly as received from the person or organization originating it. Points of view or opinions stated in this document are those of the authors and do not necessarily represent the official position or policies of the National Institute of Justice.

Permission to reproduce this ~~copyrighted~~ material has been granted by

Public Domain/IEAA

U.S. Department of Justice

to the National Criminal Justice Reference Service (NCJRS).

Further reproduction outside of the NCJRS system requires permission of the ~~copyright~~ owner.

**BASIC  
ELEMENTS  
OF  
INTELLIGENCE**

**A Manual of Theory, Structure and Procedures  
for Use by Law Enforcement Agencies  
Against Organized Crime**

By  
E. Drexel Godfrey, Jr., Ph.D.  
and  
Don R. Harris, Ph.D.

The fact that the Law Enforcement Assistance Administration furnished financial support for the writing and publishing of this manual does not necessarily indicate the concurrence of LEAA in the material presented herein.

Technical Assistance Division  
Office of Criminal Justice Assistance  
Law Enforcement Assistance Administration  
Department of Justice

November, 1971

# FOREWORD

This manual is the product of two men experienced in the processes and operations of intelligence at the national level. They have spent many years as participants in the latter stages of the intelligence process—analysis and reporting, reevaluation, and management. From these vantage points they have also been closely associated with the other elements of the process—collection, evaluation, and collation. They were asked by LEAA to bring this knowledge and experience to bear on the problems posed to the law enforcement agency by their need to develop and to improve intelligence directed against organized crime.

Since this project obviously required knowledge of how intelligence is now produced in law enforcement agencies and what are the dimensions of the target, namely, the organized criminal, the two authors went to the field to find out. The many involved in this effort at the local, State, and national level gave most generously of their time, giving the authors a full, fast, and what might have been an unique display of operations, structure, personnel, and problems. Without exception they were most encouraging in the project since there was little in the literature to guide them in their efforts to establish an intelligence unit and to operate it effectively.

During the process of drafting the manual, many of those visited also gave of their time to review the sections and chapters in draft. They offered much assistance and many ideas. In this sense the manual can be considered a joint effort by the community of intelligence units in the many law enforcement agencies which participated. They bear no responsibility for the final product, yet without them it could never have been brought into what the authors believe is direct focus with the practical problems currently faced by the intelligence units across the country.

There were some that gave specific assistance to the authors and should be recognized for their help. Mr. Charles Lister made a major input of ideas and did the initial draft of Appendix A, Intelligence and the Law. Mr. Leonard M. Zandel contributed the bulk of the section in appendix B on computer operation security. Mr. Vincent Piersante of the Michigan State Police contributed his lists of questions which were used in appendix C to provide a starting point for an agency to develop its own question form for the important function of debriefing. The New England Organized Crime Intelligence System was kind enough to permit the reproduction of two analyses used as examples of strategic intelligence reporting (appendix E). The State of Florida Department of Law Enforcement was kind enough to allow the reproduction of their excellent guidelines for use in background investigation of applicants (appendix F).

The authors are deeply indebted to Georgia Lee Furniss, not only for editing the text in a most professional manner, but even more importantly for culling from the text a series of specific principles or guidelines to be found in appendix D. The project could not have been successfully con-

cluded without the ever present assistance of Phyllis Modley, who not only combined the functions of office administrator, research assistant, and generalist to-do-what-had-to-be-done, but also is solely responsible for the excellent bibliography which appears as appendix G.

Finally, mention should be made of the several members of LEAA who gave us counsel, guidance, and the fullest of support—Mr. Martin B. Danziger, former Chief, Organized Crime Program and now Director, National Institute of Law Enforcement and Criminal Justice; Mr. Louis Scalzo, currently Director, Technical Assistance Division; Mr. Joseph A. Nardoza, Regional Administrator, Region II (New York); and Miss Karen H. Clark. Mr. Joseph F. Cahill, in addition to his other tasks, carried the burden of arranging the details of the many trips. Mike Favicchio made a major contribution in his work preparing the graphic presentations. And last but far from least, the authors express much gratitude to Misses Diane Lehr and Jan Eichenseer for bearing the burden of final manuscript typing.

# PREFACE

The basic objectives of this manual are:

- To describe the process of intelligence and to point out how law enforcement agencies may apply intelligence to combat organized crime.
- To explore structure, training, staffing, and security of intelligence units and to provide guidelines for commanders of law enforcement intelligence units to improve their overall management.
- To present trends in the law as they may now and in the future impinge on the mission and functioning of the intelligence unit of law enforcement agencies.

The guidance presented in this manual cannot be specific. It cannot be since the size of intelligence units varies widely as does the threat posed locally by organized crime. The manual does point up the changing nature of organized crime, and suggests how techniques from disciplines unfamiliar to law enforcement can be adapted effectively to aid in the fight against the organized criminal.

One focus of the manual is on the needs of the head of the law enforcement agency. His understanding of what intelligence can do to help him carry out his responsibilities is critical. If he does not understand this, the intelligence unit may employ excellent techniques to produce excellent intelligence, but it will only be tactically useful. The strategic role of the law enforcement agency in meeting the challenge of organized crime will not be served.

# TABLE OF CONTENTS

	Page
Foreword .....	iii
Preface .....	v
List of figures .....	xii
Glossary .....	xiii
CHAPTER I. THE ROLE OF INTELLIGENCE IN COMBATING ORGANIZED CRIME .....	1
Introduction .....	1
What intelligence means .....	1
The intelligence process .....	2
Tactical intelligence .....	2
Strategic intelligence .....	2
The command level and its use of intelligence .....	3
The analytic method in the service of the policymaker .....	4
Getting down to basics .....	4
The three essentials of an intelligence unit .....	4
"Add-ons" to the essentials .....	4
Factors making for sound intelligence .....	6
Intelligence as a staff function .....	6
The agency head's intelligence brief or report ..	7
Pushing out the traditional boundaries .....	7
Expanding the intelligence data base .....	7
Strengthening the analytic capacity .....	8
Use of professional specialists .....	8
Looking beyond the La Cosa Nostra .....	9
The role of the commander of the intelligence unit .	9
CHAPTER II. THE INTELLIGENCE PROCESS .....	11
Introduction .....	11
Collection .....	12
Planning the collection function .....	13
Example of collection planning .....	13
Collection methods .....	14
Overt collection .....	14

	Page
Investigators .....	14
Information from non-intelligence units .....	15
Information from other jurisdictions ..	16
Debriefing as an aid to information gathering .....	17
Information from sources other than law enforcement agencies .....	17
Complainants .....	18
Covert collection .....	19
Physical surveillance .....	19
Electronic surveillance .....	20
Informers .....	20
Undercover agents .....	21
Evaluation of intelligence inputs .....	21
Collation .....	22
Filing system .....	23
Cross-indexing .....	23
Mechanical filing aids .....	24
Analysis .....	24
An example of analysis .....	24
The role of the hypothesis .....	25
The role of research .....	26
The relationship between collation and analysis .....	26
The analyst-investigator relationship .....	27
The intelligence report .....	27
Periodic reporting .....	28
Indicative versus evidential intelligence ...	28
Role of the consumer .....	28
Dissemination .....	28
Reevaluation .....	29
Management of the intelligence process .....	30
Collection plan .....	30
Monthly report of intelligence unit's activities .....	31
Monthly evaluation of operations .....	31
 CHAPTER III. THE STRUCTURE OF AN INTELLIGENCE UNIT .....	 36
Introduction .....	36
Structure and mission .....	37
The intelligence unit and the two-way stretch ..	37
The intelligence unit and enforcement .....	37
Guiding principals of organization .....	38
Location of the intelligence unit .....	38
Intelligence as a staff function .....	38



	Page
The intelligence unit and the head of the law enforcement agency .....	39
The filtering effect .....	40
The intelligence unit and internal problems of the agency .....	40
The shape of an intelligence unit .....	41
The control of information and document flow .....	41
Logging .....	42
Circulation, filing, and storage .....	44
Division of labor—information control versus analysis .....	46
Structure and analysis .....	47
Analysts and investigators .....	47
The team approach .....	47
Supervising the team .....	48
Clerical support .....	49
Intelligence unit command .....	49
Dissemination, a command function .....	50
The intelligence unit commander .....	50
Strategic intelligence component .....	51
Intra-agency relations and the unit commander .....	51
External relations .....	51
Obstacles to effective external relations .....	52
Actions to improve external relations .....	52
The protection of intelligence information .....	53
A treaty as an aid to external relations .....	55
External liaison .....	55
 CHAPTER IV. STAFFING THE INTELLIGENCE UNIT .....	 59
Introduction .....	59
The unit commander .....	60
General criteria for staff selection .....	60
The first step—the interview .....	61
Investigator candidate testing—use of field problem .....	61
Analyst candidate testing—use of analytic model .....	62
The selection process .....	63
The special problem of choosing the intelligence investigator .....	64
Determining the analytic discipline needed .....	65
The nonspecialist analyst .....	65
The specialist analyst .....	65
Use of the academic community .....	66
The problem of the nonbadged employee .....	68

	Page
The special nature of staffing the intelligence unit . . .	69
Career considerations for intelligence personnel	70
 CHAPTER V. TRAINING AND INTELLIGENCE . . . . .	 73
Introduction . . . . .	73
The three levels of training . . . . .	74
Training for the nonintelligence officer . . . . .	75
Intelligence is not a mystery! . . . . .	75
Field reporting by the peace officer . . . . .	76
Introduction to organized crime for the general officer . . . . .	77
Understanding the role of the agency head . . . . .	77
Training of intelligence officers . . . . .	78
Intelligence theory and organized crime . . . . .	78
The target: organized crime . . . . .	79
Official corruption . . . . .	79
Organized crime beyond the "Mafia" . . . . .	80
Emphasis on analytic technique . . . . .	80
Sophisticated analysis problems . . . . .	81
Report preparation . . . . .	82
Field reports . . . . .	82
The analytic report . . . . .	82
Technical training . . . . .	83
Security training . . . . .	84
Other topics . . . . .	84
Command level training . . . . .	84
"War gaming" . . . . .	85
Writing the intelligence report . . . . .	85
Understanding methodology and process . . . . .	85
The command level and organized crime . . . . .	86
Training priorities and hardware . . . . .	86
Other training programs . . . . .	87
Training techniques . . . . .	87
Untraditional training techniques . . . . .	87
Sample problem—demonstration and test of analytic techniques . . . . .	88
 CHAPTER VI. SECURITY AND THE INTELLIGENCE PROCESS . . . . .	 92
Introduction . . . . .	92
Personal security . . . . .	94
The background investigation . . . . .	94
Update of background investigation . . . . .	95
Polygraph . . . . .	97
Security training . . . . .	97

	Page
Physical security .....	98
The office .....	98
The files .....	98
Restricted materials .....	98
Security and the computer .....	100
Security and privacy .....	100
Organization of the office for security .....	101
Operational security .....	101
The responsibility of the unit commander .....	102

#### APPENDIXES:

A. Intelligence and the Law .....	107
B. The Computer and the Intelligence Unit .....	115
C. Sample Debrief Form .....	123
D. Guidelines: Operation of an Intelligence Unit .....	128
E. Examples: Strategic Intelligence Reporting .....	137
F. Guidelines: Background Investigation of Applicants— Intelligence Unit .....	139
G. Bibliography .....	144

# LIST OF FIGURES

	Page
FIGURE 1. The structure of the intelligence unit .....	5
2. Sample intelligence report form for use by non-intelligence units .....	16
3. Sample daily patrol report form on surveillance of locations of interest to intelligence unit .....	17
4. Sample evaluation system—reliability of source and content of information .....	23
5. Sample monthly report of the intelligence unit's activities .....	32
6. Analysis .....	33
7. The intelligence process .....	34
8. Sample logsheet: Incoming documents and information received by telephone .....	43
9. Sample logsheet: Outgoing documents and reports .....	45
10. Sample record of inquiries .....	54
11. Information flow .....	56
12. Criterion for selection of intelligence unit staff .....	71
13. Suggested weighting of subjects in intelligence training courses .....	75
14. Two-week training course for intelligence analyst/investigation .....	91
15. A sample financial questionnaire .....	96
16. Sample logsheet: Visitors record .....	99
17. A sample secure office layout .....	103
18. A sample secure office layout—a small unit .....	105
19. Example: Summary printout categories and input information .....	119

# GLOSSARY

- Agency Head**—A phrase in this manual used to refer to the head of any law enforcement agency—local and State police, local and State prosecutors offices, etc.
- Analysis**—The function of assembling in a logical manner bits and pieces of information to form patterns and meaning.
- Analyst**—A person in an intelligence unit that performed the analysis function.
- Collation**—The function of handling, sorting, and filing information, including the sifting out of useless information, the orderly arrangement of collected materials so that relationships may be established, and the creation of a system for rapid retrieval of filed information.
- Hypothesis**—A tentative statement of the meaning of a collection of information when arranged in a logical manner.
- Indications Intelligence**—Information processed by an intelligence unit which informs of or suggests the occurrence of an event.
- Information**—Written or oral reports or documents, short or long, telling of an event, or an activity.
- Intelligence**—Information that has been processed—collected, evaluated, collated, analyzed, and reported.
- Intelligence Officer**—A person engaged in the substantive work of an intelligence unit—investigative, analysis, or command.
- Intelligence Reports**—Written or oral presentations that convey intelligence to consumers.
- Intelligence Studies**—Intelligence reports that cover subjects that have been researched and analyzed in depth.
- Intelligence Unit**—A phrase used in this manual to refer to intelligence organizations regardless of size or the type of agency in which they are an element.
- Investigator**—In this study it refers to the personnel in an intelligence unit that performs the investigatory task.
- Law Enforcement Agency**—Any official unit at the State or local level that has the responsibility for enforcement of ordinances and laws relevant to its jurisdiction.
- Organized Crime**—Means the unlawful activities of the members of a highly organized, disciplined association engaged in supplying illegal goods and services.
- Premonitory Intelligence**—See Indication Intelligence above.
- Raw Data**—Information that has not been put through the intelligence process.
- Strategic Intelligence**—Intelligence that indicates significant patterns of activity that may become a major inputs to the planning and decision levels of the agency.
- Tactical Intelligence**—Intelligence that is immediately useful to the enforcement element of an agency.
- Unit Commander**—A phrase used in this manual to indicate the commander of an intelligence unit regardless of size or type agency of which it is an element.

# Chapter I

## THE ROLE OF INTELLIGENCE IN COMBATING ORGANIZED CRIME

### INTRODUCTION

Special weapons are needed to combat organized crime. Unlike the street gang or the single hoodlum, the large criminal syndicates have, as their name suggests, an organization behind them, often with sophisticated members in key positions and usually with much larger "operating budgets" than the average law enforcement agency. In some localities organized crime amounts to a countersociety complete with its own set of perverse human values and societal rules. In most localities organized crime seeks to conceal itself by buying official protection. In all localities where it exists organized crime shields its leadership from prosecution by insulating the command levels from direct involvement in criminal acts.

For all these reasons organized crime presents the law enforcement agency with a special and difficult challenge. A single arrest, or even a series of arrests, may not seriously impair the effectiveness of a self-perpetuating organized crime network; indeed, picking off individual criminal figures, simply as the opportunities arise, may amount to nothing more than officially sponsored career development for the syn-

dicate. Great numbers of impatient young men have been waiting a long time on the organizational ladder for their older superiors to move on.

If law enforcement is to tackle organized crime systematically, it must have a strategy, or strategies. The development and perfecting of strategies rests on sound intelligence. This manual has as its objective the elaboration of a sound intelligence service to support law enforcement in combating organized crime. A main focus of the volume is on intelligence support to the command level of law enforcement agencies,<sup>1</sup> but there is also a substantial amount of material on intelligence support for operations. The distinctions between these two support roles will be discussed below.

### WHAT INTELLIGENCE MEANS

"Intelligence" is a word that gives grammarians headaches. It can mean a select piece of information: "I have *intelligence* which tells

---

<sup>1</sup> The phrase "law enforcement agencies" is used throughout this manual as a general reference and includes State, county, and local police departments, and prosecutors at similar levels.

me that the Second National Bank is going to be robbed." It can describe a process of physical and mental acts: "Through the use of *intelligence* techniques, I have concluded that this city may soon see a gangland war." It is sometimes used to define a specific function within a law enforcement agency: "Captain Jones from *Intelligence* tells me that he is being transferred to *Traffic*." All of these, of course, are proper usages. What concerns us here, however, is not a grammatical oddity, but an understanding of the word as it applies to 20th century law enforcement.

### THE INTELLIGENCE PROCESS

Intelligence is the end product of a complex process, sometimes physical and always intellectual. The end product is most often an informed judgment; it may also simply be a thoughtful description of a state of affairs; it can be a single fact, or best guess. The process which generates these judgments, descriptions, or facts and near facts, is called the intelligence process. (It is discussed in detail in chapter II.) The intelligence process refers to the handling of individual items of information and their conversion into material useful for law enforcement purposes. The process includes the collection of data, the collation (or combining and storage) of data, the evaluation and analysis of the collected and stored data, and the dissemination of the analyzed and evaluated material. Collection and storage are traditional pursuits of law enforcement agencies; the other parts of the intelligence process tend to be less well understood and in some cases are hardly practiced at all. A basic premise of this manual is that the systematic exploitation of raw data through the operation of the intelligence process can provide the law enforcement agency with a high-quality end product. The process turns information into intelligence.

Raw information can be processed into a variety of intelligence end products. In the simplest form it may be no more than descriptive—the biography of a known organized crime leader, the background history of a criminal activity, a sketch of the human relationships in an illegal business enterprise, etc. Such intelligence normally is used by intelligence officers to assist them in their work, as reference material to provide them with an understanding of the

criminal world they are exploring. It can also become an input to intelligence reports and studies. In some cases a piece of raw information may give a hint or warning of things to come or criminal activities developing. This type of information when received by a law enforcement agency is called premonitory or indications intelligence.

The most useful way of categorizing the differences in intelligence end products is to focus on the use of the material by consumers of intelligence. On this basis, there are two broad and sometimes overlapping categories: tactical and strategic intelligence. (See chapter II, page 11, for detailed definitions.)

### Tactical Intelligence

Tactical intelligence is that which contributes directly to the success of an immediate law enforcement objective. It may be the supplying of a lead to an investigator; it may be compilation of a list of potential surveillance subjects; it may be some small new fact supplied by an observant police officer who is aware that reports on the activities of a certain loan shark are being entered in a dossier on the subject. Clearly, tactical intelligence can take many forms. One form is as simple as passing a fact from one police intelligence unit to another: "You asked if we had any information about X. Well, not much. He is, however, an associate of Y." What transforms this item from simple information to intelligence is that a report attesting to the relationship between X and Y had previously been accepted by the first intelligence unit, evaluated as having sufficient credibility to be entered in its files, and considered substantial enough to be passed on to the second unit. It is tactical intelligence because, presumably, the intelligence unit requesting the information is in the process of assembling a file on X with a view towards eventual apprehension of X as a lawbreaker.

### Strategic Intelligence

Strategic intelligence is the highest form of the end product of the intelligence process. It is a blending of facts and analysis to produce an informed judgment on a major aspect of a law enforcement agency's objectives. An example of strategic intelligence would be a report to the head of the agency on the growth of organized

crime in a major sector of the metropolitan area. It might be an analysis of the development of certain criminal phenomena in a neighboring city with some suggestions as to how quickly the home city might be affected. Strategic intelligence differs from tactical in that it deals with the larger issues with which the top decision-makers of the agency are concerned, not the nuts and bolts of intelligence support which the investigator or patrol officer on the street must have to do his job.

To clarify further the role that strategic intelligence plays in the workings of a law enforcement agency, it is useful to consider what a principal policymaker or strategist needs to meet his responsibilities. In the case of his obligation to lead the agency in its effort to reduce or neutralize organized crime, he should have available at all times a full picture of the strength, influence, and effectiveness of criminal syndicates in his jurisdiction (and neighboring jurisdictions). He should have a strong feeling for the weaknesses in the social and economic fabric of the city he serves. For example, he should know what types of businesses, unions, social organizations, etc., are controlled or penetrated by organized crime and to what degree; equally, he should have some appreciation for which institutions are most susceptible to future penetration—and this includes, of course, the political institutions of his jurisdiction. Finally, he must know what weapons or strategies are available to him in the battle against organized crime and what he needs to sharpen his weapons or improve his strategies. A disciplined, imaginative intelligence unit, equipped with proper manpower resources, can provide him with support on all of these fronts.

## THE COMMAND LEVEL AND ITS USE OF INTELLIGENCE

But the agency head<sup>2</sup> cannot expect intelligence support on such matters to flow up to him automatically. He must make clear what his needs are to his intelligence unit commander,<sup>3</sup>

<sup>2</sup> The phrase "agency head" is used throughout this manual as a general reference, and includes chiefs of police departments, district attorneys, and State attorney generals.

<sup>3</sup> The phrase "intelligence unit commander" is used throughout this manual as a general reference and includes the head or commander of intelligence units regardless of their specific title in their own agency.

how and when and in what format he expects to receive the finished intelligence product. If the agency head is himself preoccupied with the tactical details of enforcement activities, then he will only receive tactical intelligence from his subordinates instead of the broad interpretive material that can give him a perspective on the major planning moves he must make.

The flexible use of intelligence materials as a prime tool of management may be a difficult concept for some law enforcement leaders. Their leadership style has traditionally been quite different—making the big case, being up front in the dangerous raid, responding alertly and efficiently to emergencies. These have been the hallmarks of leadership. As the size and the functions of law enforcement agencies have expanded, leaders have not always kept pace with the changes taking place all about them. They have, with rare exceptions, allowed agency size to outstrip command control, and paperwork to smother thought. Organizational structures have remained static. By and large the leadership passively receives problems instead of perceiving them in advance and heading them off. While most agencies now have small planning units, these are primarily hostages to the budget process.

What has been lacking—and too often lacking at all levels of leadership in law enforcement—is the disposition to think systematically about responsibilities and assets. Objectives are rarely viewed as problems requiring careful planning and the setting of priorities. Horizons are not scanned for potential emergencies so that premonitory action can be taken to preempt them. Or if they are, it may be at the last moment when preparations are by necessity hasty and possibly ill-conceived.

This unhappy picture, admittedly somewhat exaggerated, is a product of flabby mental discipline. It means that in many cases law enforcement leadership has not seen fit to put intelligence to work—that is, leadership has been unwilling to require a staff component to examine the agency's movement toward a given objective or the fulfillment of a specific responsibility. It has been unwilling to use the bright minds in its ranks to measure a problem, dissect it, pore over it, balance the demands of that problem against the current deployment of agency assets, and draw conclusions about a



course of action to meet the problem. Leadership has been exercised from the hip, not from the head.

### **THE ANALYTIC METHOD IN THE SERVICE OF THE POLICYMAKER**

One large metropolitan intelligence unit commander recently completed a survey of the judicial disposition of narcotics cases which his agency had brought before the city's judicial authorities. The study was detailed and thorough. It showed that a great proportion of narcotics offenders apprehended in a major sweep program over a year's time were either back in business or soon would be. The study showed more; it demonstrated that the agency's arrest procedures had been poor by citing the large number of cases thrown out of court for procedural defaults; it further showed that, given court backlogs and prison overcrowding, the agency's whole approach to the narcotics problem was bound to fail. The system simply could not absorb wholesale prosecutions and confinements.

By demonstrating the failure of the unit's narcotics control policy, effective use of the analytic method opened the door to adopting a new and hopefully more realistic policy. In this instance the raw data had nothing to do with organized crime, but were statistics from the city's criminal justice system arranged in meaningful groupings and related to the agency's own policies and arrest procedures. The story illustrates a fine piece of strategic intelligence put to work in support of a principal policy responsibility of the agency head. It is one for which there are too few parallels around the country.

### **GETTING DOWN TO BASICS**

The law enforcement agency head, who wishes to establish a sound and effective intelligence unit that can serve all operational levels of his organization (including his own), should begin by getting down to basics. He must define for himself what an intelligence unit should do, what its functions should be. He should have a firm grasp of where it should fit structurally in the agency. Finally, he should understand what the minimum essential components of a good intelligence unit are. Having satisfied himself on these counts, he will be in a position to move toward his objective.

### **THE THREE ESSENTIALS OF AN INTELLIGENCE UNIT**

There are three essential components of an intelligence unit. Or to put it another way, there must, at a minimum, be provision for three activities to take place. The absence of any one of the three could have a crippling effect on the effective functioning of the intelligence unit. (See figure 1: The structure of the intelligence unit, page 5.)

Other activities or organizational subelements can be added to the three, but they merely give the whole operation greater flexibility and sophistication.

The minimum essentials are:

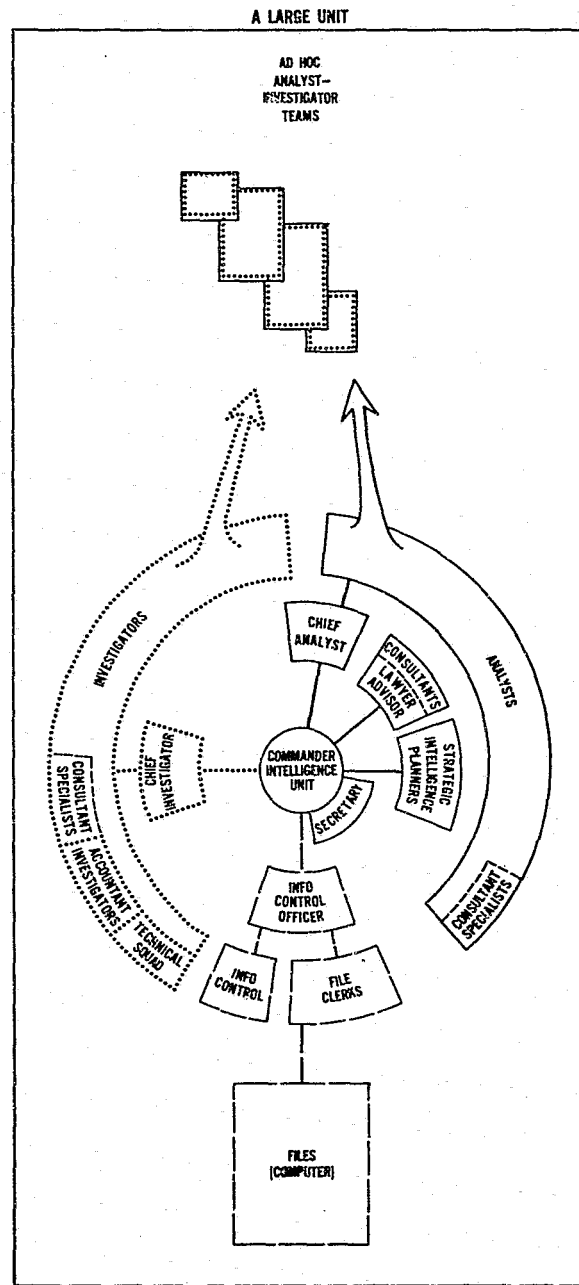
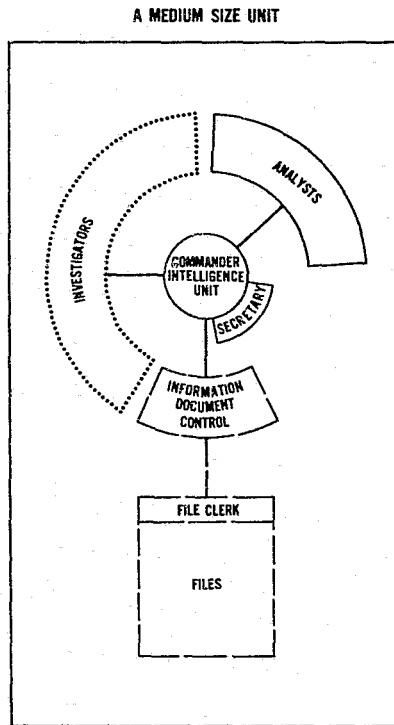
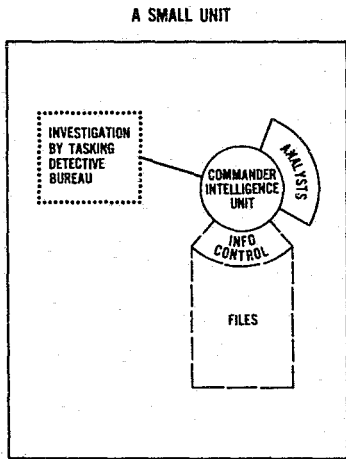
1. Files containing information arranged in a manner susceptible to rapid and effective exploitation for the purposes of analysis. They should be thoroughly cross-referenced and organized functionally as well as biographically.

2. There must be a formal, permanent arrangement for a flow of raw information to reach the unit from whatever sources can be tapped: unit investigators, technical collection devices, other reporting elements of the agency and other agencies, public and official record repositories, and private data collections where possible and legally defensible.

3. There must be one or more persons specifically designated as analysts. That person (or persons) should be capable of developing from the file records and the incoming raw information patterns, networks, connections, new areas of organized crime penetration, etc. Without the analyst, the information flow cannot be utilized effectively to contribute to the strategic purpose of the agency. Without the analyst, much of the incoming raw information will remain just that; moreover, a great deal of it will be lost forever in untapped filing cases.

### **"ADD-ONS" TO THE ESSENTIALS**

The listing above is not exclusive; many other functions and specialties can justifiably be added to an intelligence unit which serves a major metropolitan area. Beyond the essential nu-



THE STRUCTURE OF THE INTELLIGENCE UNIT

FIGURE 1

cleus, however, "add-ons" will simply be proud moments in empire building if each accretion does not contribute significantly to the overall objective of the unit: the production of sound, finished intelligence which can be of substantial use in neutralizing organized crime. But most agencies will find they can absorb "add-ons" that improve the quality and quantity of their intelligence effort. Among the possible peripheral contributors are a specially detailed investigative squad working only for the agency's intelligence needs, a technical equipment section to handle photographic and electronic surveillance equipment, liaison officers to work with precinct commanders or with other agencies, highly specialized personnel, such as accountants, systems analysts, etc., and information control technicians.

### FACTORS MAKING FOR SOUND INTELLIGENCE

Sound intelligence on organized crime can be provided to the law enforcement agency's top command level if it is demanded and if quality standards for the intelligence product are imposed. Good quality intelligence depends on a number of factors, of course, but perhaps the most important one is the separation of the intelligence function from responsibility for operations. For a number of reasons, merging of the two functions will end in the dilution of the intelligence function as the hunt reaches a climax and an arrest seems near:

1. To unravel a major criminal syndicate may take many months or years of painstaking work; it may require temporary moratoriums on arrests of criminal offenders while more intelligence is gathered to gain access to higher and higher echelons of the group.
2. Organized crime's involvement in some apparently legitimate business affairs requires the use of specialized intelligence officers, frequently from outside traditional law enforcement agencies; they would probably not be authorized to make an arrest no matter how eager they were to do so. (The separation of intelligence and operational responsibilities is discussed in chapter III.)
3. The intelligence officer must *not* be-

come a partisan of any particular operational policy. An intelligence report which winds up by recommending that an agency take specific courses of operational activity is not a good intelligence report. Should that policy fail—or some other approach be adopted and succeeded—something of the credibility of the intelligence unit will have been lost.

There is no room for the intelligence officer to develop an emotional identification with a given operational plan. Sooner or later emotions will get in the way of objectivity.

### INTELLIGENCE AS A STAFF FUNCTION

What, then, should be the relationship between the agency's chief operational planner or strategist and the intelligence unit? Ideally, it should be as close as possible. As a staff organization the unit should be expected to supply the agency head with all the intellectual material he needs to lay out his strategy or make his operational plans. The intelligence unit, or its commander, should be part of the process of strategy formation, not a proponent of any particular approach. Nevertheless, the commander should be in a position to warn of the consequences of embarking on a strategy or operational plan whose implications do not appear to be clear to the agency head. In order to do this effectively, he must not tarnish his image of objectivity by lending his support to some other strategy or plan.

The relationship between agency head and intelligence unit must be close enough so that the head's requirements can be quickly and clearly transmitted to the unit. Filtering his requirements through many hands can result in the production of intelligence he does not want or need. By the same token, it is the agency head's responsibility to insure that his views of the quality of the intelligence he is getting feeds back to the unit. In this way the end product can be developed and polished and handcrafted to a point where the agency head finds it not only useful but indispensable. At this point, intelligence will have served its proper role as a principal tool of the command level. (The place of an intelligence unit within a law enforcement agency is discussed in detail in chapter III.)

## The Agency Head's Intelligence Brief or Report

Each unit commander must decide how intelligence is to be served up to the agency head. He will have his own tastes and idiosyncrasies, but whatever these are, certain guidelines are necessary. A routine delivery or presentation schedule is useful because it becomes something that cannot easily be postponed or skipped. Some agency heads will want their intelligence reports or briefings (written or oral) daily, some once a week; it makes little difference as long as the presentation is at a fixed point in time. The contents, of course, will depend on local circumstances and personal needs, but a few minimum standards should be built into any brief.

### *Usefulness*

The intelligence contained in the agency head's brief should first of all be useful—that is, directly concerned with the head's area of responsibility for organized crime. It will only be confusing to him, for example, if extraneous material on street crime is included in an organized crime brief. If a street crime has been committed about which he should be informed, news of it should be brought to him by his enforcement division, or should be placed in a special category of the commander's report.

### *Pointedness*

The intelligence contained in the brief must be pointed—that is, shaped in such a way that the significance of the item to the agency head is immediately apparent. For example, it is next to worthless to include in the report a list of cars stolen in the city over night, complete with their descriptions, license numbers, etc. The agency head is not likely to retrieve any of them himself and, therefore, has no need to know or interest in knowing that one was a "blue 1969 Dodge sedan." On the other hand, if the city has been suffering a wave of organized car thefts, an item might be composed which said simply, "The wave of organized crime car thefts is still rolling without any signs of slowing up. Last night's count was eight, the largest since the operation began last month. No progress yet on resolution of this problem."

### *Timeliness*

The agency head's intelligence brief should also be timely. It will help neither him nor the intelligence unit if he is given information he already knows, simply because a brief is scheduled to be presented. In the case of the automobile thefts, for example, let us say that the enforcement chief has already told the agency head of the past night's score. The intelligence brief obviously should not duplicate this information. But it may be able to go a little further. Perhaps it can report on similar crime waves in neighboring cities and what breaks have been made in those cases, if any.

The brief had best be crisp—short, grammatically uncomplicated, stripped of extraneous detail, and well organized. Finally, it should be up to date—there is no point in providing the head with ancient history simply to point out the heinous nature of organized crime. Case histories can sometimes be useful, if they make a point—but the point should be clearly stated at the outset.

## PUSHING OUT THE TRADITIONAL BOUNDARIES

So far the discussion has centered around concepts of intelligence support for the agency head concerned with organized crime. Once the head has adopted the analytic methods suggested in the foregoing to meet his strategic and planning problems, he will find that his perceptiveness has increased, his capacity to think beyond the traditional boundaries of a problem enhanced. This will be critical over the next few years as organized crime changes its methods of operation and moves into more sophisticated and less obvious criminal enterprises. It will require a broad and flexible approach to cope with the subtler machinations of criminal syndicates as they develop confidence around the country.

## EXPANDING THE INTELLIGENCE DATA BASE

The simplest way for most law enforcement agencies and their intelligence units to expand their resources is to build on their present intelligence data. For many, this is now only a series of biographic files on known "family" members and assorted local hoods, which obvi-

ously is completely unable to support an analytic effort. First of all, such an ordering of data is useful only if the strategic assumptions of the agency are geared to a case-by-case approach. It presupposes that "a pick-em-off-one-by-one" strategy can cope with quite sophisticated organizations operating more or less clandestinely, sometimes illegally, but quite often legally. It presumes, also, that the law enforcement agency can keep pace with or outstrip the sophisticated practices of organized crime. It ignores the fact that for every organized crime figure knocked off by arrests, there are several subordinates of considerable experience waiting in line to fill his shoes. It also ignores the difficulty posed by the fact that organized criminal syndicates will increasingly be using individuals—either as effective partners or as fronts—who have no criminal records, no dents in their armor.

An important priority, then, is to reorganize the unit's data base on crime so that it can be manipulated in a variety of ways. First and foremost this will mean the setting up of functional files—on businesses, city sectors, travel patterns of known hoodlums, etc.—and cross-referencing them to existing biographic files. A detailed knowledge of individuals is only one element of a useful intelligence data base. By itself it is only of marginal value, but when combined with pools of knowledge about activities, localities, movements, etc., all manner of associations and patterns of criminal or suspicious behavior may emerge. In the past it was sometimes possible to put together quite complex "pictures" by combining biographic data with intensive surveillance of specific individuals. What is being suggested here is that such patterns could have been discerned all along from existing stored data had not one dimensional filing techniques hidden the relationships from intelligence analysts. (Chapters II and III contain considerable material on this general topic.)

By using a truly manipulative data base, many intelligence units will find themselves in a position to exploit materials long untouched in their files. They will be able to detect hitherto unsuspected links and associations; they may even uncover legal fronts for illegal activities, and they may be able to accomplish this without as much reliance as in the past on single case surveillance and electronic eavesdropping techniques.

The larger and better heeled law enforcement agencies will be casting about for ways to apply the computer to these efforts. Even where an ADP capability appears remote (and to some law enforcement officers, threatening), any revamping of current filing systems should be done in a manner that does not foreclose the move into computer storage and retrieval facilities at a later date. (See appendix B on the use of ADP techniques in intelligence.)

### **STRENGTHENING THE ANALYTIC CAPACITY**

Technical improvement of filing methods can be accomplished in many law enforcement agencies by the short-term employment of information consultants. Beefing up the analytic capability of the intelligence unit is another matter. It may require considerable soul searching about sacred traditions of the agency, such as: the introduction of nonbadged personnel, stepping into civil service entanglements, and contemplation of a freer exchange of information with other law enforcement agencies. All of these points are touched on elsewhere in this manual, but it is essential to pause here for a word or two on the permanent use of trained professional specialists.

Organized crime increasingly is moving away from reliance on muscle and violence and putting more dependence on guile, detailed knowledge of the intricacies of business and commerce, and on mobility. More and more the strategic emphasis of criminal syndicate leaders is on careful exploitation of legal loopholes, the quick movement of goods or cash, and even on such esoteric matters as market mechanics. An adequate response to this trend will require that law enforcement agencies have at least the same type of weapons as the enemy—if not yet equal firepower.

### **USE OF PROFESSIONAL SPECIALISTS**

Accordingly, intelligence units must face up to the need of hiring such specialists as economists, accountants, attorneys, and even systems analysts. The problems their employment may pose for the personnel policies of the agency involved had best be faced, studied, and prepared for in advance. There are also implications for the training programs of the agency,

not only for its intelligence unit, but for all its ranks. (Training is discussed in detail in chapter V.) The role of intelligence—and particularly its modern role of direct support for the command level—should be thoroughly appreciated by all hands. If it is, the anxieties over integration of specialists into the agency and the bureaucratic problems related to such a change may be somewhat ameliorated. But in the final analysis, the agency head who goes this route must be prepared to anticipate some difficulties from within his organization. (Staffing problems are discussed in detail in chapter IV.)

The returns, however, should be worth the price. Some of the benefits, of course, will be less than obvious. An improvement in analytic potential is not something easily measureable, particularly in a field such as fighting organized crime, where victories come rarely and the advances of the enemy often go undetected for years at a time. But if the analytic component of the intelligence unit has been selected with care and discrimination, a more vigorous intellectual tone in the workings of the unit should soon emerge and the effectiveness of the unit should improve.

### **LOOKING BEYOND THE LA COSA NOSTRA IMAGE**

One major objective which the unit commander should have in mind in strengthening his analytic component and adding specialists to his staff, should be to widen the unit's concept of what organized crime is. He and the unit must look beyond the traditional "Mafia families" or La Cosa Nostra imagery to the organized criminal networks that may characterize the 1970's.

It is not possible now to predict the forms that organized crime will assume throughout the country over the next decade, but it is possible to say with some conviction that they will be different, and certainly more complex. The ethnic composition of criminal groupings is changing; more overall heterogeneity can be expected as mental dexterity displaces brute force and violent codes of discipline. Finally, the law enforcement agency that stays with the old-fashioned emphasis on specific ethnic groups and "families" will be unable to move to a strategy based on attacking identifiable illegal activi-

ties and eliminating them as discrete functional operations. After all, it is criminal enterprise that constitutes organized crime, not necessarily a homogeneous ethnic association.

There can, in other words, be little comfort for the law enforcement agency head who has felt himself fortunate over the years that no "family member" was located in his jurisdiction. The presence of industrial or commercial wealth may be as sure an indication that organized crime is at least viewing his city with interest as the visit of a notorious "capo." White-collar crime is on the rise. On the other hand, large concentrations of disadvantaged poor in a defined and compacted sector of the city may attract those always ready to exploit the defenseless and uneducated. Only an imaginative and sophisticated intelligence unit can be cognizant of changes as they occur—changes in the nature of criminal organization and makeup, as well as changes in the susceptibility to crime of certain areas of the city.

### **THE ROLE OF THE COMMANDER OF THE INTELLIGENCE UNIT**

The final word in this introduction must emphasize the role and responsibilities of the intelligence unit's commander. In most cases it is he who must take the initiative in improving his staff, in fighting to insure that he has unfettered access to the agency head, and in educating the agency as a whole to what it can gain from the activities of his unit.

The commander of the intelligence unit is in a unique position in the agency. He will normally be somewhat junior to other principal officers with access to the chief. In many cases, he will have to take energetic action to preserve his unit's independence without antagonizing others who might nominally consider themselves his superiors. In particular, his people may develop information pointing to corrupt acts on the part of members of another element of the agency. He must in this and in all other cases take actions that reflect the impeccable integrity of his unit and himself.

In the struggle for the allocation of resources, it is the unit commander who must prove his case. And his case will be more difficult to prove than other unit heads, because he will not be able to point to numbers of arrests or other con-

crete indicators as measures of his unit's success. Indeed, he may have been working closely with other jurisdictions, giving them developed cases, since the statutes of his local jurisdiction are inadequate for successful prosecution. In any

event, it is up to him to come up with a sufficiently convincing picture of the extent and nature of the threat of organized crime operations in his jurisdiction to gain support for his unit.

# Chapter II

## THE INTELLIGENCE PROCESS

*Intelligence is a process made up of a series of interconnected functions or activities: collection, evaluation, collation, analysis, reporting, dissemination, and reevaluation.*

*Collection is the gathering of raw data or information which in its raw state or in a finish analytic report becomes an intelligence input to law enforcement activities.*

- *Collection must be planned and focussed to be effective.*
- *Collection activities include both overt and covert methods, and the utilization and coordination of nonintelligence elements of law enforcement agencies.*

*Collation is the first step in the process of translating information into intelligence.*

- *Collation is more than simple storage of materials in files.*
- *The information must be evaluated, arranged in files so that it can be rapidly retrieved, and cross-indexed so that relationships between data elements can be established.*

*Analysis is the function that assembles bits and pieces of information from many sources and puts them together in such a manner as to show pattern and meaning.*

- *The hypothesis is an important tool of the analyst—it is tentative statement of the meaning of a collection of information when arranged in a logical manner.*

*The end product of the intelligence process is an intelligence report—it may be long or short, it may be oral or written, it may be used for planning or for enforcement action.*

*Essential to the management of the intelligence process is the function of reevaluation.*

- *The unit commander must continuously review the functioning of his unit and must seek feedback from his consumers, especially his agency head, as to effectiveness of his operation.*

### INTRODUCTION

-Intelligence can best be thought of as a process. (See figure 7, page 34, at the end of the chapter, which portrays the intelligence process.) It is a process made up of a series of interconnected functions or activities: collection, evaluation, collation, analysis, reporting, dissemination, and reevaluation. The products of each, beginning with collection, feed into and are essential to

the operation of its adjoining function. At the same time there is continuous feedback in play as the performance of functions further down the process indicate that something more should be done in one or more of the prior functions back up the line. For example, should a clear need for more information develop while a report is being prepared, a request can be made to collection, to the investigator, informer, or whatever source is available. This information



when received would go through all steps of the process, through collation and analysis and enter into the report being drafted. The process is ordinarily thought to be completed when the report is disseminated.

However, from the point of view of managing the process the function of reevaluation must still be performed. This function involves continuous review of the operation of the process in order to detect any weak points before they cause major problems. Part of this function is the determination of how well the products of the process are serving the consumer—this is known as feedback and is the final act that in fact closes the loop of the intelligence process.

The discussion below will focus in turn on each of the several functions of the process. But this should not create a misconception that an intelligence unit in operation should be rigid and highly compartmentalized. The intelligence process is dynamic, and in most units personnel involved will perform more than one function. It is often difficult to separate neatly one function from another. Finally, the commander of the unit, the manager of the process, will be making daily decisions regarding one or more of the elements of the process. These decisions could call for a shift in collection efforts, a change in the filing system, a different focus in analysis, a modification of the reporting, or perhaps only changes in dissemination.

Many who are involved in intelligence tend to forget the components that make up the total process. As each person focuses on his own part of the process or as several parts or functions are performed by one person, the distinctions between the elements blur. An individual may be aware that he is performing several particular functions, but he may not be able to discern where one component in the process ends and another begins. It is vital to understand each specific function in order to design the most effective system for the total process. This is not to say that there need be a separate office, much less a separate person, to do each function. But it is important that an intelligence unit be aware of all specific activities to be performed, and, therefore, confident that each is being performed as efficiently as possible.

Regardless of how efficiently the system appears to be operating, if the final product, that is, the report to the law enforcement agency

head or the ultimate consumer, does not convey to him the extent of knowledge and the conclusions of the intelligence unit, then the system as a whole has failed.

## COLLECTION

The first function, collection, is the one that is normally explicitly recognized by all. Some may not call it collection; it may be called investigatory reporting. It may include the soliciting of police reports and reports from informants. It may include taking notes on public documents, listening to electronic surveillance gear, and many other activities which are parts of collection.

Information resulting from collection activities can generally be categorized according to its end use. But it should be noted that items of information may fit into more than one category, being used in several different ways. The four general categories are:

1. *Indicative or premonitory intelligence.*—Information in this category is that which suggests new developments or new operations by organized criminals. It may be fragmentary and often impossible to substantiate immediately, or it may be hard facts. It can be included both in a report of indications of new developments or filed to await further information that confirms or disproves the trend or event it originally suggested.

2. *Tactical intelligence.*—The distinguishing feature of information in this category is that it has an immediacy in calling for action. Since the intelligence unit should not be an action unit, this type of information should be turned over to one of the other elements of the agency to be acted upon. Tactical intelligence can lead to an arrest, or it can lead to further information gathering and a subsequent arrest. Information of a tactical nature can also be filed to be used in one of the other categories as noted below.

3. *Strategic intelligence.*—Information in this category is that which is collected over time and put together by an analyst to indicate a new (or newly discovered) pattern of activity by organized criminals. Some of the information on persons and functions may already have been used in an indications report or as tactical intelligence. The information may be confirmed or be in the form of a still unsubstantiated alle-

gation. The pattern into which the information is fitted may be an hypothesis based on fragmentary data. The importance of information that enters into strategic intelligence is that it is used by the head of the agency in planning the strategy of his agency or the allocation of his resources over a period of time in the future.

4. *Evidential intelligence.*—As the name indicates, the information in this category is factual and precise. It can be presented in court. Whether and when it will be used depends on other elements entering into the case building. Decisions on case building are normally not in the hands of the intelligence unit but in those of the action elements of the agency or of the prosecutor. This kind of information may be filed to be used in developing a strategic report, or it may have tactical value and be currently useful in a case that is being pressed.

### Planning the Collection Function

Collection to be efficient must be focused. It must be directed against a target. The several methods of collection must be coordinated with respect to the target. A coordinated approach to investigating a given criminal activity saves resources by avoiding duplication of efforts. It commits the collection system with the best chances of success to the task. Collection planning also takes into account data that are on hand and insures that additional collection is directed at gaps in the information; good planning avoids the waste of laying on a new investigation to cover old ground. Collection planning should be reviewed at different phases during an investigation. During the early, exploratory phase the type of information desired is less exact than that which will be required during the latter stages when precise evidence is needed. Regardless of certain traditional views, namely, that the course of an investigation can be directed intuitively by "gut feeling," the resources available to any one department are too limited to permit such an approach.

### Example of Collection Planning

To emphasize the importance of collection planning, consider the following outline of a developing situation:

Investigator Able, in line with a general instruction, keeps an eye out for any activity

of known criminals involving auto supply stores. During the course of a period of a week, he spots Hood Zeke and Hood Walzak in two different auto supply stores. In each case they seem to be in deep discussion with the store managers.

Investigator Able reports his findings, adding that he had noticed some change in the composition of customers in one of the two stores. (Indicative intelligence) Lt. Harry, commander of the organized crime intelligence unit and the immediate superior of Investigator Able, calls a meeting of his analysts and investigators. The lieutenant decides after the meeting to write an alerting memo to his agency head. But at the same time he advises his crew to keep at their normal tasks, not to change their pattern of work until Able's report is evaluated.

The lieutenant does go ahead and contacts his friends in the DA's office, the U.S. Attorney General's strike force, the representative of the State police in the agency, and the inspector in charge of burglary. The DA tells him of an increased number of reports of car strippings. The inspector of burglary tells him of several hijackings of automotive supply items, items which could be retailed easily through auto supply stores.

The lieutenant reports his findings to the agency head. On the basis of the findings to date, the agency head decides to place the auto supply stores on his target list. However, it is to remain low in priority. He has promised the DA to press as hard as possible on gambling in the next few weeks, and has also agreed to help the State police in their efforts against three suspected cigarette smugglers (the tax in this particular State is 5 cents higher than it is in surrounding States). In addition, he has promised to lend a few men to assist the Federal strike force as they develop a major case against a syndicate leader whose home base is in a major city some hundred miles away. The agency head does agree however, that all patrol personnel will be asked to report on activities in and around auto supply stores while they are on their normal patrols.

On the basis of the agency head's decision the lieutenant increases to two the number of investigators directly committed to auto

supply stores. He also directs one of his undercover agents to apply for a job at one of the stores first visited by Able. But all the rest of the Lieutenant's assets are committed to the higher priority items as determined by the agency head.

(At this point, the situation would be out of hand if the lieutenant had jumped at the flood of information developed by his crew regarding the auto supply stores. His assets would have been misapplied since the head, as principal policymaker, knew of other more pressing requirements. It was apparent to the agency head that the auto supply case could be handled as a slowly developing situation and, thus, should receive a lower priority in terms of manpower applied.)

The lieutenant now receives word from his undercover agent employed at the auto supply store that the store has, in fact, become an outlet for stolen goods. He further determines that the payoff is made to a recognized underling of the syndicate. Again he reports to the agency head, this time urging that the problem be assigned a higher priority.

(We will not follow this problem any further! However, it serves to point up the problem of determining priorities: the importance of information looks different from different levels of command. It points up the problem of accepting requirements from outside the department when resources are limited. It suggests that some problems may have an importance derived from the political situation; this cannot be overlooked if the context is to be stated honestly. But most of all, it shows bluntly how planning must be applied to the limited assets that are available to any department or element engaged in law enforcement.)

### Collection Methods

Collection can be broken down into two general areas: overt and covert. Overt and covert refer to the means by which information is collected.

#### Overt Collection

The intelligence unit should be prepared to use all sources available to obtain data on organized crime. These include not only information developed by investigators assigned to the

unit, but also reports by the general force—that is, the patrolmen and the detectives, and extra-departmental sources. The latter can be the district attorney's office, investigators for other elements such as a crime commission, and open sources including newspapers, public trial records, congressional hearings, legislative hearings, crime commission hearings, etc. The intelligence unit should also seek to encourage the public to write letters pointing out activities that are illegal and that suggest corruption of public officials.

#### *Investigators*

In general, the single most effective overt collection source will be the investigators assigned to the intelligence unit. The word "investigator" as used in the manual refers to any officer who collects information in the field for intelligence purposes. Where he comes from—burglary squad, vice squad, narcotics, or directly from uniformed ranks—is less important than what he does for the intelligence unit. He is a fieldworker gathering data on organized crime figures and enterprises. In some jurisdictions he may be called an intelligence officer or an intelligence agent. (Throughout this manual the term "investigator" is employed to distinguish the activities of the fieldworker from those of the analyst, who generally remains in headquarters. Both are intelligence officers in the sense that they serve the intelligence unit.)

It is the investigators' function to develop the indications of criminal activity contained in the inputs collected from one or more general sources. Investigators check out reports obtained from informers, especially those whose reliability is untested or believed not to be high. In conjunction with the analyst (be he an individual with such a title, the sergeant in charge of the files or the officer in charge of the unit) they increasingly sharpen the precision of targeting as the investigation changes from a "looking into the situation" to the compilation of a study in depth or to a gathering of evidence for prosecution. (See chapter V for a discussion of investigator training.)

Every effort should be made to develop report forms that are simple and will encourage the investigator to put all his findings down as a matter of record. The aim should be to get his observations on paper (or tape) while they are

still fresh. The analyst may then be able to add a new dimension or recommend another approach to the investigator. This is not to suggest that investigators should be discouraged from thinking analytically while conducting their investigations. The more analytic the investigator's report, the more useful it will be.

#### *Information from nonintelligence units*

With regard to reports from elsewhere within its own agency, the intelligence unit should seek to work out specific forms to be used by the patrolmen, patrol car officers, detectives, desk sergeants, etc. Special efforts should be made to encourage the men in other units to report any activity which relates to organized crime. (See figure 2, page 16, for a sample form with questions which might be asked. See also chapter V where further suggestions are outlined to help in developing the flow of reports.)

Any new information entered into the general files of the agency's records section referring to organized crime activities or personnel should be made available to the intelligence unit. To systematize this, flag cards can be placed in the general files against the names of major figures in organized crime. Another approach is to have a standing order requiring the passage to the intelligence unit of any information which relates to known organized crime activities—gambling, narcotics, prostitution, usury, etc.

Routine patrol units can be particularly useful in assisting in the daily collection of data. These units should report activities noted at the residences or places of business of known organized crime leaders. For example, car or foot patrol personnel could be asked to record any unusual event taking place at these locations, to record the license numbers of any cars that are parked at these addresses, and—to the extent that they are known—to report by name the people who frequent the particular house or office. This is an example of a source of information which is relatively cheap to get, but can be useful through time as it builds up lists of known and unknown associates that can be categorized through license numbers. It can also become a source of initial indications of interconnections if license numbers are noted at one or more of these leaders' homes or places of business. (See figure 3, page 17, for a sample report form.)

Of course, this system would be less effective in downtown areas where there would be difficulty in associating parked cars with a specific building. Moreover, the increased use of rental cars by organized criminals makes more difficult the linkup between the car and the person using it. Nevertheless, the presence of rented cars in the vicinity of known or alleged organized criminals' homes or places of business should be treated as a valuable piece of intelligence information. For example, it can be used to trace back to the rental agency that is being used most often, and the cooperation of that rental office can be requested. If a greater effort appears to be merited, this type of patrol surveillance can be augmented by photographic and fixed surveillance.

There are many different methods for developing the source of information represented by the patrolmen in the districts. Three are suggested here.

1. *Patrol units whose area encompasses known residences or businesses of major criminals are requested to note any activity, including license numbers of cars in the area, on a special report form* (see figure 3, page 17, for a sample form).—This should be done each time the address is passed. Such a routine check has the advantage of keeping in continuous, though periodic, surveillance on desired locations without requiring that an investigator be detached on a special mission. It also has the advantage of using the patrol car or foot patrol which, because it is known in the area, will raise no suspicions of surveillance.

2. *The intelligence unit encourages reporting by singling out active, observant patrolmen.*—The intelligence unit should review activity reports of patrolmen in areas of special interest. Where these indicate that a patrolman is showing particular zeal in his job (measured in part by his reports on persons stopped for questioning), he can be contacted for special treatment. He can be praised and given additional information to sharpen his efforts. He can be asked to contact the intelligence unit directly on matters of interest (though also being encouraged to keep his district commander or supervisor informed).

3. *Shift-change formations used to request specific help.*—A representative of the intelligence unit can meet with the patrolmen before

FIGURE 2.—Sample intelligence report form for use by nonintelligence units <sup>1</sup>

INFORMATION REPORT FOR INTELLIGENCE UNIT		
Date:	Time:	Location:
Reporting officer and unit:		
Type event:		
Names of persons involved:		
Any identification material noted: (Licenses, telephone numbers, serial numbers, identification numbers, etc.)		

<sup>1</sup> This form, not shown at actual size, should come in a pad and be printed on colored paper. The distinctive color used for all nonintelligence unit reporting to the intelligence unit emphasizes the special, and at the same time important nature of this function.

they are dispatched on their shift. He can tell them about his problems and items of special interest, that is, who or what is most important in terms of information desired. He can also meet with the shift coming off duty and debrief those with specific information. (See below for a discussion of debriefing.)

Regardless of the approach adopted, two features should be present. First, it should include the use of a special report form such as shown in figure 2, above. This form should only be used where the officer will not fill out another form such as an arrest form. Second, the intelligence report should be routed directly to the intelligence unit (lateral distribution within a precinct or district or up through the patrol channels can be done where required—but this should not prevent the initial direct distribution of the report to the intelligence unit). This second feature is important since it will avoid clogging the main command communication channels with intelligence information and reports. It will encourage the intelligence unit commander to make contacts with the patrolman for followup, to encourage him to do more and, where indicated, to elicit more information about the event reported. But, most important, it insures a rapid, timely, direct flow of bits of information to the intelligence unit.

Finally, the intelligence unit should press for the allocation of time in the various training courses, including rookie classes, to describe organized crime and the way intelligence is put to work against it. This is essential to make sure that the force as a whole knows the nature of the problem and appreciates that each member can help in the fight. (Training is discussed in more detail in chapter V.)

#### *Securing information from other jurisdictions*

In many, if not most cases, other jurisdictions must be contacted for information. For example, where an organized crime ring is operating both within a city and in its separate jurisdictional suburbs it will be essential to ask for assistance. Where there is to be a major exchange of information between two jurisdictions, it is often useful to appoint officers to act in a liaison capacity. These officers can expedite the transmission of data between the units, and they should be responsible for keeping both departments aware of the progress of the particular investigation. This technique becomes an ideal way for developing personal connections which can serve as a basis for trust between the departments involved. (See chapter III for a more complete discussion of this problem.)



from other areas can also be a useful device to jump the information flow over jurisdictional boundaries. The possibility of controlled exchange of information with more trusted newspaper reporters should be considered.

The more usual method for obtaining information from newspapers (and other periodicals) is to clip articles and to file them, making cross-references where appropriate. Clipping can be done either by a member of the intelligence unit or by a clipping service. The cost of the two should be compared relative to the output in a particular unit, and a decision reached as to the best method. However, when relative cost favors the clipping service (still a high-cost item), care must be taken in developing the contract to be sure the correct materials are clipped and that important items of interest are not overlooked.

Instead of clipping, the staff of an intelligence unit can be called upon to abstract articles in periodicals. In this manner important points can be highlighted, and file bulk reduced. Effective, concise abstracting can be done by experienced personnel almost as rapidly as clipping, and the end product in many instances is easier to use. A file of newspapers going back over 12 months could be maintained in the event the full text of the subject article is ever needed (or the public library or newspaper office files can be relied upon).

Whether in clipping or abstracting, attention should of course be given to any items about known or suspected criminals and their associates—their marriages, deaths, and the higher educational focus of the children of organized criminals. But attention should also be given to stories suggesting new opportunities for organized crime or changes in operation or management of businesses indicative that criminal involvement has already started. The potential new fields are as varied as the economy and the demands of a high-consuming and pleasure-loving people. They include real estate, banking, manufacturing, insurance, trucking, trash hauling, retail stores, restaurants, etc. The intelligence newspaper reader should be looking not only for names of known criminals, but also for their lawyers, the banks they use, and companies in which they or their associates have an interest. He should also be looking for major deals in which a great deal of money is involved, deals

that can be considered as “honey” attracting criminals. These criminals have the funds available to buy into legitimate deals, but they almost always make their transactions through fronts. Thus, efforts should be made to discover the names of these financial fronts. Newspaper stories on city requests for bids and those companies replying should also be explored for any suggestion of organized crime participation, directly or through one of their “legitimate” fronts.

Other excellent sources of intelligence data are public records and documents—for example, trial records and grand jury proceedings (to the extent they can be made available). Records of this type provide indicators as to activities and associations of organized crime characters other than those who were directly involved in the particular trial at hand. The intelligence unit should be aware of—and review the output of—local, State, and national crime commission hearings, and investigative hearings by State and Federal legislators. Again, such hearings tend to provide indications intelligence rather than evidential, but important leads can be developed from the relationships that may be presented.

The intelligence unit should also use all available sources of financial information—local stores, bonding houses, banks, insurance companies, etc. The specific amount of information that can be obtained formally will depend on State laws and local ordinances. However, informal approaches can often produce useful leads which are especially valuable in the early stages of an investigation. Another excellent source of indicative as well as evidential intelligence is telephone toll charges.

The intelligence unit should also make contact with State and/or local agencies, such as those responsible for overseeing the operations of banks, hospitals, insurance, mortgage and deeds, corporations, etc. A list of names, including criminals, their associates, lawyers, and front organization men can be given to these governmental staffs (or one of their members who is willing to help and is known to be honest) with a request that notice be given whenever an activity involves any name on the list.

#### *Complainants*

Mention should also be made of complainants. These are persons who either appear in person

at the various police departments or prosecutors' offices, or who write letters, signed or anonymous. They complain about questionable situations or activities or they cite illegal acts by a person or persons. The complainant is often one whose legitimate occupation places him in a position to see, hear, and possibly record facts of value concerning a crime. He will reveal this information as a matter of civic duty. However, unless the particular complainant is known, the information must be checked out by the intelligence unit's own personnel before its reliability is assessed.

The complainant is different from the informer. The latter is a person whose mode of living, habits, and personal relations place him in contact with criminals. His identity must be kept secret for his own protection and in order to maintain him as a source. The intelligence unit should be alert to the possibility of recruiting as informers those complainants whose information is generally accurate and useful. The use of informers is discussed in the next section.

### **Covert Collection**

Covert collection is the acquisition of information from a subject who is unaware he is being observed or overheard, although he may suspect that he is a target. If covert collection is used effectively, his suspicions will not be confirmed until it is too late; he will continue to perform his illegal activity and to speak and act with a degree of confidence. Even if he suspects that he is being observed or overheard and attempts security measures as a matter of prudence, the probabilities are high that as long as he does not know for a fact that he is under observation, he will make mistakes.

Covert collection methods are essential if evidence that can be used in court against organized crime leaders is to be obtained. These leaders make every effort to avoid being directly associated with the criminal acts committed by their underlings, and normal police surveillance and investigations are not enough to unearth the connections between the leaders and the crimes. Evidence is needed to prove that the leader issued orders for or received money from the act. In sophisticated penetrations of legitimate business, involving such illegal acts as unfair business practices, illegal restraint of trade, and

fraud, the connectors may be even more difficult to discover. Fronts will be used; individuals acting as though for themselves may in fact be under the control of a criminal. There can be several cutouts, or persons, between the crook and his business front.

Covert collection is expensive in terms of manpower. This is the case whether physical surveillance or electronic methods are used. In both instances investigators must focus on the particular operation at the expense of investigating other potential sources of information or pursuing several leads. Special precautions must be taken to insure that the covert operation remains covert. This also requires time and effort. In most cases, the operation will be run on a three-shift, around-the-clock basis. Thus, any decision to resort to covert collection should require a specific decision by the unit commander. The commander must weigh the value of this use of the unit's manpower not only against the importance of expected information but also against the potential merit of other tasks.

### *Physical surveillance*

Covert physical surveillance is the observation of the movements of suspected criminals without their knowledge. The purpose of the activity is to discover associates, places visited, and activities engaged in by the subject (insofar as it is possible). Surveillance may include foot, auto, and stationary positions by intelligence investigators. Because organized criminals are sensitive to the probability of being watched, most surveillance operations require several investigators in order to conceal their coverage.

Physical surveillance by itself has certain limitations. Although it can indicate a pattern of movement and a pattern of associates, it may fail to uncover the purpose of the movements and of the meetings with associates; what is being discussed with associates is usually the vital matter.

Accordingly, other methods needed to supplement physical surveillance may have to be brought into play. Such methods could include electronic surveillance or the use of informer or undercover agents. These are discussed below. Where possible, and where it is deemed essential, a photographic record should be made of important meetings (or at least of the persons



going into the meeting place), of cars used, of other places visited.

### *Electronic surveillance*

The principal means of covert collection against organized crime operations is electronic surveillance—wiretap, eavesdrop, or body recorder. Many believe that effective action against leaders of organized crime can be taken only if electronic surveillance is permitted. Physical surveillance can determine who is meeting in what building. But knowledge of what is done or said at the meeting can come only from an eavesdrop (or from a person present). Because both planning arrangements for meetings and fund pickups and orders to underlings must be communicated, the telephone is essential to organized crime. Wiretaps can make this flow of communication available to the law enforcement agencies. (The trends in law relating to the use of electronic surveillance are discussed in appendix A.)

The racketeers have tried many dodges—use of third person and public telephones, attempts to maintain strict security in conversations, substitution of code names for persons and places, etc.—but none of these has been totally effective. By the use of physical surveillance, or through informers or undercover agents, phones used by the leaders can be identified, and sufficient data then developed for a show-cause order to obtain court approval to tap the phone in question. Even in supposedly guarded conversations, slips are likely. Perhaps the most important contribution of electronic surveillance is the evidence it provides of a direct relationship between a crime leader and an illegal act—evidence that often can be obtained in no other way.

When electronic surveillance is permitted, plans should be made to exploit leads and indications beyond the specific case under investigation (due account being taken of the limits set by law). This will raise personnel and workload problems, especially where the investigators who maintain the wiretap must translate the information onto a typed report. But the amount of information obtained can be worth the effort. One helpful approach might be to acquire specialists in translating tapes. Perhaps one or more typists should be trained to understand voices and the use of tapes, and then to transcribe the material.

Once some form of electronic surveillance is decided upon, the actual operation should be turned over to experts. The eavesdrop operation in particular calls for skillful application. Proper equipment should be used and the tap or eavesdrop placed in the most effective position, a position that can be occupied without disclosing its existence to the suspect. Consideration must be given to potential noise sources that could blanket any conversation. The sophistication of the suspects must also be considered; what is the probability that they will know how to examine a room effectively in searching for a possible listening device?

### *Informers*

Another major source of covert intelligence information is the informer. The importance of this source is indicated by a saying common among law enforcement officers: "An officer is just as good as his informers." The informer is a person who is not a member of the department or staff but who is part of the scene where organized criminals operate, and who is willing, for whatever the reason, to provide information. The information furnished by the informer is normally considered raw material which must be checked out. (A possible exception exists where an informer has worked in position for a number of years and has come to be trusted.)

In most cases the informer will want direct compensation for the risks he is taking, but occasionally an informer can be developed on a basis other than payment of money. The informer who does not work for money may be providing information in order to gain revenge on some member of his organization. Or he may have been caught in a compromising situation and may agree to give information, if a crime is involved, in return for a lesser sentence (in the case of police this would be a promise of intercession with the prosecutor). Or he may simply enjoy his police contact—because he trusts him and feels that he is a good man. In some extreme cases he may want a promise of assistance in moving to another area should his cover be blown by inadvertent actions or by his having to surface to give testimony. In the final analysis, regardless of the kind and amount of reward, the maintenance of a good informer depends basically on his belief that his contact is being honest with him in all matters.

The payment of money to informers raises serious problems for the department. A fund for this purpose must be approved by the financial unit of the agency. Then there must be an agreement reached on safeguards, so that the use made of the funds can be checked. Safeguards could involve receipts or the presence of a witness when the paying officer passes the money to the informer. Sometimes, however, an informer may be so suspicious that he will work with only one person he knows in the agency and will give no receipts. The decision on the accompanying risks versus the value of information will have to be made on a case-by-case basis. Information on crime leaders can be expensive and usually becomes more so the higher the level of target. It appears that despite the problems, the effort to get a substantial fund for informers is worthwhile.

There are two approaches to management of informers. The traditional approach is to maintain no central record, and, in fact, no recorded identification of the informer other than his association with the detective or investigator to whom he is willing to confide his information. This preservation of anonymity takes into account the nervousness of the informer and his concern that word of his actions might get back to his friends.

A more systematic approach is followed in some intelligence units—the central registration of the names of informers. But even though such a list is handled with the utmost security, the fact that it exists concerns informers, and in some cases informers have refused to operate under these circumstances. Where the list-of-names system is in effect, the only reference to informers in reports must be by number, and the relationship between number and name must be known only to the unit commander. The value of this second approach is that it obviates the possibility of an informer selling his wares to more than one person in one agency or to several agencies. It also assists in the evaluation of the report since more than one person (other than the investigator running the informer) knows who the informer is and can form an independent judgment through time as to the validity of his reports.

Consideration should be given to the possibility of upgrading informers. In some cases, the judicious use of feedback information to an

informer may help him to be promoted within the ranks of the organization to which he belongs and thus improve the quality of the information which he contributes. It should be noted, however, that there are problems with this approach; one of the greatest is that the informer in his new position may be called upon to commit a major crime, a crime for which the enforcement unit could not avoid arresting him.

#### *Undercover agents*

Another covert source is the undercover agent. He is a law enforcement officer operating clandestinely on the fringes of an organized criminal group. He ordinarily takes on the coloration of a hanger-on in the same bars and restaurants as are frequented by the gang, or he works in their enterprises. He might also become a minor operator, such as a runner. However, since the gang normally requires that each of its members has committed a major crime—armed robbery or murder—it is almost impossible to conceive of inserting an undercover agent into the hierarchy of a major criminal group. Depending on the calculation of the risks involved, the undercover agent, as well as the informer, can be made more effective by wiring him for sound so that he picks up the various conversations that he enters into or that go on around him.

Money is also a problem for the undercover agent. He must have funds available for entertaining, for purchase of stolen goods, for buying drugs that are offered, for gambling, etc., and these funds must be so allocated and controlled that the undercover man has them available when he goes into operation. If he is to escape suspicion, he cannot find someone to sell him stolen goods, and then say he has to go back to the bank and get the funds. The requirement for funds is a significant problem, especially for smaller police units and prosecutors' offices.

#### **Evaluation of Intelligence Inputs**

Evaluation can be divided into two parts. The first is a judgment of the validity of a particular piece of information whether it be written or verbal; that is, the extent to which the information is factual. The second part of the evaluation is an assessment of the truthfulness and reliability of the source. A source of high reliability may indicate that the report he is transmitting is rumor or secondhand and that its

validity should therefore not be accepted with full confidence. The person in charge of the intelligence unit must decide how best to relate this report to other reports he is receiving from a number of directions, some from men of his own squad, some from other members of the agency, and some from people outside of the agency, including ordinary citizens sending in complaints or persons wishing to become informers.

Evaluation as a function consists of two major activities. Initially, the commander of the intelligence unit evaluates reports containing leads and indications to determine which require a followup by his own investigators (or to request help from others where necessary), and which can be filed until something further develops. This evaluation or review can be related to the further development of evidence in a current case, as well as to indications of new activity by organized criminal figures or new associates of known criminals. Evaluation related to an action decision is common; it is performed daily in intelligence units without the function necessarily being identified as evaluation.

The second activity of the evaluation function is the explicit grading of the worth of the source and of the substance of his information. It is performed too infrequently in general practice and, in fact, is often not regarded as a necessary procedure. Each piece of information must be evaluated and it must be evaluated when filed or it will often be too late—the persons involved or the circumstances may be forgotten. Proper evaluation requires some means of transmitting the assessment of the worth of a piece of information to all subsequent readers. When a file is pulled, whether a day or a year later, it is unlikely that the person so doing will know about all the reports in the file, or will have immediately available the men who might know. Therefore, it is necessary that an intelligence unit establish some means of indicating evaluation on each item of information.

The evaluation system can be simple. Color of paper can be used to indicate general source: inside the agency, patrol, detective bureau, precinct, or vice squad; or outside, including other law enforcement agencies, complainants, informers, etc. Or a letter or numerical code can be used. But an evaluation of the source, regardless of who he is, should be given. Then,

and of equal importance, there should be some indicator to tell the reader how reliable the content of the report was assessed. The system should allow for separate evaluation by all knowledgeable persons involved such as investigators, other informers, undercover agents, the analyst in the intelligence unit, and finally the unit commander himself. This is not to say the system should force evaluation on everyone listed above. Only those with definite knowledge of the source or substance of a report should contribute to the evaluation. On the other hand, the more contributions the better. The views of officers at different levels in the agency or information chain who may have had different experiences or relationships to the person or subject of the information report will enrich the report and facilitate its overall evaluation. (See figure 4, page 23, for a sample of a classification system.)

It is also important to apply the evaluation system when a report for the agency head or for the prosecutor is compiled. It is essential that the consumer have some concept of whether the particular item that is being brought to his attention is rumor or fact or something in between, possibly true. He should know if it is a potential piece of evidence. He should also know the source from which it came. In order to protect sources, it would be most appropriate to have some sort of a lettering system to indicate whether the material came from a policeman on patrol, an informer, an undercover man, as a result of electronic surveillance, or from a letter written in by a citizen. To protect identity, the person giving the report, if asked, could tell the agency head the specific source of the material.

### Collation

In a sense, the intelligence produced by the many collection efforts can be considered as no more than information. Intelligence is not so much a kind of information or data, but rather how it is analyzed and used. In large measure the word "intelligence" is more applicable to the finished product of the total process. The subject of this section, collation, is the first step in the process of translating raw information into intelligence. Collation means more than the simple storage of materials in files. It includes the sifting out of useless or nonrelevant

FIGURE 4.—Sample evaluation system—reliability of source and content of information

1. General source of information can be indicated by a color tab, for example:

Intelligence investigator .....	Red.
Intelligence unit, informer .....	Red cross-hatching.
Other intelligence units .....	Red dots.
Other elements, same agency .....	Green.
Other elements, other agency .....	Green dots.

Or a tab can display a number, figure, or letter to indicate general source of information. Or the two can be combined with the color to show general type of agency and with number, figure, or letter to show element within an agency.

For example:

Other element, same agency—burglary squad..... Green tab with large B in the center.

2. Specific evaluation to source and content of bit of information can be provided by a combination of letter and number indicators, for example:

<i>Source</i>	<i>Content of information</i>
1. Highly reliable.	A. Factual.
2. Usually reliable.	B. Views of reporter.
3. Not often reliable.	C. Heresay/unsubstantiated allegation.
4. Unknown.	D. Unknown.

Thus, a report from a source that is considered usually reliable and containing some unsupported statements would be classified on the report as being 2-C.

3. The system could be expanded to indicate a further classification for the source, for example:

- 1. Highly reliable
  - 1a. Highly reliable informer
  - 1b. Highly reliable intelligence investigator
  - 1c. Highly reliable officer, other element of agency

Thus, a report from an informer that was considered highly reliable and contained factual information would be classified as follows: 1a-A.

or incorrect information, the orderly arrangement of collected materials so that relationships between apparently disconnected data elements may be established, and the creation of a system for rapid retrieval of stored (filed) information.

### Filing System

At the heart of collation is the system for filing the information gathered. It is essential that the information being reported is filed in such a manner that it can be easily retrieved. This is basic. But just as important, the information must be filed so that it can be related to other information of a similar nature. In other words, it is not sufficient to keep filing reports on Joe Hood in his jacket file. All this provides is a single source of references; that is, Joe Hood. The reports received on him may convey information about places he frequents, such as bars and restaurants. There may be references to his associates and to other activities. The information in this particular report must therefore be cross-indexed to files of businesses and illegal

activities. It is the overall organization of the files that eventually makes possible effective analysis.

### Cross-Indexing

It is important for indications intelligence to file bits of information by function as well as by a person's name. As information begins to accumulate on the activity of organized criminals in a field where they have not been active before, all such information can then readily be brought out for analysis. But unless this information is filed or cross-referenced as it comes in, it may be lost in the totality of the files because the human memory approach is unreliable at best and may, because of transfers, retirements, or deaths, be totally ineffectual.

Basic to effective collation is a coding system which permits cross-filing and cross-referencing of several items of information on one report, and at the same time assures effective retrieval of the information when it is needed. It is essential that the coding of the material for distribu-

tion within the filing system be performed by one person or by a disciplined group that is responsible for the care and maintenance of the files. It is also important that a systematic approach is used in the classification of information under whatever index coding is adopted. There must be uniformity in this matter so that when queried, the files will turn out the information desired. This can only be achieved through precise and systematic classification as reflected in the index to the files. In addition, the files must be structured so that material from confidential sources, or that is in itself confidential, can be restricted only to those with a need to know. (See chapter III for further discussion of the handling of confidential or restricted information.)

### Mechanical Filing Aids

Because of the increasingly complex operations of organized crime, any action against it will require improved systems of collating and retrieving intelligence data. The filing system should be developed so that it is susceptible eventually to mechanization. Microfilm filing and retrieval of reports, the use of punchcards to correlate material by function, or the use of automatic data processing are some of the approaches that might be adopted. To prepare for the use of mechanical means it is also necessary to have a format of reporting that is conducive to the particular system desired. For example, on some forms it is very simple to add a numerical code to each information box. This information can then easily be placed in a computer and retrieved as needed.

In many jurisdictions the proliferation of organized criminal activities has run ahead of the capacity of the local filing systems. Filing systems based largely on names connected with gambling can do little to assist in ferreting out organized criminals as they take over an economic area such as cleaning, scavenging, wholesale meat, etc. Files in which the bulk of the information is kept in original handwritten reports may be of marginal effectiveness when the correlation of data from many different reports is essential.

These problems indicate that in some areas serious consideration will have to be given to the use of mechanical aids, such as automatic data processing. This raises a host of new prob-

lems revolving around cost and the restructuring of files and inserting the information into the machine. If the law enforcement agency does not have a computer, the risks of using a non-dedicated computer on a share-time basis must be weighed. The security problem exists and must be lived with if the value of the data processing approach is considered essential. (The use of automatic data processing and its attendant problems are discussed in more detail in appendix B.)

### Analysis

If there is a heart to the intelligence system, it is the analysis function. It is this function or activity that converts information into focused finished intelligence. It is the analysis function that assembles the bits and pieces of information that have been collected by many different collection systems or from various sources and puts them together in such a manner as to show pattern and meaning. Without the analysis function, a piece of information in the files remains just that. Such pieces are essential to the investigator or detective who is looking for additional information or leads as he pursues a specific investigation. But unanalyzed information tells little about a developing pattern or a potential area of activity of the subject under analysis. (See figure 6, page 33, for a depiction of the analytic process.)

### An Example of Analysis

To emphasize the role of analysis in the intelligence process let us return to our story of the apparent association of a group of organized criminals connected with an auto supply store.

Lieutenant Harry now believes there is enough information for a case to be developed against the auto supply stores on the grounds that they have been receiving and selling stolen goods. He has reached this conclusion on the basis of reports from many different sources, including his own investigators, patrol reports, reports by detectives in burglary, informers, two of his undercover men, the newspaper, and his contact in the Federal strike force. The district attorney is apprised of this information and agrees with lieutenant Harry. At this point, Harry recommends to his chief that another unit of the agency take over the information

and develop the evidence for final case building.

Lieutenant Harry recognizes that the activity he has been investigating may be more than fencing. His problem is to determine whether the fencing operation was only that, or was related to a larger activity including hijacking. He feels it is also possible that the organized crime element in his city is seeking to penetrate legitimate business and to use it for illegal purposes.

In the meantime, Analyst Sam has been reviewing the flow of reporting focused on the supply stores and Hood Zeke and Hood Walzak. In particular, he has noticed from surveillance reports on the auto supply stores: (1) the names of three trucking firms and the license numbers of their trucks; (2) pictures of the drivers; (3) name of the bank where the auto supply store funds are deposited. From a review of the ownership of the stores, he has obtained a list of several names of lawyers and a mortgage company. And from a clerk in the stores he has learned the name of their union and some of its officers.

On the basis of these leads he has queried his biographic and functional files to see what relationship the leads might have to other activities. From his files he discovered the following: (1) the XYZ Trucking firm's president was the brother of "Patsy," captain in the local syndicate. (2) The clerk's union has been reported by an informer to be working closely with the trucker's local, the leader of which was a brother of Joseph, reported to be the head of the syndicate. (3) The hijacking file indicated several recent hauls not only of auto supplies but women's and men's clothing, TV's, and electrical goods. (4) In his file on unions, there are reports that the trucker's local had been negotiating with other clerks and truckers' locals to develop a closer "working" relation. (5) In the mortgage company file, he found the names of several known hoods that had been reported using the PDQ Corporation, and that the PDQ Corporation was one of a complex of holding companies, the ultimate ownership of which was not clear. (6) In the insurance files there were no connections between the subject insurance company and other activities in which there were known hoods.

Analyst Sam has by then developed an hypothesis. (1) It appears that the syndicate is building an interconnecting structure to

encompass both legal and illegal activity. (2) One main objective seems to be to develop control of legitimate retail outlets through which to sell hijacked goods. (3) Another major theme seems to be the use of the PDQ Corporation to gain a relationship with businessmen through the corporation's ownership of mortgages. (4) Finally the syndicate seems to be developing control of clerk and trucker locals to coerce members to conceal the hoods' activities and to coerce the target stores to use the XYZ Truck Line and to buy goods from designated suppliers. (The latter seems aimed at situations where the hoods cannot gain control of the stores but still require an outlet.)

Analyst Sam reports his findings to Lieutenant Harry. Harry, convinced of its validity, lays on a plan to begin investigations to check out the implications of Sam's hypothesis.

(This is as far as this example will be taken. It is intended to point out the important role of the analyst and the requirement that he has available files based on other than biographic classifications so that they can be rapidly queried. It shows in particular the vital role of the analyst in the premonitory or indicative intelligence. By putting together the bits and pieces of information into a pattern, he was able to suggest new areas of organized crime activities. It also shows his responsibility in pointing out further information that he needs to develop a particular hypothesis. Finally, it highlights the role of intelligence analysis as an input to strategic planning.)

### The Role of the Hypothesis

The hypothesis is an important tool of the analyst. He uses it to help establish the meaning (or alternative meanings) of a collection of pieces of information about a particular subject (a gambling operation, hijacking/fencing gang, or whatever criminal activity is suspected, but where the full scope of the operation is not fully understood. The analyst studies the available pieces of information and attempts to assemble them into a logical pattern. In the process, he develops a tentative statement which he believes may describe the operation under review. This is his hypothesis. In many cases, if the information is limited and poorly related, it may fit several logical patterns. Thus, the analyst may develop several alternative hypotheses.

In developing his logical pattern, the analyst must often "construct" activities that he either estimates or assumes should have happened if the overall logical pattern is to reflect what actually happened. These constructed activities may relate to persons believed to be involved. They may describe how an operation is carried out—an operation about which relatively little is known specifically. The constructed pieces of information are inserted into the hypothesis to help reach tentative conclusions.

The analyst must now test his hypothesis. If there is a scarcity of information, the testing must await further collection efforts. If the hypothesis is fairly well documented, then the unit commander will have to send his staff into the field to determine the validity of the logical pattern. In either case, the hypothesis becomes an instrument for levying further requirements on the collection machinery.

The formation of patterns or hypotheses relating to potential major new activities on the part of organized criminals leads to important strategic intelligence inputs. They are included in reports to the agency chief and will serve both to warn him of new developments and to assist him in deciding on future allocation of his resources.

The head of the intelligence unit must keep the analyst and his hypothesis building under review. He must be prepared to stop the effort when it appears that too much time will be required relative to the foreseen outcome, or that new information indicates the developing hypothesis is in fact wrong. Or the hypothesis may point the way to a new area of activity by a group of organized criminals, but fail to connect their apparent involvement with any illegal activities or the breaking of any existing laws. The commander of the intelligence unit must, however, be prepared to support an analyst whose developing hypothesis is uncovering an entirely new area of criminal involvement by ordering an increased collection effort to provide the analyst with additional information.

### **The Role of Research**

One other element of the function of an analyst should be emphasized—research. It is through research that the analyst begins to develop ideas and concepts which later become the basis for hypotheses. The analyst must have

knowledge of how to conduct research. He must develop a capability not only for locating sources of data connected with crime but also within the society in general. Research is critical, especially in the indicative, premonitory stage where intelligence is probing for new patterns, new areas where organized crime may be operating. It is through research the analyst can often best find areas and patterns of operations which may seem lucrative to criminals who are trying to make large amounts of money in a hurry.

The researcher (or the analyst if they are combined) also has an important role to play in terms of the legal aspect of the search for indications. The researcher-analyst should be on the outlook for acts which appear to be committed by organizations associated with the syndicate but are not considered illegal in his particular jurisdiction. Through research it can be determined how other jurisdictions handle similar activities and how a case can be developed for suggested legislation in the research-analyst's own jurisdiction. For example, to cite a common case, in some States usury, or loansharking, is not considered a crime. In such a jurisdiction the research-analyst could, by probing the effectiveness of usuary laws in other jurisdictions, construct a model ordinance or State law on usuary. If his superiors successfully press it on the State legislature or city council, the new law, in turn, could become a weapon for dealing with the activities of organized crime.

### **The Relationship Between Collation and Analysis**

The various parts of the intelligence process should not be thought of as watertight compartments. This is especially true of collation and analysis; the two functions are frequently performed simultaneously, and in some circumstances they are inseparable. Good collation practice requires that the analyst is capable of bringing good judgment and synthesis to an intelligence problem. The analyst is supposed to look beyond the immediate "face value" of an item of information. He must ask, "where does it fit?" "would it dovetail with some other information not apparently related to the immediate problem I'm working on or is it unrelated to the bits and pieces of paper on my desk?"

An example will show how collation consists of a series of judgments, that collation is not as mechanical as it might at first seem.

Let us suppose that Analyst Sam receives on his desk one morning a report from the narcotics squad giving the details of a raid the previous night on a pool hall that had been under surveillance for some weeks. Same is assigned to detecting new developments in organized crime in the area of the city where the pool hall is located. Two well-known pushers were arrested and several other people at the hall detained, questioned, and released. The names of these people were given in the report, along with brief summaries of how they had responded to questioning. Sam, noting that the report had not been routed by information control for Officer Jones, who is charged with probing for indications that a major narcotics figure is moving into the city's dope market, sends him a copy. He then consults the files to determine if they contain anything on the persons other than the pushers in the hall. He quickly "makes a hit." One of the people detailed was mentioned several months ago by a new informer as a recent arrival in town with an eye on the vending machine business.

At this point, Analyst Sam turns to his teammate, Investigator Able, and suggests that he have a talk with the pool hall operator. The next day, Able reports that the pool hall operator, although no symbol of civic rectitude himself, was indeed outraged at several recent attempts by one of his patrons to bully him into changing his vending machine license. He identified the man detained for questioning the night before as the patron in question. Sam does two things: he opens a file on vending machine licensees in the suspect business file and he obtains the report of the informer from the biographic files. To this report he adds the comment that a major item passed by the new informer has been corroborated, and cross-references the vice squad's report on the raid and the report of the interview between Able and the pool hall operator.

Analyst Sam has not only initiated a new line of inquiry (vending machines) and laid a paper base for such an inquiry, he has also made two significant moves in the collation process. He saw to it that incidental intelligence got to an interested party (report of the arrest of the two pushers to Officer

Jones). He also strengthened the credibility of the unit's new informer by indicating officially that some of his information had been corroborated. Any unit officer using the informant's material in the future would now do so with greater confidence.

### **The Analyst-Investigator Relationship**

There should be a close working relationship in the intelligence unit between the analyst and the investigator. While the analyst may be able to develop suggested avenues of investigation and research, it often requires the services of a trained investigator to obtain information under conditions short of a full-fledged investigation. It is important in the premonitory or indicative period to be able to develop information without the power of the subpoena. The latter can only be employed when there is enough information to make it appear profitable to lay on a full-fledged investigation. It is the trained investigator who understands best how information can be obtained in circumstances where he has no legal powers—by discussion, by talking to people, by indirectly approaching the subject.

### **The Intelligence Report**

The word "report" is used in a variety of ways in law enforcement agencies. In its most familiar form it refers to the information dispatched by patrolmen or investigators or even informers to headquarters. Such field reports constitute inputs of information. They are discussed in the section on "collection" earlier in this chapter. It is essential to a comprehension of the intelligence process to understand that the "information" contained in field reports cannot properly be thought of as "intelligence" until it is evaluated in the intelligence unit, compared to other information already on file and possibly combined with other data.

Intelligence reports as used here refer to the end products of the intelligence process. They are the distillations of all the elements in the process prepared in written or oral form. Some may be quite brief, for example a summary of the suspicious activities of a tavern owner to be given to the precinct commander where the tavern is located. Some may be quite complex documents, prepared specifically for the highest consumer, the agency head or the prosecutor.



In any case they should be tailored to the particular requirements of the consumers in question.

The intelligence report must be objective in order that the decisionmaker, the one who determines which future courses of action will be followed, will know exactly what existing information and analysis can tell him. The report should be written in such a way that there is a clear delineation between positive information or facts, those pieces which have gone into developing a hypothesis, and the conclusions which are drawn from both the facts and the hypotheses. In the indicative stage of intelligence alternative hypotheses may be included in the report to help suggest to the policymaker the extent of the uncertainty and also the potential areas in which he may want to lay on further investigation before deciding what his specific course of action will be.

### **Periodic Reporting**

The intelligence report may be a daily or weekly periodic report or a special report called for to cover a specific item of interest or a developing case. The report may be focused on biographic data, it may present the general background on a specific problem or a specific case that is developing, or it may be in a sense an estimate of the situation—the intelligence unit's best analysis of a developing situation indicating where it believes the current trends will lead.

In most cases, intelligence reports should have two parts. One part should be an analytic statement giving the conclusions of the unit's chief (and analyst) as to the meaning of the data collected in the report. This statement is not a summary of the information in the report, but answers the questions: "So what? What does this report mean? Why should I read it?" The reader should be given a concise statement of what the information indicates—certain illegal activities are becoming more important, new lines of investigation are required, an arrest should be made, a shift in priorities should be considered, this week has been worse than last week, etc.

The other part of the report should be a summary of the information that backs up the conclusion. It would be an abstract giving times, dates, sources, and a brief statement of the criminal activity involved. (See appendix E for two

brief examples of such reports, one of which describes new developments in a specific criminal activity, the other of which warns of a new development that may attract organized crime.)

### **Indicative Versus Evidential Intelligence**

A relatively clear distinction can be made between the two general areas of intelligence functioning, namely, the premonitory or indicative phase and the case or evidential phase. In the former, intelligence reports will often be hypotheses pointing to the development of courses of action and trends which are based on some, but not complete, information. They may even be based on research to indicate areas in which organized crime could profitably start activities, even though there is no information to link it with the particular area at the time the report is written. In the latter or the evidential stage, ordinarily another element of the agency or the prosecutor will have the responsibility for case building. However, the intelligence unit may still be furnishing reports on information that it has in its files. In such cases, the analyst may make a contribution by suggesting what the various pieces of evidence gathered so far suggest, and where other evidence may be found.

### **Role of Consumer**

It is important in thinking of the problem of the intelligence report to emphasize that the report content and format should be defined by the primary consumer. It does little good for the intelligence unit to suggest what it should report and how it should report, when its ideas differ from those of the chief planner or prosecutor. On the other hand, the consumer often is not fully aware of what he wants. Thus, the format of reporting should be a matter of discussion between the intelligence commander and the primary consumer of intelligence in the department or agency. Moreover, reporting should be reviewed from time to time to insure that the final product of the intelligence process is as effective as possible.

### **Dissemination**

The primary function of dissemination in the intelligence process is to distribute the finished product or report to command and enforcement

elements where they will be used. Reports which remain locked up inside the intelligence unit, to be read only by intelligence personnel, fail to fulfill their primary role. But dissemination is more than the mere sending out of reports. It involves specific decisions by the unit commander as to whom should receive what product of his unit. In many cases these decisions must be approved by the agency head himself. The recipients are indicated basically by the criterion of "need-to-know." Also involved, however, is the degree of sensitivity of the information, especially as it relates to the source. Moreover, reports in the indicative stage could contain hypotheses which, if misread or misused, would lead to the maldeployment of resources in the department.

Thus, as in the case of the report format and content, dissemination should be established on the basis of discussion between the intelligence unit leader and the agency chief. The dissemination should be determined by the purpose of the report, those who have a need to know, and the commander's decision as to additional readers he wishes to make aware of the flow of intelligence information and analysis. Security is important but rarely should it be the determining factor in deciding who should read the reports and what offices should get them. If the chief wishes the intelligence unit to produce imaginative pieces for him in which there is a free-swinging discussion of problems, he may wish these to be for his eyes only. But this is not a matter of security so much as a matter of protecting persons who are developing ideas from potential trouble.

The most important single rule of dissemination is that intelligence analysis is delivered intact to the head of the agency. Only in this manner can the integrity of the intelligence unit be insured. Only in this manner can the head be assured that the unit will keep him fully informed; only in this manner will the intelligence staff know that others are not editing or slanting their reports. It is also vital that the head be made aware directly of very sensitive material that may have a bearing on a current case of corruption in political leadership or among his own people. It is important that the integrity of the intelligence reporting system be insured.

Finally, there is the problem of external dissemination. There will be requests for various

kinds of information from other law enforcement units. Decisions must be made from within the department on how these are to be handled. (For a discussion of this problem, see chapter III.)

### Reevaluation

The final element of the intelligence process is reevaluation. The commander of the intelligence unit should be aware that it is his function to continuously review the effectiveness of his operation on the basis of his own observation of how effective is the reporting, how good is the analysis in terms of pointing out new areas of operation before the organized criminals actually get there, how good is his collection system. But, in addition to this, he should have established a formal feedback process or system which requires the agency head to tell the commander of the intelligence unit how useful or how pointed his reporting is. No matter how observant the commander is, he cannot without guidance really understand the requirements of the agency head, and therefore he must establish a formal means to elicit this type of information from the head.

Reevaluation raises a management problem that might be called measures of effectiveness. It is certainly not the size of the files or the number of entries that determine the effectiveness of the intelligence unit. The commander should think more in terms of how he might test the ability of his system to produce analyses quickly with a minimum of file-search time. He might analyze his operation in terms of ability through time to have detected new operations of the organized criminal before either operations actually start, or before anybody else actually detects them. This is a hard test, but, after all, the function of intelligence is to warn of new developments, to suggest areas where the organized criminal might turn next. A final test might be the extent to which the unit has detected criminals beginning to operate in legitimate business with apparently legal means—legal, that is, because there is no ordinance or State law or Federal law against the particular operation.

These are all very stiff measures of effectiveness. They are also difficult to quantify. Nevertheless, the intelligence unit commander must try to develop his own tests of effectiveness be-

cause his responsibility is so different from the normal line functions. The effectiveness of the motorized patrol in the traffic bureau can be tested by the way the traffic is flowing. If it is moving smoothly, it is being successful. In the burglary squad, if the number of actual break-ins declines and the number of arrests and convictions goes up, the operation is effective. But in organized crime the number of arrests of policy runners and gambling-game operators is no real test of the effectiveness of the intelligence system. The payoff basically is when the intelligence process can provide information which leads to the breakup of a major portion of a syndicate, including especially the arrest and conviction of one or more of the major leaders. (Obviously, in this examination, account would have to be taken of a failure on the part of the prosecution or on the part of the judge or courts to pursue vigorously the case that has been made.)

Reviews and post mortems will serve little purpose unless they result in action of some kind to correct the deficiencies uncovered or lead to the institution of new methods or experimentation with unfamiliar techniques. Some of the practical consequences of good, hard-hitting reevaluation might be: the dropping of an informant who is fast losing his connections, the addition of new cross-reference items for all future filing entries, the assignment of a liaison officer on a part-time basis to the local Federal strike force, the abandonment of a file on street narcotics pushers (and the dispatch of this file to the vice squad in operations), the laying on of a long-range study of the practices of the local securities market, the acquisition of a short term consultant from a local university to devise an RFP for a contract survey of the economic costs of organized pilferage in the dock area. These examples represent only a few of the infinite number of decisions that can flow from effective reevaluation. They do suggest, however, that reevaluation as an intelligence manager's tool is *not* for nit-picking.

The commander's final responsibility in reevaluation is to establish some system for reviewing his records. These records should be kept current and not accumulate a vast amount of unnecessary material. In particular, there should be some means developed for purging the records of incorrect information. (Purging for privacy purposes is discussed in appendix A.)

## Management of the Intelligence Process

In the process developed above there are three activities which, in addition to being essential to the production of intelligence, are important tools for managing the intelligence process: collection planning, periodic reporting, and reevaluation. These sources provide the intelligence commander with the essential tools to direct the proper allocation of his resources, to review the effectiveness of his decisions, and to report to his higher command in the management chain.

Specifically, the head of the intelligence unit should have his unit produce monthly the following reports:

### Collection Plan

This document should briefly review the focus of efforts over the past month, analyze current requirements, and indicate areas of focus for collection for the next month. The report should be divided into two parts, one having to do with premonitory or indicative intelligence requirements, and the second with evidential or case-building requirements. Efforts should be made to indicate what agency or group should be tasked to collect desired information. For example, in the premonitory or indicative area, the responsibility might be given to researchers and investigators of the intelligence unit. If appropriate reference should be made, to what could be expected from requests for information from other departments. In the evidential area, the recommendation might be made to hand the case over to the prosecutor and his staff or a Federal agency for development of full evidence needed for an eventual prosecution in the courts. Or it might be noted that the intelligence unit's own staff would have to cover all of the collection. The collection plan should also address exploration of type sources, such as informers, undercover agents, electronic devices, business analysts, etc.

The report does not have to be lengthy. It can include a form on which to update, modify, or leave unchanged current allocation of resources. The purpose behind this document is once again to force formal and periodic review. And review without an explicit statement of the problem and situation tends to be meaningless.

The document should be valuable to the head

of the agency because if he agrees to the collection targets of his intelligence unit, it tells him what is required of other units. If he disagrees, it provides him with an explicit mechanism (his review of the collection plan) to reach such a decision.

### Monthly Report of Intelligence Unit's Activities

A monthly report provides the management chain with an explicit statement of what the intelligence unit did for them during the past month. It should be directly related to the collection plan for the month. (A sample format is shown in figure 5, page 32.) It should provide substantive backup for discussions of the collection plan and material for the evaluation of operations discussed next.

### Monthly Evaluation of Operations

The section above on reevaluation as a function of the intelligence process provides the rationale for this activity. It should be made a part of the monthly management review of the activities of the unit. The commander of the intelligence unit should meet with his principal assistants, or better, his whole staff) once a month. At this meeting, collectively they should try to answer a series of specific questions that a member of the staff (or someone from outside the unit) has formulated. Examples of the type of questions that could be posed are:

- Does the unit know more about organized crime activities in its area of jurisdiction than it did a month ago?
- If the answer is yes, then: What has been learned? How was it learned? Could more have been learned by better approaches? What is being done to exploit the gain in knowledge? Can some specific cases be developed? Should there be a shift in the investigative effort? etc.
- If the answer is no, then: Why not? Is analysis failing to keep track of activities of organized crime? Are investigators focused only on low-level operations? What developments have been learned from outside agencies? Have they been followed up? etc.

- Are there reports or rumors of organized crime activities that the unit itself has no other information about? What has been done to check out the rumors?
- What developments on organized crime have been reported by neighboring (or other) jurisdictions? Have investigations in their own jurisdiction been focused in these areas to see if such developments are occurring here?
- What developments elsewhere have been suggested by questions received (about persons or activities) from other jurisdictions? Have they been checked out locally?
- Has there been a flow of information from others in the agency? Have patrolmen, in particular, been responsive to the unit's request for information? Have the reports been followed up?
- Has the filing system been responsive to questions directed at it? Have there been questions that have not been answered because of the filing system? Have analysts noted need for other categories? For more extensive cross-filing?
- Have there been reactions to the units reporting? Have the consumers been queried as to usefulness and the material being on target? Have there been any leaks?
- What questions should be asked next month?

The whole concept outlined above is a formal, directed, self-examination of the successes, failures, and general operation of the unit. Under no conditions should the activity be considered as a bull session. The meeting should result in a report on gains and losses, and suggestions for improvement. This report can be reviewed at the following meeting to see what action has been taken—it becomes a long needle to force improvement.

The nature of the intelligence function, its security and compartmentation, makes evaluation difficult. Self-examination seems to be the most useful approach. This puts a heavy responsibility on the commander of the intelligence unit.

FIGURE 5.—Sample monthly report of intelligence unit's activities

1. General utilization of staff—

Type activity	Number			Man-hours	
	Initiated during month	Completed during month	Continuing	Investigator	Analyst
Investigation:					
Subject/unit initiated .....	_____	_____	_____	_____	_____
Subject/requested by other element in agency:					
Chief .....	_____	_____	_____	_____	_____
Detective element .....	_____	_____	_____	_____	_____
Enforcement element .....	_____	_____	_____	_____	_____
Internal squad .....	_____	_____	_____	_____	_____
Other .....	_____	_____	_____	_____	_____
Subject/requested by other agency:					
Prosecutor (same jurisdiction) .....	_____	_____	_____	_____	_____
State agency .....	_____	_____	_____	_____	_____
Federal agency .....	_____	_____	_____	_____	_____
Other .....	_____	_____	_____	_____	_____
Special study/analysis title and requestor:					
_____					
_____					

2. Subject area of activity—

Areas of continuing study investigation (by function or person)

- a. \_\_\_\_\_
- b. \_\_\_\_\_

New areas of study/investigation (by function or person)

- a. \_\_\_\_\_
- b. \_\_\_\_\_

3. Developments which suggest new activities by organized criminals—

- a. \_\_\_\_\_
- b. \_\_\_\_\_

**FIGURE 6—ANALYSIS**



**1. Assembling available data on problem.**



**2. Identifying unavailable data and defining new collection targets to collectors.**



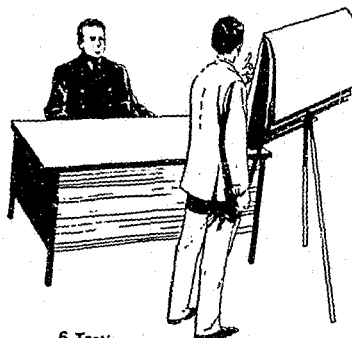
**3. Additional data provided by collector adds to picture.**



**4. Reassembling data and checking with other analysts, investigators or other agencies.**



**5. Forming the hypothesis.**

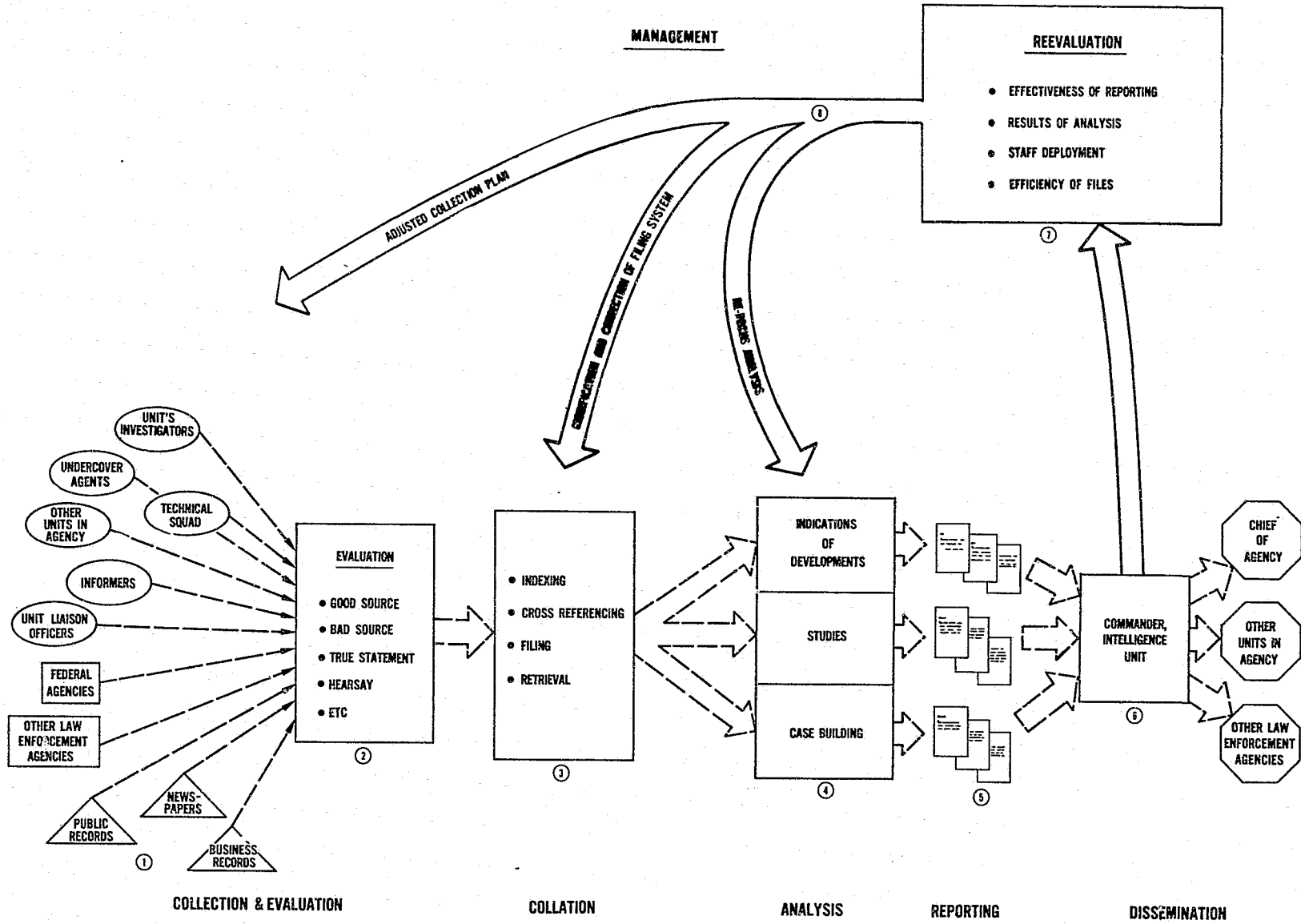


**6. Testing the hypothesis.**



**7. Writing the report.**

FIGURE 7—THE INTELLIGENCE PROCESS



**FIGURE 7—THE INTELLIGENCE PROCESS**

<u>Step</u>	<u>Activity</u>
1.	The ultimate success of the intelligence process depends on a continuing flow of accurate, up-to-date, and relevant information from all possible sources.
2.	Each intelligence unit must have some method for determining the value of incoming information that is to be entered into its files and/or to be acted upon. The evaluation can be initiated by the collection element but should also be performed by a knowledgeable person (knowledgeable in terms of accuracy of the reporter and correctness of the data reported) in the intelligence unit. Recording the evaluation can be simplified by use of number or letter code system.
3.	It is essential that the information to be retained in the unit's files be indexed, cross-referenced, and filed in such a manner that it may be efficiently retrieved as required. The classification of files by name, address, business, function, etc., and the cross-referencing should be done in a manner that supports the analysts.
4.	On the basis of the information flow, the analyst will seek to determine new developments and warn of impending activities, to perform on request studies of trends and networks of activities by organized criminals (or those suspected of such activities), and to assist in putting together evidence for case building.
5.	The intelligence unit is responsible for producing reports, both those specifically requested and those generated by the flow of information.
6.	The intelligence unit commander should in most circumstances approve of reports prepared in his unit before they are sent out.
7.	The connecting link between the intelligence process and the management of the process is the action of reevaluation or assessment of the effectiveness with which the particular intelligence unit is performing its mission—that is, performing the intelligence process in such a manner that it is making an effective input to the agency's effort against organized crime. On the day-to-day basis, the commander of the intelligence unit must perform this function of reevaluation, of assessing the effectiveness of the operation of his unit. Periodically, the agency head will have some outside element inspect the unit.
8.	The outcome of the reevaluation, whether it is performed by the commander alone or in a more formal manner, becomes the basis on which the commander redeploys or refocuses his assets.



# Chapter III

## THE STRUCTURE OF AN INTELLIGENCE UNIT

*Intelligence unit must be organized to provide strategic intelligence to agency head and tactical intelligence to operational units.*

*Intelligence unit should be a staff organization reporting directly to agency head.*

*Essential intelligence reports go directly from unit to agency head to preclude filtering effect.*

*Intelligence unit must not have responsibility for internal squad function.*

*Structure of the intelligence unit must ensure all functions of intelligence process can be performed.*

- *A single person may perform more than one function.*
- *Structure must provide control and direction for flow of information—in, out, and within unit.*
- *Structure must permit coordinated effort of intelligence investigators and analysts; use of team approach where appropriate.*

*Command element of unit responsible for dissemination and evaluation, for management of process.*

- *Responsible for intra-agency and external relations in all facets of process.*
- *Take initiative in developing bases for establishing and improving relations with other agencies but within guidelines of security.*
- *Develop use of liaison officers as means for improving value and productivity of external relations.*

### INTRODUCTION

Shaping and building an intelligence unit targeted against organized crime must be a matter of customized tailoring. No two law enforcement agencies have the same requirements or local needs or the same powerful traditions that may have to be accommodated in precisely the same way. This chapter will not set down rigid prescriptions for size, structural relations, or even organizational form. What it will at-

tempt to do is enunciate some principles which, regardless of other factors or conditions, constitute minimal elements of sound structural practice for intelligence units. These principles can be adapted to the needs of agencies of various sizes and with varying degrees of an organized crime problem.

Because organized crime knows no jurisdictional or geographic boundaries, the structure of an intelligence unit to cope with it cannot be

discussed without considerable attention to external relations. In many cases, the organization of an intelligence unit is of less importance than the capacity of the unit to do business effectively beyond its own suite of offices or array of desks and files. Thus, considerable emphasis will be given to built-in arrangements for dealing with other agencies at all levels. Perhaps the first principle for a sound approach to intelligence unit structure is a negative one: Whatever else it may be, an intelligence unit should *not* be an hermetically sealed, totally self-contained unit, living by and for itself, recycling its own stale air for survival. It must, in other words, have a vital external life; it must be able to reach out not only up and down the organizational ladder, but also beyond it to other ladders.

### STRUCTURE AND MISSION

Traditionally the intelligence unit in law enforcement agencies has been looked upon as a clearinghouse or reference point primarily of use to the field investigator in developing his casework. Slowly this old-fashioned concept is giving way to that of a two-directional unit which supports and services the agency head on the one hand, and the field investigator and prosecutor's office on the other. This dual mission, this two-way stretch, constitutes a recognition of the differences between strategic intelligence and tactical intelligence (see chapter II, page 11, for a discussion of the differences between tactical and strategic intelligence).

#### The Intelligence Unit and the Two-Way Stretch

The most difficult structural problem for the designer of an intelligence unit is to build this two-way stretch: The unit must have an information system that can rapidly and effectively respond to requirements from its own investigators and requests for information from other elements of the agency and from other agencies—this is the rapid response function of the unit. At the same time, it must have the capability to produce intelligence reports that are responsive to the requirements of the agency head.

In the larger units, there should be sufficient personnel to have some assigned to information control and the answering of requests for spot information, and others assigned to the analysis-

reporting function to meet the requirement to have strategic intelligence inputs for the agency head. Small intelligence units probably will have to rely on a handful of flexible and harried officers to meet both needs, often simultaneously.

A major preoccupation of the intelligence unit commander should be to insure that proper balance is maintained between the two requirements. He must not only constantly review the functioning of the outside demands on his files/information system, but must also keep whatever analytic capability he has focussed on what he and the agency head perceive to be the most pressing problems. Whenever he is faced with a cruel choice because his people are seriously overtaxed in keeping up with both requirements, he must always direct his own skills to meeting the requirements of the agency head. For if he does not, he will be in danger of losing the war for the sake of winning an immediate battle. Moreover, if he is not in a position to provide his superiors with an overall picture of organized crime in the jurisdiction, there is probably no one else who can. There will always be persuasive advocates impatient to monopolize the policymaker's attention on such perennial questions as traffic safety, riot control, and new squad cars.

#### The Intelligence Unit and Enforcement

Another major function of the intelligence unit, especially its commander, is to deliver critiques of major pending enforcement tactical moves of the agency on four levels:

1. The potential impact on continuing intelligence collection activities in the area or with respect to the subject at hand. For example, will the operation cause the identity of a valuable informer to become known?

2. The extent to which all available intelligence has been made available to the tactical planners.

3. The interpretation placed on the reliability of information by the tactical planners. It is important that planners not base their plan on information that they are giving higher reliability to than the intelligence unit believes is correct.

4. Where appropriate, an appraisal of the potential value of the planned enforcement action. Thus, if the vice squad, for example, has con-

vinced the agency head to clean out a string of prostitution houses in a certain district, the intelligence unit commander might be called upon to answer such questions as: "Will the prostitution problem merely move from one precinct to another, and if this proves to be the case, is the harassment factor sufficient to justify the operation?"

The intelligence unit commander must also be brought into the planning for major raids since they can be important information collecting sources. The intelligence commander may recommend that some of his personnel go with the raiders to be sure that all possible information is gained—data beyond the evidence collected against the criminals at the scene. The intelligence personnel will be looking for information which will help to explain the relations between the current operation and the larger network of organized criminals. At a minimum, the intelligence unit can provide questions for the raiding party to put to the entrepreneurs involved about their superiors at a time when they are apprehensive and possibly off guard. In short, the intelligence unit, while not a part of the enforcement mechanism, while not itself operational, cannot and should not stand apart and aside from enforcement responsibility.

### Guiding Principals of Organization

The necessity of encompassing intelligence to serve all the needs of an agency imposes peculiar structural burdens on those responsible for organization planning. In practice, there are no wholly correct structural solutions—only principles that must not be ignored if the intelligence product is to reach its varied consumers clearly, pointedly, urgently, and with effective impact. These principles are:

1. Intelligence, particularly intelligence focused on organized crime, is a commodity not necessarily understood by all law enforcement officers simply because they wear a uniform, carry a badge, or have passed a bar exam.

2. The usefulness of intelligence may not always be appreciated by either superiors or subordinates and accordingly it is often neglected by both.

3. Regardless of how the intelligence function is structured into a law enforcement agency, it should be placed within the mainstream of the

agency's life so that it does indeed become a part of the vital activity of the agency. In other words, an intelligence unit—although it may be saddled with sensitive security considerations unknown elsewhere in the agency—cannot by reason of its placement in the agency be permitted to become a quiet retreat detached from the rest of the organization's activity.

4. The unit must disseminate its product to appropriate consumers in order to demonstrate its usefulness and to perform a real, albeit somewhat unique, role in law enforcement.

### LOCATION OF THE INTELLIGENCE UNIT

The proper placement of an intelligence unit in a law enforcement agency depends on a variety of local factors such as the overall size of the agency, the criticality of the organized crime problem in the area served, the mission of the agency (e.g., investigation, prosecution, labor relations, etc.) and, candidly, the integrity quotient of the agency's personnel. There are situations where for a variety of sensitive reasons—and the foremost of these is internal corruption—an agency head may find it necessary to combine intelligence functions with other functions, usually internal investigations. This should be regarded as more or less unique and generally is an undesirable confusion of functional objectives. The focus of the discussion that follows will be on the discrete unit with the single mission of conducting intelligence for the law enforcement agency against the organized crime target.

### Intelligence as a Staff Function

Ideally, the organized crime intelligence unit is a staff organization whose commander reports directly to the agency head. It should be a staff organization so that operational obligations are minimized. It should report directly to the chief because the substance of organized crime intelligence is often extremely delicate and because the unit should be providing the highest authority with material which enables him to make effective policy decisions. Let us examine both these propositions.

The intelligence unit must be in a staff role because:

1. *Such a positioning is an implicit recogni-*

tion that the personnel assigned to the unit are to be primarily concerned with intelligence. That is to say they will be "men in the middle," constructing a coherent picture of organized crime as it operates in their jurisdiction (and beyond if necessary). They will not participate directly in the eradication of organized crime in the sense of making raids and arrests. While they may conduct investigations on the street, such fieldwork will be done as a necessary means of collection pieces of information on developing activities of organized criminals, or to follow up leads already developed by analysis. They may frequently advise (and even accompany) operational units in the conduct of enforcement activities, but in such cases their participation merely constitutes a service in support of traditional police operations.

The more the intelligence officer is drawn into operational activity the more he will be deflected from his primary mission. There are, after all, concrete satisfactions in making arrests, in personally interfering with the professional career of an organized crime network. The temptation to be in on the climax will be strong, but to so confuse roles and missions almost always means that the less glamorous routine of the intelligence officer will be the loser.

2. *The intelligence unit should be insulated as much as possible from day-to-day police functions (including long court appearances) so that it can stick to its intelligence mission—and perform that mission as objectively as possible.* Once an intelligence unit is permitted (or persuaded) to involve itself in operational activities for which it provides the intelligence base, the success of the operation inevitably becomes paramount. The cool, dispassionate, even impersonal view of the professional intelligence officer may become clouded. He may begin to examine new information from the perspective of someone committed to a certain operational path; he may unconsciously seek material which will justify the undertaking rather than question its premises. In other words, once he is a party to the operation, he may be less able to spot the flaw in its planning assumptions; equally he may find that he is less than eager to credit new evidence which suggests that the targeting is poor or the real quarry has already skipped town, or whatever.

## The Intelligence Unit and the Head of the Law Enforcement Agency

An intelligence unit must be prepared to serve the policymaking echelon of the law enforcement agency by contributing to its capacity to make effective decisions (see chapter I on this point). After all, that is one of the fundamental assumptions of its existence. It should, therefore, be so placed (or the unit's commander so placed) that a reciprocal understanding of the needs of the agency head and the capability the unit to deliver is developed. As the commander of the intelligence unit learns more about the daily preoccupations of the agency head, he will tailor his reports and briefings to fit more closely with these preoccupations; similarly, the agency head will find himself involved in a learning process—learning, that is, what his intelligence unit can do for him.

The best agency head is the one who learns to stretch the capabilities of the unit, test its flexibility, question its hypotheses, and insist on increasingly high standards of performance. If the agency head is truly skillful in his role, he will discover that he has drawn more out of his intelligence unit than even the commander of the unit originally thought was possible. This ideal effect can only be achieved, however, if the agency head insists on maintaining one other level of excellence—that is, the excellence of the personnel committed to the intelligence unit. Any failure on his part to insist on the highest standards—or any indulgence on his part of personnel raids by other units of the agency against the intelligence unit—will to a degree undermine the quality of the staff he has developed to serve his needs. (For a discussion of personnel selection, see chapter IV.)

For many agencies the kind of relationship discussed above is difficult to achieve because political winds are constantly blowing old agency heads out of office and new heads in. The commander of the intelligence unit may have relatively little time to develop effective working relationships with the agency head, much less to hone the intelligence products produced for the agency head on the wheel of this relationship. In such circumstances the intelligence unit commander must rely on his wits to establish a pattern of service to the agency head and, at the same time, preserve his unit's momentum de-

spite changes at the top. The only rule he can follow is to regard all demands, all requirements, all hints he may get from the agency head, as immediate and urgent levies on his unit. He must devise a formula of briefings or reports geared to the daily life and preoccupations of his elusive superior.

### The Filtering Effect

Proximity of the intelligence commander to the agency head is also essential as a barrier against the filtering effect—the distortion or dilution of finished intelligence that is bound to occur if it passes through several hands on its way to the ultimate consumer, the agency head. In extreme cases, this can be damaging both to content and objectivity.

Let us assume that an intelligence unit situated well down the organizational ladder prepares a premonitory type report flagging the possibility that organized crime is about to enter the laundry services of the city. This report contains some names of known criminal figures, but it is primarily a warning paper pointing out potential new area of organized crime penetration. The intelligence unit chief passes it to his superior with the admonition that it not yet be used as a basis for action, the evidence is still less than conclusive, the penetration not yet at a dangerous point, etc. The commander's immediate superior promises to "get it to the chief," but decides that the only way to capture *his* immediate superior's attention is to describe the laundering activities of organized crime in the city as "substantial, growing, and threatening." He attaches a buckslip to this effect and urges the paper on its course.

The next officer in line (who reports directly to the agency head) sees something else in the paper: mention of a suspect whom he has long yearned to put away for reasons of professional pride. (He had once had a well documented case against the suspect thrown out by a young and contemptuous prosecutor.) A week later he uses the original report and the comments affixed to it by his immediate subordinate as a vehicle to make a special plea to the agency head for starting a new investigation against his old nemesis mentioned in the report. The purpose of the original document has been—albeit unintentionally—thwarted, the cave-

ats about cautionary use of the material lost, and if the agency head actually does approve a special investigation of the suspect in question, the fact of the agency's interest in criminal activity in the laundry business may be prematurely disclosed. Filtering has done good intelligence work a bad service.

### The Intelligence Unit and Internal Problems of the Agency

The filtering effect is particularly pernicious where an agency has had serious integrity problems. If organized crime in the jurisdiction has made inroads on the force itself or on political leaders associated with law enforcement, the first evidence of this may be unearthed by the investigative diggers of the intelligence unit. Such sensitive matters obviously must be closely held, not only to prevent compromise or coverup by the individuals involved but also to protect the "clean" members of the agency or the area's political leadership from unwarranted suspicion. Direct access to the agency head is the most expeditious means to handle such information. It might be argued that cross-agency communication with the director of the internal squad is all that is needed. This may be true for minor instances of petty corrupt practices, but where a member of the agency or the political establishment is alleged to have been reached by a representative of organized crime—no matter how lowly that representative may be—the agency head must be advised urgently and directly. Such information, after all, is the most pointed material an agency head can receive. If anything can give him a picture of the environment in which he must carry out his job, it is knowledge of how successful organized crime has been in cultivating his associates or subordinates.

In sensitive cases direct access to the agency head is also critical to achieve some measure of organizational distance between the intelligence unit and the agency internal squad. Since the internal squad normally functions as an integral part of the office of the agency head, only he can keep the missions of the two units clearly separated. To put it another way, the intervention of the agency head may be necessary to keep the intelligence unit from becoming involved in internal affairs matters. If the unit is allowed

to be drawn into such matters, it will soon find itself shut off from cooperation with the principal line elements of the agency. Once it has become known as "the head-hunting unit," the intelligence unit will find itself frustrated in attempting to draw raw intelligence from the street patrolman or detective squad. In addition, any hopes for developing other forms of intra-agency collaboration will be lost.

If, because of agency size or some other intractable obstacle, an intelligence unit is placed in a position where it is not directly responsible to the agency head, special access arrangements should be sought. These might entail "skip-echelon" agreements between the intelligence unit commander, his immediate superiors, and the agency head to permit the commander daily, or at least frequent, visitation rights with the agency head on certain prescribed subjects. In most cases, the officers occupying positions in the intervening echelons will insist on participating in these discussions.

The principle that the intelligence unit should have direct access to the agency head should be observed in any case, no matter how numerous the participants. This means quite simply that the intelligence unit commander should have on a routine basis the privilege—indeed, the obligation—of raising matters which he believes are significant with the agency head. The number of more senior officers clustered about the agency head during such talks is less important than the fact that he uses the privilege—or exercises his obligation—with force, directness, and cogent analysis. Should even this procedure not be possible, it may be necessary for the intelligence unit commander to resort to more informal procedures to insure some measure of direct communication. He might, for example, request a place at the periodic meetings of the agency head's senior staff circle, or the installation of a special, open phone line between his desk and the agency head's desk. If all else fails, he might attach to his unit an officer of recognized integrity who is known to enjoy a special relationship with the agency head. But whatever substitute arrangements he may be forced to adopt, the intelligence unit or organized crime bureau commander cannot remain satisfied until his function is recognized as so essential to the agency head that direct access is offered him. And whether this door is opened

to him more often than not will depend on the quality of the finished product served up by his intelligence unit.

## THE SHAPE OF AN INTELLIGENCE UNIT

As noted earlier in chapter II, it is not essential that all the classical functions of an intelligence unit be performed by separate people or separate groups of people. What is essential, however, is that each identifiable step in the process (collection, collation, analysis, dissemination, etc.) be thought of as distinct and that the workflow of the office be so structured as to insure a dynamic movement from one step to another—a smooth continuing flow. With this in mind, it is possible to define basic physical and human requirements necessary to sustain momentum in the process. An examination of this process and its requirements will, in turn, provide an organizational base onto which can be grafted numbers of people occupied in the activities defined. The exact numbers assigned will differ enormously according to agency size, skills available, and any number of other variables. In this section only the pieces of the process will be discussed—not the numbers of people committed to the individual pieces of the process. Management officers will be more than anxious to pick up where this manual leaves off; that is, at the point where the pieces of the process are converted to boxes on an organization chart and numbers are inscribed inside the boxes.

### The Control of Information and Document Flow<sup>1</sup>

To begin with, raw information must be received by the intelligence unit. It is being manufactured around the clock, on the streets, in offices, bars, other law enforcement agencies, newspaper editorial rooms, on electronic surveillance gear, etc. So, clearly, there must be a reception point, and, if some of the information is of a sensitive nature, perhaps there will be two or more reception points, one for general information, the other(s) for more sensitive inputs. The practice will vary according to the division

<sup>1</sup> See figure 11 at the end of the chapter which portrays control and flow of information and documents in an intelligence unit.

of labor in a unit. In some instances, receiving may be the function of a clerical employee, in others a relatively junior police officer, or in a prosecutor's office, a legal secretary. Sensitive material, properly labeled as such, should only be entrusted to a supervising officer of the unit. Once a reception point or points are established, several questions remain to be answered which relate directly to structure: How often is reception to take place, how is incoming material to be recorded, if at all, and how is the flow to be controlled?

The first of these questions is significant only for larger departments or agencies. As a practical matter, most intelligence units will close their file drawers and their doors at fixed terminal points in the day's work and, barring emergencies or states of crisis, will simply permit information to pile up overnight. The evening's take will be received the next morning. Larger departments may feel the need of operating—at least, on a skeletal basis—around the clock. Thus, they can receive all night long, either in their regular offices, or through the service of their own officers assigned rotationally to the agency's command and control center. Whatever the arrangements, the purpose is the same: to insure that incoming information, which may contain critical intelligence, is received by the unit which has responsibility for the agency's intelligence function.

It goes without saying that the simple capacity to receive such information is of no importance unless arrangements are also available to transmit it to an officer or officers who appreciate its contents and can successfully exploit it during off-duty hours. Most large intelligence units maintain an on-call duty officer to perform this function. He can be invaluable in certain situations, particularly if the agency has an established practice of referring plans for large-scale enforcement actions to the intelligence unit for critique. Items of information arriving at off-duty hours require careful recording; they are likely to be overlooked if they have not been received during the normal working day. A careful log of all incoming phone calls, messages, important teletype items, and the like will provide the regular personnel with some view of what went on overnight when they report for duty in the morning. Equally important, the overnight items will not be lost in the shuffle,

but will be available for normal processing. The regular receiver can track them down from the log entries and submit them to standard handling procedures.

### Logging

Generally speaking, incoming material should be logged as a matter of course. (See figure 8, page 43, for a sample logsheet.) Naturally this does not apply to such items as letters addressed to individual members of the unit, or newspapers for clipping, or periodicals for whom there are routinely designated recipients. However, police reports, surveillance readouts, and the like should be logged—if only by title, date, subject matter, and originator—as the first step in a watertight information control system. Logging can become a considerable burden and from time to time it may be necessary to review the logging requirement. If, for example, one of the officers in the unit is routinely sent all police and detective reports, then it may be considered redundant for the original receiver to log these items as they come in. Their location is a known factor. But if a police report should for any reason come in ticketed for a different officer in the unit, or be received during an emergency, say, by the on-call duty officer, then this unusual flow should be recorded in the receiver's log.

Any office should have some system of information control. The placement of this function will vary according to the size and complexity of the intelligence unit, but in a great number of cases the best location for it is at the receiving point, whatever or whoever that may be. This will not always be an easy task, given the tendency of law enforcement officers, like most people, to stuff papers in their pockets and wander off unaware of what they have done—or aware of what they have done and determined to put the papers back in their rightful place almost, but not quite immediately. Other details of a control system need not be explored in this volume, except to emphasize that there are sensitive points in the movement of paper around a law enforcement agency which require special attention. One of these, obviously, is the departure of a record, or extract of a file in response to a request from an element of the agency outside the intelligence unit or by another agency altogether. No matter that these





are legitimate requests; they should be recorded fully and a copy of whatever is passed on maintained in the files. Similar restrictive procedures should be imposed on materials dealing with electronic surveillance and eavesdrop tapes, etc. In short, any documentation susceptible to illegal or malicious exploitation requires special handling of the most scrupulous kind. (See figure 11, page 56, which shows graphically the importance of information control.)

A careful log should be kept of all copies made for external passage—this, of course, primarily as a record of who outside the agency has access to what materials. (See figure 9, page 45, for a sample logsheet for outgoing documents.) To each item so passed a dated buckslip should be attached indicating the intended recipient by name, title, and agency. The buckslip should be signed by the authorizing officer of the originating agency. One copy of the buckslip should be placed in the appropriate subject files from whence the material was drawn and another copy kept separately with all other notations of materials so passed out of the agency. Finally, a receipt should be attached to all materials sent out of the agency to be signed and returned by the designated recipient. When the receipt returns to the originating agency, it should be filed with the separate collection of buckslips authorizing the passage of the material receipted. This step closes the circle. If, of course, no receipt is received in a reasonable amount of time, a followup phone call may be necessary. These procedures may seem cumbersome, but if they enable an intelligence unit commander to give as full an accounting as possible of who has access to his materials, and if the receipt procedure impresses on the receiving agency the seriousness with which the material is regarded by its originating agency, then the mechanics of the process will have been justified.

### Circulation, Filing, and Storage

Once received, information must be passed on and routed internally to those who need it. Subsequently decisions must be made as to whether it is to be filed or stored, and if so, how. The circulation and storage function is not wholly a clerical one. Recognition of significant nuggets of intelligence in incoming material is an essential part of the *collation* process, and it should be done by a trained analyst or analysts with

clerical assistance. Obviously, the choices of what to do with any single item of information are numerous, but by and large, the objective in this stage of the intelligence operation is to get the item to the person or persons within the office system—and sometimes beyond it—where it may add value to the overall effort. The analyst who reads incoming traffic has to bear in mind that several uses may be made of a single item and so indicate on the item as he prepares it to continue its journey to a particular desk, to several desks, to a particular file or files, or to the computer storage system. (See chapter II for a discussion of various classes of intelligence.) In many cases this is the beginning of the collation process.

By making the judgment that "Officer Jones would like to see this item because he is assembling a file on the subject," an analyst is ticketing an item as suitable for combining with other similar or related materials. It will, of course, be up to Officer Jones when he receives the item to determine finally whether it is related in some way to the other materials he has collected. Officer Jones may feel that it indeed is pertinent to the study he is preparing and examine it against the base of what he already has on hand. By adding it to his collection—and by discerning where it fits, however indirectly with his other material—Officer Jones will have almost completed the collation process. A final step may remain, however. Jones may decide that not only does the item belong in the files indicated by the original analyst, but that it also bears on others and should be cross-referenced to them.

The foregoing description stops short of the analysis function, but it has included, if only implicitly, one aspect of another major strand of intelligence activity. Two separate decisions have been made as the item passed from the original reading analyst to Officer Jones. Both thought the item was worthy of attention—even as the collector had already done. At a minimum both decided the item was not wholly worthless. Evaluation begun by collector, continued at the point the analyst passed the item to Jones, took place once again when Jones decided it fit in some fashion with his collection, and was sustained by the secondary decisions of both to store copies of the item in various files for possible future recall.

As indicated in chapter II, evaluation is yet



another finite step in the intelligence process. Final evaluation occurs when Jones studies more carefully the relationship of the item to other materials. He could decide finally that, although interesting, the report in question contained some rather dubious material and should not be considered valid until corroborated, at least in part, by other information. One of his reasons for banking the information (after suitable coding), even though it does seem questionable, is that he must allow time for either corroborative or disproving information to appear.

### **Division of Labor—Information Control Versus Analysis**

The structural apparatus necessary to complete the initial, preanalysis steps in the intelligence process can be as simple or complex as the size of the unit dictates. Clearly, one intelligent person can perform almost all the acts described so far: It is quite possible for a single police officer or civilian employee to be the receiving point of the office, to be the information control authority, to route the materials as they arrive, to make initial decisions as to filing, and to be charged with preparing and maintaining certain substantive accounts (studies or cases). In other words, Officer Jones (or Able or Sam) could by himself perform—with one possible exception—any of the acts described so far, and more besides. Ideally, however, a sharper division of labor should obtain. The person who carries out information control responsibilities with the zeal necessary to insure an orderly and systematized flow of materials may have neither the time nor the inclination to be a judicious analyst of substantive matters. Something will have to slip; one function or the other will suffer.

A quite trim organization can be built on the basis of separating what are purely information control activities and what are analytic activities. Thus, at the beginning of the organizational chain there would be a small information control section, which would concern itself with receiving materials, making prescribed routings, and marking up the materials for the more obvious filing destinations. All reproduction of materials, as, for example, when one item would be relevant to two or more staff members, would be undertaken in this section. The document

and request logs would be maintained here, and the filing performed as documents flowed back from the analysts for storage. Cross-referencing as indicated by the analysts would also be performed here. In some intelligence units with a large volume of business, this kind of activity can become burdensome, and the commander of the intelligence unit may well have to spend considerable time assisting the information control personnel in perfecting the office's flow of paper and insuring that the system is respected and followed by all members of the unit. Such a section, if working properly, can contribute much more than simply keeping an office from drowning in its own paper. It can assure that the collation process functions as it should—that cross-references are plentiful, subject files informatively indexed, and the maximum opportunity for "making matches" (e.g., relating addresses to people; associates of criminals to places of illegal business; telephone numbers to license plates, etc.) is afforded all analytic personnel.

An information control section can also provide the crucial service of protecting sensitive materials from unauthorized circulation outside the intelligence unit or outside the agency. This service has two parts, equally important. One is the relatively mechanical operation of controlling documentary flow—the physical movement of material outside of the unit only to the appropriate recipient and the recording of receipts from the outside recipient in the case of highly sensitive documents (see figure 9, page 45).

The second part requires more painstaking methods. It is the whole range of activities connected with recording evaluative judgments on reports, carrying through on purging the files of what proves to be fallacious matter, and the pursuit and correction of documents that have been passed out of the unit into other elements of the agency or other agencies. The importance of these procedures cannot be emphasized too strongly. They not only insure that unit of solid professional standards, but, even more importantly, protect the rights of citizens whose activities are the raw material of intelligence files and records (see appendix A). An intelligence unit commander must be able to satisfy himself on both counts if he is to operate responsibly in a free society.

## Structure and Analysis

The next step in the intelligence process to be charted is analysis. Once again this function can be performed by one person or by many. It consists of so many acts, mental and physical, that no full catalog is possible. For our purposes, it is sufficient to generalize the activity as one in which the collected materials are examined, studied, and pored over for leads, trends, clues or the beginnings of a possible pattern. It also includes the final phase of evaluation; it may often result in further investigation—either on the street, or in the files, or by communication with other elements of the agency or other agencies. All this activity may produce a written report, an oral report, or a decision suggesting some action by enforcement or prosecuting attorney. It may also result simply in the determination by the analyst or his supervisor that the materials he has on hand have not yet jelled sufficiently to permit him to reach any conclusions, and that he must put them away for awhile until more material is forthcoming.

### Analysts and Investigators

There must, at any rate, be an analytic section, preferably one removed slightly from the information control element. In larger agencies a junior member could, in collaboration with information control, perform each morning the initial routing and file designation of the unit's new materials. Where possible, there should be representatives on the analytic staff from a variety of disciplines: economists, sociologists, accountants, attorneys, etc. There should also be experienced investigators of the traditional variety, who in their own rights are specialists in a highly demanding discipline. The melding of these various talents into one team pulling in the same direction may not be the difficult task it would appear at first glance.

Seldom would all the investigators and all the analysts be at work on one large problem. In all probability, they would be working in small groups of two or three—or even one—toward a deeper understanding of some particular aspect of the larger organized crime problem. One can envisage situations where the accountant might be engaged, with occasional assistance from the attorney, on a long-range layout study of organized crime manipulations in the securities field;

three shifts of two investigators each would be running around-the-clock surveillance on a gambling operation which was being mapped by a general analyst, while another investigator and the sociologist were trying to get an understanding of narcotics movements in the dock-workers union.

Furthermore, in certain circumstances, personnel who normally perform their duties as analysts may be employed as investigators, and vice versa. Thus, a member of the intelligence unit who is a trained accountant and has developed a keen understanding of the bookkeeping procedures of a suspect business, may find that he can only add to his knowledge, or "cap an active case" by visiting the premises or interviewing directly officers of the firm. In such a circumstance the accountant/analyst would probably form a two-man team with an officer more experienced in field investigations, but less schooled in accounting. By the same token, personnel normally involved in investigative work will probably contribute increasingly to the analysis process as they become more and more familiar with how their knowledge can be used in conjunction with other information to construct finished intelligence analyses.

### The Team Approach

The close professional relationship between analyst and investigator has already been discussed in chapter II. The team approach can be structured into an intelligence unit as the working core of the operation. In such a system a team or teams of investigators and analysts would be targeted on particular organized crime problems. Practically, of course, one analyst may work with several investigators on different projects. But the objective would be in all cases to maintain continuity on studies to build a foundation of mutual respect and cooperation between analysts and investigators.

Physically there would appear to be some advantage in housing the analytic and investigative element not in a bullpen as in the past, but in a series of different sized small cubicles accommodating two to six persons. This arrangement would provide some degree of privacy and coherence for specific studies or investigations; it would also provide for intercommunication between the teams when needed without the circus-like chaos of the bullpen. The cubicle

layout would make it possible for investigators to come in from their fieldwork and discuss their findings with normally headquarters-bound analysts without disrupting the work of all the individuals in the analytic force. (See figures 17 and 18 at end of chapter VI.)

In such an atmosphere the relationship between analyst and investigator could ripen into a truly effective one. The investigator could become absorbed in the methodology of the analyst, and the analyst, enjoying the opportunity to more thoroughly debrief the investigator, could suggest questions to be put to witnesses or discuss different approaches to fieldwork. Thus, truly effective multiskilled teams might evolve that would hold together, even as subject matter or targets changed.

The suggestion of the team approach does not mean necessarily that analysts and investigators will be assigned to a team for an indefinite period. The team would be organized for the duration of a project. At the end of the investigation, they would normally break up and be reassigned to other team formations if there were investigations requiring this approach. As indicated above, investigators and, especially, analysts might be assigned to more than one team at one time. This would be particularly likely where the investigations appeared to be long and drawn out and not under time pressure. Finally, adoption of the team approach does not rule out an individual handling a particular case or investigation where the scope is relatively limited.

The foregoing description of the working relationships of field investigators and professional analysts is not meant to suggest that the analyst is handcuffed forever to his headquarters desk. Mention has already been made of circumstances when a team, consisting of a specialist and a seasoned investigator would visit the premises of a business being exploited by organized crime. There are any number of occasions when the specialist or analyst could and should sally forth on his own to conduct inquiries or collect documentary evidence that he can best recognize and evaluate on the spot. For that matter, it does not require an officer wearing a holster and gun to serve a subpoena for records on banks, insurance companies, and the like. In certain jurisdictions there may be complications about the definition of a police officers, but where this is

not a problem, intelligence unit commanders should encourage the most flexible use of their personnel—both within and without the headquarters building.

### Supervising the Team

The direction, supervision, and guidance of the analytic and investigative force are delicate matters. On the one hand, investigators, generally operating alone in the field or in pairs, may require closer control than analysts. On the other hand, analysts, generally working in-house with files, statistics, and scraps of worksheets, may become absorbed with the problem they are working on for its own sake. The field investigator may need a system of prods (and a routine reporting-in schedule) to keep him *on* the job; the analyst may need more than a prod to get him *off* a job where the well is running dry, the returns are slight, and the man-hours costly.

While it is incontestable that good analysis takes time, the intelligence unit commander must be prepared to set limits on an analytic study within the context of his own unit's or the agency's priorities. This will require periodic reappraisal of his unit's intelligence activities and possibly the imposition of a formal report requirement from each team on its accomplishments, expectations, and disappointments. Such reports should be made orally (and preferably in the team's cubicle) so that the unit commander can challenge what he hears, suggest new departures or leads to the team, or even rotate the personnel if he feels the need.

Periodic appraisal of the teams is an aspect of reevaluation described in chapter II. The procedures sketched out above are not for the purpose of "the tightest ship in the Navy," and are not intended in any sense as disciplinary measures. They are, rather, means by which the commander can guard against the development of natural but unfortunate working habits by his teams and preserve the validity of his own or his agency's planning priorities.

In the more modest sized units, it will be the unit commander himself who provides direct leadership for the analytic and investigative detachment. Larger intelligence units will obviously require more complex supervisory arrangements—for example, senior officers in charge of broad groupings of functional specialists:

accountants and economists, investigators, narcotics specialists, gambling specialists, what-have-you (see figure 1, page 5).

More appropriately, but perhaps feasible only over time as the investigator-specialist teams develop reciprocal working relationships, would be the command concept of several team chiefs reporting to a superior officer in overall charge of the analytic-investigative function. This arrangement would have several advantages. In the first place, it would tend to soften the hard protective shells that often encase law enforcement officers who have specialized in a particular field for many years. Instead of the narcotics officers continuing to be grouped and supervised as such within the intelligence unit (or detached as a subelement of the unit), they would be assigned to teams that were preoccupied with a variety of targets. Optimally, a broadening of perspective might develop; the old adage, "once a narc always a narc," would lose some of its bite.

The second advantage to team-oriented supervisory arrangements would be the obvious one of giving the team approach more punch. Team members would probably come to regard their performance (or their teamwork) as a critical factor in the ratings they received from supervisors. No longer would they be evaluated simply as experienced narcotics investigators, but rather as productive and cooperative members of Team A or B, etc. Finally, the increasing sophistication of organized crime demands that intelligence tactics become multifaceted. It is quite likely that in the large intelligence units, the analytic and investigative teams will be assigned whole criminal networks to study. They can serve best if a variety of skills under single control is targeted against a particular network.

### Clerical Support

So far then, the structural picture emerging is one of three identifiable functional groups: one devoted to information control and the others to analysis and investigation. Clearly these three elements must be physically proximate and probably in many agencies will, by force of space and other considerations, have to be intermingled. The clerical assistants to the information control person(s) will almost surely have to double as clerical support for the analytic and investigative personnel. But in this process, clerical sup-

port must not be spread so thin that it becomes ineffective in supporting all functions.

Nothing is more wasteful than skimping on clerical support. It is wasteful first and foremost because of its mortal impact on large amounts of useful intelligence. The investigator will often shorten his report—or not file one at all—if he has to prepare it entirely on his own. The analyst will hesitate to make a document for cross-referencing if he knows he will have to battle the copying machine himself to get the job done. Inestimable amounts of raw intelligence have been lost for all time because investigators with an aversion for the pen did not have ready access to a dictaphone and/or a typist. The other side of the intelligence waste coin is the use of highly skilled and experienced personnel on tasks for which they are unsuited. Where investigators and analysts are obliged to perform their own clerical support functions—typing of reports, reproduction and filing of documents, etc.—they cannot be applying themselves to what they do best and what they presumably are paid relatively high salaries to do, namely, investigate and analyze. Moreover, because in most cases they are likely to be better investigators and analysts than they are typists and file clerks, they will probably spend more time than necessary in typing a report and commit more filing bobbles than would a competent clerk-typist—and they will be paid a great deal more than necessary for shabby clerical performances. This is cost effectiveness in its dreariest reverse form.

### Intelligence Unit Command

In addition to the information control and analytic-investigative elements, one other broad functional area should be institutionalized in an intelligence unit. This functional area combines in a general way the intelligence processes not yet wholly touched on in this chapter and provides monitoring for all parts of the process. In military parlance, it would be called the command element. As the name implies, it provides the structure with command or direction: it also furnishes strategic (or policy) support to the agency chief or to the public prosecutor. In addition, it concerns itself with such basic intelligence processes as evaluation, reevaluation, reporting, and dissemination. The discussion

here will deal first with how all these processes can be structured into an organized crime intelligence unit and, secondly, on the vertical, or unit to agency head relationship.

The final judgment in the unit on the analyses and studies produced is made by the unit command level. Is the study produced by the analyst persuasive? Is the dossier assembled a credible depiction of criminal activities? Is the case put together one which would normally be acceptable to prosecutor for action? These are all questions which an intelligence unit commander is likely to ask himself as he evaluates what he has received from his subordinates. Obviously, there are occasions when his judgment may be "no" to any of these questions even though he personally believes that what has been presented to him is valid. There are many reasons why it may be impossible to move the matter forward.

### **Dissemination, a Command Function**

In any event, if his answer is "yes" to any of these questions, the unit commander has also made an important judgment—one which under usual circumstances means he must now take another step in the intelligence process: dissemination. Dissemination as used here refers to the exposure of a finished intelligence product to those whom it is designed to serve or support in some way.

It is essential that this step in the process be the prerogative of the intelligence unit commander. He is responsible for the product of his unit, for the combined judgments of the group of persons who worked on the report, study, or case. Moreover he, more than anyone else in the unit, should be in a position to know where it can be most useful—and at what point to serve it up, or send it to his opposite number in another agency. If he allows finished intelligence material to flow uncontrolled from his unit at the decision of subordinates, the quality standards he has set for himself and his unit will rapidly collapse. He may soon suffer the consequences; e.g., a study based on less than factual data may get into the hands of another law enforcement agency, which, believing it to be sound, takes action against an element of the criminal conspiracy in its own jurisdiction mentioned in the study. The action fails for one reason or another, but the faulty basis for acting

is not forgotten—either by the other law enforcement agency or the innocent victim of the action, if indeed he is innocent.

Another reason for concentrating dissemination authority in the hands of the intelligence unit commander is that, assuming he is properly placed in the structure of the law enforcement agency, i.e., close to the agency head, he alone will probably be in a position to know who should *not* receive it. He should have a knowledge of "soft spots," if any, in the agency outside his own unit; moreover, he and the agency head are more likely to be knowledgeable about the softness of other, neighboring agencies to whom the material might otherwise be of interest.

### **The Intelligence Unit Commander**

Structurally, the office of the unit commander may be quite simple. If his unit is small, he can operate alone with an investigator or analyst designated as deputy in his absence. It can be more ambitious for a larger unit, but size should depend on the responsibilities imposed on the unit by his superior. He can exercise dissemination control by utilizing the services of whoever acts as information control officer. In this case, it would be the information control officer's duty to devise internal procedures whereby reports, studies, dossiers, cases—all those things that constitute finished intelligence—do not leave the unit without the commander's official sanction or written instruction prepared, say, before the document's final typing.

The unit commander's responsibility to serve directly the policymaking apparatus of the agency may require more elaborate arrangements. He may, for example, carry the obligation of reporting daily or weekly on organized crime intelligence developments to the agency head. He may be in a position to prepare the report himself—or, if he is heavily burdened by the unit's multiple activities, he may have to delegate to an assistant or particularly resourceful analyst or to the strategic intelligence section, if there is one.

Whatever the particular circumstances, this is a function which should merit the closest personal attention. It can, of course, if properly conceived, designed, and supported, embrace all the analytic and investigative efforts of his unit; it can set the pace for the quality of the other materials produced in the unit. Needless to say,

if the report is found useful by the agency head, it may also have a profound impact on the immediate law enforcement community. So, it is not unreasonable for the unit commander to focus considerable energy on this responsibility, and to have the effort and any personnel it may require, attached to his immediate, personal office. Even if the report is prepared by an assistant or subordinate, the unit commander must insist on bringing himself into the preparation process directly, frequently, and with energy. It is in part the culmination of his unit's mission; he must be central to the effort. The report must feel his personal impact.

### **Strategic Intelligence Component**

Larger intelligence units, say those serving major metropolitan agencies, should put a high priority on the assignment of a few well qualified personnel to a strategic intelligence component or section serving directly the unit commander. This component might consist of a small nucleus of more or less interchangeable officers with a broad knowledge of all intelligence functions and a keen sensitivity to the intelligence needs of the law enforcement community. This group should have the authority to levy requirements for collection or data compilation on the rest of the intelligence unit—and in so doing set priorities for targeting and the beginning of analytic projects. It would be in this group that daily or weekly summaries for the agency head should be prepared, liaison with other agencies on intelligence matters conducted, and the tactical plans of enforcement units critiqued. In no sense should this group be considered the clerical or file-keeping squad of the intelligence unit. In all likelihood the main concern of collators or file clerks or retrieval specialists would be with tactical support for field investigators.

There will, of course, be difficulties in any such division of duties in an intelligence unit. For one thing, intelligence is power, and power will be quickly recognized and appreciated by those who have less of it than others. The unit's commander will have to use all the leadership skills at his disposal to keep the strategic group open and accessible to those not in it. He will have to devise means to move personnel from one group to the other for specific assignments. His objective, in other words, must be to keep the strategic component from becoming a closed,

elite corps, resented by the rest of the unit and even the agency.

### **Intra-Agency Relations and the Unit Commander**

More than anyone else the unit commander will be responsible for the quality of the relationships maintained with other elements of the agency. Since he must rely greatly on the personnel of other units to feed his own with raw information, the way his organization is regarded by the patrol division, the detective bureau, etc., will be critical. Because all law enforcement agencies are more or less unique organizations, there is little point in detailing here how this intricate set of relationships should be structured or how they might be exploited by the intelligence unit commander. There are, however, certain steps that the commander can take to harmonize the relations between his unit and others in the agency.

In particular, a system of tying the intelligence unit more closely to local precincts may help in some jurisdictions. This could take the form of periodic visits by officers of the intelligence unit to precinct shift formations, or it could be the more permanent position of an officer with liaison responsibilities in the precinct. Few intelligence units would have sufficient personnel to afford the luxury of detailing an officer to each precinct, so one or two men might be shifted from precinct to precinct for visits of several weeks duration. By means of such a system better targeting procedures by the patrol officers could develop, and the liaison officers could serve as conduits for getting helpful information from them to the intelligence unit, and vice versa. (See chapter II for a further discussion of methods to develop a flow of information from other elements of the agency.)

### **External Relations**

Any survey of the structure of an intelligence unit targeted against organized crime perforce has to treat the external relations of the unit; organized crime disregards the neat jurisdictional boundaries within which most law enforcement agencies operate. Yet, external relations, as practiced today by most intelligence units, are often characterized by mistrust or jealousy and frequently are limited to informal conver-



sations between longstanding professional intimates.

### **Obstacles to Effective External Relations**

There may be good reasons for hesitation in seeking external associations. The neighboring agency may have a reputation for corruption so strong that it is wisest to be wary about all levels of its structure. If its officers are not corrupt, they may be naive or undisciplined, and the consequences of their mishandling a delicate matter of concern to both agencies might be deeply injurious to both.

Moreover, physical factors may justifiably inhibit good communications between agencies. The neighboring agency may be housed in decaying buildings that are impossible to secure, for example, or be laboring under unrealistic workloads that result in the warping of proper intelligence procedures despite the best will and talent in the world. And there is the bedrock problem that cooperation between two or more agencies depends in the final analysis on an acceptable degree of reciprocity. If one of the agencies involved does not want to cooperate with another, there is little that the latter can do but keep on trying to initiate a productive relationship.

In some cases mistrust or hostility between agencies is based primarily on tradition. A longstanding policy of not cooperating or communicating with a neighboring agency may have its roots, for example, in a history of earlier corruption or political influence that has now in fact begun to be corrected. Old habits, however, keep the agencies apart because neither party has reexamined the situation. In other instances trusting relationships have been established only between certain units or particular individuals. In effect, certain limited channels have been tested and found worthy. Such channels are discreetly maintained in an atmosphere which tends to inhibit the development of new openings. But they are better than no channels at all.

Other apprehensions may be based on unit pride—or scorn directed at another unit—or on concern for such things as receiving credit for successful joint operations, or at least a proper share of the resulting headlines. If one agency opens a press policy, another may be scared off because the head is fearful lest his materials

appear on the front pages of the morning newspaper. There may be political differences which keep police agencies apart or, as is more often the case, a prosecutor's office of one political persuasion may refuse to cooperate with a city police department in a jurisdiction where the mayor is of a different political stripe. Separated by politics, the professionals in each agency often find that, even though they might wish to get together, an official (often unstated) policy deters any contacts other than the most perfunctory.

Finally, there are those situations where an agency contents itself with the form of external contact but not substance. Exchanges of information take place, officers visit back and forth regularly, but the intelligence moved from one agency to the other is inconsequential—often no more than official arrest records and newspaper clippings. This is not effective external relations: it is a sham designed to cover some concealed motive for not wishing to communicate. Or it may conceal an unrealistic evaluation of the sensitivity of materials held by the first agency that would be useful to the second.

### **Actions To Improve External Relations**

The intelligence unit commander can improve his external relations; he can maximize his collection take from outside sources, and he may even be able to coordinate strategy against the very mobile target, organized crime. The first task, clearly, is to define those law enforcement agencies that are likely to be of most value in terms of exchanging information and coordinating strategy and to review past and present policies concerning cooperation with them. Having determined which ones are either not open to him or open only on a limited basis, the unit commander should fully explore the reasons therefore and identify where new efforts might pay off, as well as where it would still be wise to say aloof. With his targets selected he can then poll his associates to determine who has personal or even official contacts in the target agencies.

It is important before he initiates approaches that the intelligence unit commander have a precise plan in mind. Would it be more fruitful to adopt a policy of full faith and credit—to open the doors wide to personnel from the other agency in exchange for a reciprocal guarantee—or would it be preferable to suggest exchanges at first on a certain limited and agreed list of

subjects between certain designated officers? Or, given past history, would it be better to start cautiously by proposing a series of informal get-togethers for the purpose of building confidence before talking business? If some suspicion of the integrity of the target agency lingers on in the mind of the unit commander, should he test the water first before entering into any more ambitious exchange plans? A simple test could be made. The target agency could be given some information that would require further action on its part, including perhaps the arrest of a known hood. The information should not be so sensitive that its misuse could be harmful to the releasing unit. The recipient agency could then be observed for a period of time to see what it does with the sensitive information received. Such a simple, one-shot test hardly constitutes a clean bill of health if the results are favorable, but it may help the unit commander to overcome hesitation in his own agency and provide the impetus necessary to carry the probe a little further.

### The Protection of Intelligence Information

Once embarked on a course of exploiting external contacts, the intelligence unit commander must look to his own house. He must be confident that what he has to offer his newly developed partners in the fight against organized crime will be worthy of exchange—or to put it more crassly, that it will produce something equally valuable from the other agency. To do this he must be confident of the validity of his own restrictive procedures. This entails a considerable output of intellectual energy and, if storage methods are all too sloppy, some vigorous redirection of the information management function. First and foremost he must ask himself whether he has set too high the restrictions on the movement of materials outside of his unit. Are restrictions, for example, imposed on all informants' reports whether or not they reveal something of the informant's identity? Are *all* the documents pertaining to a certain matter or a particular individual actually as sensitive as those at the core of the file? Only the unit commander can in the end answer most of these questions, but he can get help by instituting a full-scale review and reevaluation of his unit's files. On the basis of such a survey he can, hopefully, make intelligent decisions and he may be

able to institute new or revised procedures. (The handling of restricted material is discussed in detail in chapter VI. See figure 10, page 54, for a sample log which is designed to provide data useful in any analysis of external flow of intelligence materials.)

Reciprocal external arrangements will require certain procedures that do not place all the burden on the agency to which materials are being passed. Establishing (or reviewing) contacts with another agency when the relationship has long been moribund or nonexistent, is a delicate matter. There is no point, however, in assuming the worst about the new partner and, as the song goes, "willing him to fail." The agency originating the passage of materials can take procedural steps which, in effect, protect the relationship by protecting both agencies against misuse. The simplest and most widely used device is to excerpt materials from sensitive files, carefully "sanitizing" those parts that are most critical as to source, circumstances of collection, or whatever. The synopsis or "sanitized" summary can then be passed without fear of the consequences of mishandling. This is a useful procedure when dealing with highly sensitive matters or documents which, if revealed *entoto*, could be construed as an invasion of privacy rights. It is, however, time and manpower consuming and where possible exact copies of file or documented materials should be used instead. Here special precautions are essential. (Detailed control features are spelled out in the section entitled "Information Control" earlier in this chapter.)

There is no means of guaranteeing absolutely that the receiving agency will not misuse the materials received in some way. It will certainly be able to copy them or to send them on to other agencies not approved by the originator. For this reason, the buckslip attached to such materials, or the materials themselves, should not only be clearly marked as to origin, but should also bear a stamped legend, "not authorized for external use except by . . . ." with the intended recipient agency's name inked in the blank. Unauthorized public exposure of documents bearing this legend would, of course, remove the responsibility of the originating agency, although it might well be harmful to the individuals mentioned in the documents.

In the last analysis the only inhibition to



frivolous—or malevolent—mishandling of materials by another agency is the shutting off of contacts by the originating agency. Indeed, if there is suspicion of illegal use, the best recourse may be to Federal authority. This is a harsh sanction for one law enforcement agency to use against another—particularly where efforts to enlarge communication flow have been made—but it may be the only available means of enforcing acceptable standards of professional conduct on some elements of the law enforcement community.

### **A Treaty as an Aid to External Relations**

Where the barriers against effective contact between law enforcement agencies, or subunits of them, are based not so much on integrity factors but on other considerations, such as jealousy, personal frictions, or ingrained habits that have become practices to live by, there may be some benefit in what might be called the institutional approach. This approach can take many forms. The analogy drawn from international relations of the treaty can be usefully applied to one form. By this method the head of State (agency chief) designates a senior associate (deputy or chief inspector) to act as plenipotentiary (negotiator) with some representative of the other State (agency). Negotiations (discussions) are held to determine, first, what minimum set of common objectives desirable to both parties can be agreed upon. These findings are communicated to the two heads of State (agency chiefs) and if both parties feel they give promise of producing effective areas of cooperation, a second session is held by the negotiators to hammer out a treaty (agreement).

The agreement might cover only the bare essentials at first: levels of material to be exchanged and rules for exchange; some predetermined schedule for periodic official get-togethers to eliminate misunderstandings and improve mechanics; a formula for joint press releases in the event of arrests or other action resulting from the passage of one agency's information to the other. Naturally, the potential areas for agreement are almost unlimited; new elements can be added at any time as long as there are opportunities for periodic discussions. Equally obvious is the fact that as cooperation grows, less and less commitment to the making of

formal amendments to the "treaty" will be necessary.

In some major cities that are also State capitals, and where many law enforcement agencies, local, State, and Federal, work in overlapping jurisdictions, an organized crime intelligence committee with regular meetings and agreed-on arrangements for exchange of information may be a practical device. Similarly, Federal strike forces could sponsor subcommittees on intelligence as part of their own apparatus. Apart from other benefits, this device would probably help toward better techniques of targeting against organized crime.

The institutional approach to external relations is limited only by geographic proximity, good faith, and imagination. At its best, it could be a prescription for regional coordination of intelligence—and even strategy; tasks could be allotted, arrangements made for joint operations, and new intelligence requirements agreed upon and allocated. Relations beyond the immediate urban area in which the law enforcement agency is located will probably have to continue for some time on a catch as catch can basis. Here personal relations will be critical. Intelligence unit commanders will have to avail themselves of every opportunity of contacting distant opposite numbers, by attending conferences whenever possible, by themselves traveling on extradition trips to make the acquaintance of opposite numbers, and encouraging the latter to return the visit, etc.

### **External Liaison**

Liaison officers can be key figures in the external relations function of the unit. Liaison can best be thought of as extending the unit commander's authority or voice to areas beyond his immediate responsibility. It can scarcely succeed unless it does indeed carry the weight of the commander, and for this reason the function should be controlled from the commander's personal office. In a very real sense, liaison is simply another form of dissemination, and if it is done skillfully, it can also be another form of collection.

But what the liaison officer collects he may not necessarily be free to channel into the unit's receiving point for normal processing through the system. The information obtained, say, from the unit's liaison with a Federal agency,

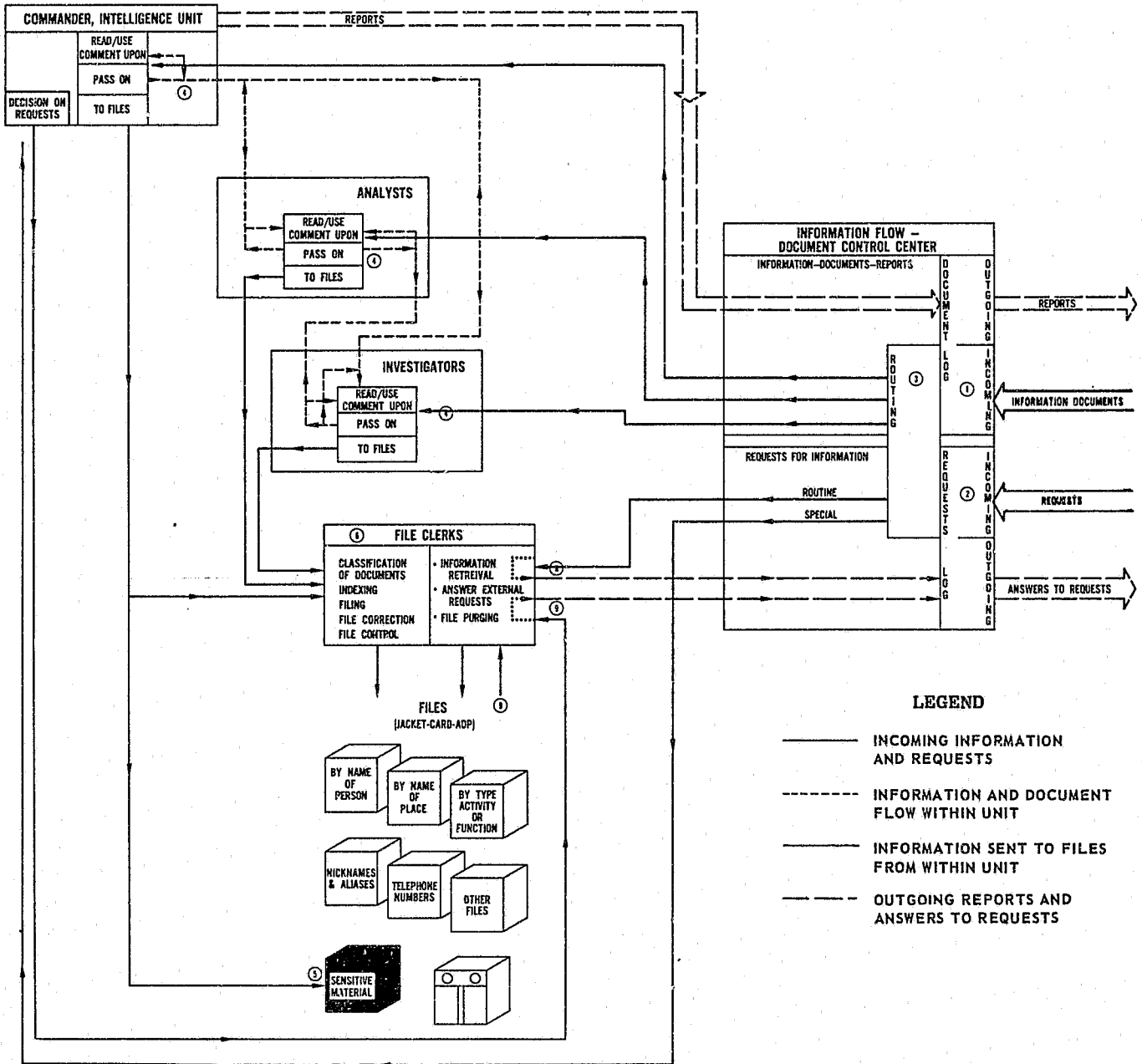


FIGURE 11

**CONTROL AND FLOW OF INFORMATION AND DOCUMENTS**

### FIGURE 11 – CONTROL AND FLOW OF INFORMATION AND DOCUMENTS

<u>Step</u>	<u>Activity</u>
1.	All documents and pieces of information must enter through a single point in the intelligence unit and be logged in. The log should show date, time, subject, originating office, and initial recipient in unit.
2.	All requests for information, whether from inside or outside the agency, are to be logged separately in a request log. Data on the log sheet should include date, time, subject, requestor, and whether routine or special handling. Routine requests are those covered by unit SOP; special requests are those requiring approval of the unit commander before action taken.
3.	All documents and pieces of information must be routed to commander, analysts, or investigators for decision on disposition after having been read.
4.	The recipients of the documents and information—the commander, the analysts, and/or the investigators—may do one of several things with the material as it comes to their desks. They may <u>read</u> , <u>initial</u> , and <u>pass on</u> . In addition to reading, they may make some <u>comments on</u> items in the material. The material may also be <u>current</u> and they may <u>make use</u> of it by adding to the information they are accumulating on a current research project, or a current case.  In passing the material on, each recipient may choose (or his actions may largely be determined by SOP) to pass it to one or both of the other recipients, to send to the files, or to throw away. The secondary and tertiary recipients must also go through the same procedures (although often the first recipient will have marked the disposition he desires on the document).
5.	Ordinarily the handling and storage of material considered to be of a sensitive nature will be under the control of the commander of the intelligence unit.
6.	All filing should be done by the filing clerks. They should classify and index new information. They should be responsible for refiling material that has been taken out of the files for use. They should, to the greatest extent possible, be the only persons allowed to pull information out of the files. Where such information is to be removed from the file room, it should be taken only by a person authorized to do so and record must be made of the action—date, time, file number, and recipient.
7.	The organization and nature of the files will depend on the system adopted by each individual unit. However, in all cases, cross-indexing must be pushed further than merely name files. In particular, functional files should be established as an essential tool of the analysts.
8.	Requests for information that the information control determines, on the basis of his SOP, to be routine will be sent directly to the file clerks who will answer the request on the basis of specific SOP set forth by the commander.
9.	Requests for information that information control judges to be special will be sent directly to the commander (or to a person designated by him to have the responsibility) for decision as to how it should be answered and specifically what information is to be given.

may be restricted for passage only to the commander. In this case, of course, the commander will find himself in a position to use the information as a test against his own; it will be an evaluative tool, assuming he cannot pass it on in a useful way to his superior.

Using liaison personnel will remain a luxury for most departments until such time as the value of collection-in and dissemination-out become obvious to agency heads and their budget directors. Indeed few unit commanders will enjoy the services of more than one or two liaison personnel—if they can afford any at all. Thus efficient use of this rare asset is good business.

On balance, experience suggests that instead of sending the liaison officer out as one would a traveling salesman to cover as many customers as possible in a given tour, his program should be carefully planned by the unit commander. He should spend most of his time at that agency from which the greatest returns are to be anticipated, or where missionary work has long been neglected. Repeated visits at offices already cooperating will probably evolve into social affairs. (On the other hand, an occasional check into friendly premises may prevent minor abrasions from festering into ugly sores.) A good working assumption is that where there has been little contact and cooperation in the past, the liaison officer will have to spend a considerable amount

of time establishing his good faith and credibility. His commander had best not expect sudden miracles; it will be a painstakingly slow process.

The liaison officer will probably find it useful to keep a running, written account of the commitments he has made and has had made to him. This will be useful if he has to appeal to his commander for assistance in nudging the commander's opposite number into being more forthcoming in the relationship. It can also serve as a planning base against which to judge the desirability of moving the liaison officer on to more fruitful targets. If the account shows that the other agency's promises of delivery are mostly unfilled or under-fulfilled, then scarce talents may better be applied to knocking on other doors. Finally, successful use of a liaison officer will depend in great part on his own knowledge of what goes on in his home unit. He should be obliged to spend at least a third of his time in his own headquarters keeping abreast of new developments, longstanding needs, and recently elaborated requirements. He is, after all, not only an emissary for his unit's commander, but also a prime collector for the unit. As a collector he may pump away at dry wells for a good part of his assignment, but his services will have been worthwhile if he brings in an occasional gusher.

# Chapter IV

## STAFFING THE INTELLIGENCE UNIT

*Special selection problems for each category—commander, investigator, analyst.*

*Highest criteria for selecting personnel in all categories: integrity, intellectual/analytic capacity, meticulousness.*

*Personal interview important step in selection process, especially in determining motivation.*

*Most effective selection requires realistic testing, using on-the-job problems.*

*Changing nature of organized crime increases requirement for generalist and specialist analysts.*

*The academic community as source of specialist analysts on consulting basis.*

*Agency career development must take account of special problems posed by personnel requirements of intelligence unit.*

### INTRODUCTION

Any supervisor setting out to fill a critical and sensitive position in his organization asks himself two basic questions: "Is the person I am considering for the position capable of doing the job?" and, "Can other officers work with him effectively?" In law enforcement (as well as in many other occupations) there is always a third question: "Can I trust the person I am considering; is he clean?" And then, from the point of view of intelligence: "Can this man think analytically; can he assemble and structure pieces of information to answer the question, why?"

In looking at the staffing of an intelligence unit, personnel requirements can be divided into four general categories. Most important is the unit commander. Selecting a commander usually becomes a problem of trying to match the capabilities of a senior member of the agency with the unique requirements of the position.

A critical category is that of the analyst. This chapter will put considerable emphasis on the analyst since he is a member of a relatively rare species in the law enforcement aviary. In many agencies, the analyst will not be a transfer but a professional hired from the outside.

The investigator category poses yet another selection problem. Unlike the analyst, the investigator usually will be a transfer. But, he will be faced with unique challenging requirements. In addition to being able to conduct an investigation, the investigator in an intelligence unit must be able to work on a team with analysts, develop new approaches to the increasingly sophisticated illegal enterprises of organized criminals, and, at the same time, draw satisfaction from making investigations without making arrests. The selection of investigators and analysts is generally treated as a common problem, since, where possible, these functions should be thought of as interchangeable and to a great ex-



tent requiring the same level of intellectual equipment. The fourth category is information control and clerical. This group poses no unique recruitment problems and is not discussed in this chapter.

### THE UNIT COMMANDER

Choosing an intelligence unit commander requires a positive answer to all the selection questions mentioned above, but the rather special character of the position to be filled makes for a somewhat different weighting of the questions. The right man for the post of organized crime intelligence unit commander cannot, of course, be found by any process. All sorts of limits, which are familiar to any bureaucracy, are built into the system of choosing. The selector may find himself with imperfect choices. As he mentally juggles the attractions of what may already be a smaller list of availables than he would have wished, he may have to give lower than desirable marks for some qualifications like cooperativeness while satisfying himself that, "nobody can fault X on brainpower." Or he may be thoroughly confident of Y's integrity, but suspects that Y's taciturnity hides not wisdom, but smugness.

However, if he has any misgivings whatsoever about the integrity of X or Y, he should no longer even entertain their candidacies as acceptable. The intelligence unit commander has to be—if nothing else—vigilant about the possibility that organized crime will be seeking in any way it can to corrupt the law enforcement officers of the agency. There is no room for compromise on this point. Any weakness or softness in the element of the agency most concerned with the penetrative stratagems of organized crime, and any weakness or softness in the element of the agency charged with the collection and maintenance of the most delicate of intelligence materials, would be perilous to the agency as a whole.

Thus, integrity is a primary consideration in selecting an organized crime intelligence unit commander; it is critical. In making his choice the supervisor can give nothing away on integrity even if the scales holding mental agility and cooperativeness are imbalanced. There is one other obvious but nonetheless highly critical reason for insisting, as a starter, that the intelli-

gence unit commander have impeccable integrity credentials. In great measure he will (or should) set the tone for his unit. He must not only symbolize incorruptibility by his own recruitment policies and personnel management practices, he should be instilling in his unit a deep sense of pride in its own unassailable integrity. The agency head can expect no less of the intelligence unit than that it be clean.

### GENERAL CRITERIA FOR STAFF SELECTION

Much of the same general criteria as apply to selection of an intelligence unit commander will obtain in recruiting the balance of the unit's staff. (See figure 12, page 71, "Criteria for Selection," at end of chapter.) This is not to say that the commander should seek to fill his office exclusively with subordinates who think as he does. He will, on the contrary, need all manner of men and women who can look at intelligence problems from a variety of perspectives. But whatever their individual views or skills, they must have a strong sense of integrity and high intellectual level. As far as being "comfortable" with his subordinates, a unit commander is better off if he has some "prickly pears" in his basket, who will not hesitate to suggest the unorthodox approach and challenge traditional assumptions, than if he has a collection of agreeable, think alike yes-men.

A search for bright, tough-minded personnel can present difficulties. The unit commander should take care to avoid certain personality types who, though they may be impressive at first acquaintance, will not have the flexibility for sound intelligence work. The officer with his mind made up on most issues—no matter how polished that mind may be—will have difficulty dealing with the unexpected. If, for example, his investigation has led him to conclude that a certain target is surely the wanted culprit in a complex case, he may tend to overlook evidence that begins to suggest the contrary; he may have more confidence in his own intuition than in the facts. At the worst, such personality types become zealots or crusaders, singlemindedly pursuing objectives they have identified for themselves with little regard for the obligations of the unit or even the law enforcement agency as a whole. It may occasionally be possible to

harness such a person to a specific and narrow specialty where his burning, uninterrupted interest in the subject can be an asset, but this is seldom the case.

One approach to intelligence personnel recruitment is to begin by setting age limits quite low and then identifying the candidates with a genuine thirst for self-education and self-improvement. Intelligence is a mind-stretching business, its targets change, its methodologies are improving constantly and require more and more innovative ideas to cope with the growing sophistication of organized crime. These are aspects of intelligence work which can be used both as appealing temptations to the bright candidate and also as simple conversational topics designed to gage the candidate's responsiveness to challenges.

### The First Step — the Interview<sup>1</sup>

It is almost always beneficial to include a healthy amount of personal interviewing in the staff selection process. Beyond building the supervisor's confidence that his choice is a good one, the interview technique sometimes accomplishes what the written test can rarely do objectively. It allows the quality of a man's mind and his disposition toward the proposal at hand (in this case tackling intelligence work) to filter through unequal or uneven educational backgrounds or mediocre fitness reports from previous supervisors.

The most fruitful interview is that which is prepared for by both parties. A useful requirement is that the candidate submit in advance a brief autobiography (usually no more than two pages), which should contain at least one statement about his career expectations in the agency. This requirement has several advantages:

1. It discourages frivolous applications;
2. It may surface dimensions of the applicant not revealed in his personnel file;
3. It is, or it may be, depending on what degree of help he may have received in its preparation, an early glimpse of his capacity for written articulation;
4. It impresses on the candidate the special

<sup>1</sup> One hurdle is not discussed in this chapter—the full field background investigation of applicants. This is covered in chapter VI.

5. It provides the interviewer with something to talk about.

The interviewer must, of course, do more than read the autobiography. He should, as carefully as possible, compare the autobiography with the contents of the candidate's preliminary background investigation or personnel jacket. Moreover, the interviewer should be prepared to level with the applicant. He must know and be candid about any career disadvantages implicit in the candidate's moving into intelligence work; he must be prepared to open himself to probing questions on this score. In other words, he had best be completely confident about agency policy and agency traditions in personnel practice.

Obviously, any good interview will concentrate on probing motivations. This is especially important for intelligence work where the rewards are more often the satisfaction of unravelling a problem than they are monetary or direct participation in pursuit of the criminal. There are, also, other qualities to probe for that few people willingly and openly display. Foremost among these is meticulousness or scrupulous attention to detail. Without this quality, good intelligence discipline can quickly dissipate, analytic studies can founder, and cases may be rejected by the prosecutor. A law enforcement officer who has previously had investigative experience should be asked to bring in a copy or copies of old field reports he has written. In a subsequent or followup interview, this report can be used as the basis for a discussion of personal work habits, collection techniques, thoroughness in following up leads, etc. For a more exacting measure of a candidate's tendency to think and work with precision, commercial tests are available. Because of cost factors, they are worthwhile only if more than a handful of candidates are being considered.

### Investigator Candidate Testing — Use of Field Problem

If, after the initial interview, a prospective intelligence investigator shows promise, it may be wise to involve him in a structured field problem (or the designing of an analysis model). Such tests require considerable advance prepara-

tion if they are to reveal much that is useful or new about the participant. For example, a field problem might be put together by an experienced investigator using materials drawn from a variety of past investigative activities. A rather simple, noninterrogative problem could be devised that would require some passive surveillance, address and automobile license checks, public library research, an examination of official records and the like. The applicant would be obliged to fill out two written statements at the conclusion of his field problem: one, a standard investigator's report, which he would be given at the start of the exercise; and two, a complementary form in which he recorded a log of his activities with an explanation as to why he decided to move on from one investigative point to the next. There should be no "school solution" to such a field problem, but good discipline would require a fixed time table for completion of the exercise.

Clearly the two written reports would be products of great interest to the selectors. They would, if the exercise were well designed, indicate the candidate's capability for advance planning (or his tendency to bolt into situations), for careful husbanding of his time (or, contrarily, for wasting his energies pursuing nonproductive leads), for thoroughness, clarity, attention to detail, etc. A good field exercise report would also reveal something of the candidate's imaginative-ness and flexibility—whether or not he had followed any set path that finally had hit the selected target.

### **Analyst Candidate Testing -- Use of Analytic Model**

Testing an analyst candidate by involving him or her in the construction of an analytic model is in many ways a more delicate selection technique than the field exercise. First, there is the practical problem that this approach requires the use of real files about real or suspected criminal conspiracies. If the candidate is not yet a full-fledged member of the law enforcement agency, or if no full background investigation has been completed, there is a risk, albeit slight, that the files could be compromised. Fabrication of names, addresses, etc., in existing files to overcome this difficulty would be a herculean and probably uneconomic task. But, presuming

that the candidate is sufficiently well known and regarded by the intelligence unit to merit already a measure of trust, a good test can be devised on the basis of in-house materials.

The purpose of the test would be to observe how the candidate tackles the challenge of solving an intellectual problem in intelligence. The test might consist of a single question: "By exploiting existing files and documents in the unit's storage facilities, can you suggest ways and means of establishing whether there is a relationship between person X and business Y and illegal activity Z?" Or, depending on the materials available, it might be made more complex: "Prepare a statement describing the likelihood of there being an organized criminal element active in business X, and suggest an approach for deeper exploration of this subject, complete with the goals you would hope to achieve in such an exploration." In both cases, the applicant would be given a timetable, specific files would be made available for perusal, and an on-duty analyst would be assigned to the candidate to answer specific questions as to the availability of other files or resources.

The on-duty analyst's role would not be that of coach or adviser, but simply that of interpreter of the available data base against which the candidate was working. The on-duty analyst would volunteer nothing and probably, in most circumstances, his main task would be to respond to questions put by the candidate, "I can't tell you that. You have to make your request more specific. If you do, I can tell you whether what you are looking for is available or not, and if it is, where you can find it."

The role of the on-duty analyst in this form of testing is two edged. First, he saves the time of all concerned by pointing out where wanted materials are located. The applicant need not spend valuable time learning the particular filing and storage system employed in the unit. Secondly, the on-duty analyst can be called on by the selection officer to give an account of how the applicant handled the assignment; that is, whether the process came quickly and easily, whether bad leads produced evident frustration and discouragement, whether the files were handled with care, etc.

But the principal product for the selector's concern will be the applicant's answers to the questions posed and the logic of his manner of

tackling the problem. What answers he comes up with, of course, are less significant at this point than how they were handled and what ingenuity was shown in shaping them. Unless a seasoned analyst from some other law enforcement agency is under consideration, it is not experience that is being tested in the circumstances described above, but imaginativeness, resourcefulness, thoroughness, logical use of research tools, and self-discipline.

### The Selection Process

If the performance of two or more applicants in any or all of the screening devices described above could be measured against one another, it would be relatively simple to decide which one had done the best job, and, other things being equal, he should be certified to fill the vacancy. But this happy state of affairs may not always obtain. Candidates may appear one at a time or irregularly throughout the year so that satisfactory comparisons cannot be made directly. The selector or selectors, then, will have to develop consciously their own sense of standards and stick to them. The momentary need to beef up an overtaxed staff should not be used as an excuse to lower the entry threshold for newcomers. An ill-prepared investigator or analyst will, over the long run, put a greater burden on his (or her) more skilled associates than if his slot remained unmanned until a qualified applicant turned up.

A problem of a different nature arises when there is an embarrassment of riches; that is to say, when an intelligence unit has a number of qualified applicants for but one or two places and is hard put to make a choice. On the surface this is an enviable condition for the intelligence unit. The commander can hardly go wrong because whomever he picks will probably become a sound member of the team. True enough, but will he pick the *best* of the lot by exercising careful self-examination of his own selection technique?

The natural human tendency under these circumstances is to find reasons for *eliminating* one or more applicants, not reasons to *select* one or more out of the lot for the job. This is a far more subtle, and often subconscious, process than that practiced at the moment when application papers are filed or early interviews are

held. In the early stages of selection there are clearly those who may have the potential for the position and those who clearly do not under any circumstances. The latter are shaken out with relative ease according to more or less uniform standards. If the qualities of an applicant remain in doubt after the initial cut, he or she can be passed along to participate in the more intensive interviews and field or analytic exercises. Assuming, however, that all these barriers have been successfully overcome, the selector is now on the spot.

Up until this point he has thought positively about the candidates who were successfully moving along the selection process. If he has been personally involved in the various stages of interviews and testings, he may even have envisaged in his mind's eye how each one of the candidates would fit into his apparatus. "X would work well with George. Y looks as though she's just right to take over information control from Harry so we could put Harry back in the field . . ." etc. But, faced with choosing among several demonstrably capable applicants, the selector often turns negative. He must winnow the field to one or two, so he starts looking for disqualifiers that have not hitherto surfaced or, if they have, were regarded as irrelevant or insignificant. Exhaustive negative scrutiny finally produces one or two candidates with the least number of possible disqualifiers (and they are only possible at this point) and the prize is awarded to the most inoffensive.

The insidious effect for such a technique, of course, is that by emphasizing the search for weaknesses in the candidates, any slight deficiencies noted tend to become exaggerated in the mind of the selector: Two spelling mistakes remembered on the investigative report exercise of X very quickly slides into scepticism as to X's ability to handle the English language. The on-duty analyst working with applicant Y noted that he was "highly curious" about the promotion possibilities in the unit, so Y may be dangerously ambitious. At the worst this kind of thinking can lead to a form of amateur psychoanalysis of the applicants with bizarre results: "Hmm, I wonder why Z is *still* a bachelor?" Obviously, in all these cases the selector is doing the unit no service at all by straining for reasons to eliminate qualified candidates rather than pinpointing the best of the good.

Selecting the best out of the good is, of course, no easy matter. Very often the choice will have to be made on the basis of fine tailoring. One of the candidates will have a range of attributes more suitable to the particular opening than his competitors. If this is not the case, however, the determination become a little more complicated. About all the selector can do at this point is to start searching for qualities that were not necessarily qualifiers at the beginning of the process. Some of the most telling in this regard are the range of a candidate's interests—what does he do with his spare time? What books does he read for relaxation?—his candor as well as his self-confidence; without resort to self-deprecation, how honest is he about himself? What about his capacity to synthesize many and varied inputs; can he take fragments of a conversation or the various elements of a biographic file and come to generalized conclusions rapidly but undogmatically?

There are, quite naturally, many other qualities or characteristics to look for that may be more appealing to the individual unit commander who must do the selecting than those listed above, or that may more precisely measure the applicant's capacities for the opening in question. The following are offered here only because they are in themselves important attributes for the good intelligence officer: a broad range of interests because this may signify a flexible, thirsty mind with a wider than average social interest; candor about himself because this is a good gauge of innate honesty and integrity; capacity to synthesize because successful intelligence depends on getting at the core of a problem no matter how dense the trivia surrounding it.

### **The Special Problem of Choosing the Intelligence Investigator**

Under normal circumstances, the intelligence investigator will be transferred into the unit from the detective branch. He will have gained experience in the more traditional modes of investigative work. He will be part of the normal career structure, looking forward to further promotion which likely will take him out of the intelligence unit. The area of conflict thus posed is that of the special requirements of the intelligence unit versus the career service of the agency. The intelligence unit commander will

have to fight hard for freedom to select from among the best investigators in the agency. Where he can find none that fit his needs, he may have to fight even harder to get the right to hire from outside.

The intelligence unit should look for trained investigators. In most circumstances, the unit will be relatively small and will have little time to train investigators on the job. The difficult nature of organized crime investigations demand experienced personnel. Investigators should already know the city and at least the street level operations of organized crime and the main areas of such activity. Hopefully, they will have served in one or more of the precincts which are major operating areas for the organized criminal.

But the trained investigator also presents a problem in the selection process. The best target is an investigator who has done well at routine work but is not satisfied. He should respond positively when the more complex investigatory work involved in fighting organized crime is discussed. He must be a man that can both take direction and have sufficient initiative to develop avenues of approach to a problem over and above those suggested. The trained investigator who seeks only the rapid arrest should be avoided. He will not be able to live in a world where a complex investigation might go on for months and where the ultimate arrest is the responsibility of another unit; that is, the case he begins would be turned over to others.

The intelligence investigator must be able to work in harness with the analyst. He must be willing to take leads from the man (or woman) sitting in the office. He must be able to participate in the analysis itself, to help guide the analyst in turn. He must be factually correct in his reporting. But he must also be able to develop a capacity for at least "first-cut" analysis and interpretation of the meaning of his findings. In fact, he should relish this aspect of investigatory work.

The intelligence commander in many cases should think of developing his unit in such a way that at least some of the investigators and analysts can be interchangeable. (See chapter III for a discussion of this point.) In most cases, this would mean that they would both have to be badged or sworn officers. It would also mean that the analyst would have filled an investigator billet before being selected for his current role.

The interchangeability of at least some of the staff greatly enhances the flexibility of what is normally a small staff. Personnel can be shifted to investigation when cases are in their early stages, and then to analysis as the information begins to accumulate.

### **Determining the Analytic Discipline Needed**

Since the introduction of professional analysts to organized crime intelligence is a relatively new phenomenon, there are more theories about which skills to apply than there are analysts in position. The use of accountants and attorneys in piecing together disparate pieces of information to form a finished intelligence product (or more often an actionable case) is not unique in law enforcement, but the employment of economists, sociologists, anthropologists, psychologists, etc., certainly is. What then, are such specialists able to do for an intelligence unit? Which skill fits which problem area? There are no easy answers to these questions, but it is possible to make some generalizations which may serve as pathfinders for intelligence unit commanders—who, after all, must deal with local situations and the local characteristics of organized crime as they see them.

#### **The Nonspecialist Analyst**

To begin with the least specialized analytic talent, many intelligence units in the country have found that the use of recent liberal arts graduates is rewarding. Such people, frequently young women, are quite simply analysts. On arrival they may know nothing about criminology, or police work, or the law, or even the methodology of data analysis, but if they are intelligent, precise, and anxious to explore generally uncharted waters, they can soon make important contributions to criminal analysis.

By and large they should deal with aspects of the collation process and the pure analytic function, which is the search for relationships. Where an intelligence operation is newly under way or is revamping its approaches, nonspecialist analysts can be invaluable in designing filing and cross-referencing systems best attuned to the analytic process. The analysis they do will mostly involve charting patterns of criminal conspiracies or legal and illegal holdings and interests of organized criminals. They may prepare

appraisals of the state of organized crime in their jurisdictions, or reports on the trends of criminal activity in the area based on the soundings of investigators or drawn from other sources. They may be used to research complex problems by exploiting public records of other official institutions and libraries. In short, they will be applying logical deductive techniques effective in any context to the task of unraveling and (ultimately) exposing covert criminal activity.

#### **The Specialist Analyst**

Not all analysts are equipped to handle the more technical explorations and studies necessary to achieve an understanding of such things as business frauds, securities manipulation, and shady financing and accounting arrangements for otherwise legal businesses. Where organized crime has moved into high gear and is operating more or less covertly in these areas, highly skilled specialists, such as accountants and economists, may have to be called upon. Naturally, an intelligence unit commander must look to the most efficient way of getting such analysis done. If he is confident that the target group represents the only sophisticated threat in his jurisdiction and that, if it is rolled up, no other group is likely to come along and enter the vacuum, he may decide that it is best to get the job done by using borrowed personnel—from some other law enforcement agency in the locality. If there are no such specialists available in law enforcement harness, he may rely on specialists on a consultant basis. If he feels he is likely to have a continuing problem, then the unit commander must enlarge his staff directly to cope over time with this complex dimension of criminal behavior.

Similarly, sociologists and psychologists or anthropologists can be profitably deployed in analyzing intergroup behavior with a view towards detecting weak links in organized crime combinations for the application of countermeasures. For example, if two or more ethnic minority groups are working together in a marriage of criminal convenience but not of devotion, the dynamics of such an uneasy relationship could be studied by a specialist familiar with the cultural imperatives of the groups with a view towards better understanding what makes the combination hold together, or what would be likely to pull it apart. In like fashion, soci-

ologists can often be helpful in counseling undercover agents on acceptable behavior in the roles they must assume, and psychologists can assist in developing techniques for the delicate business of handling recalcitrant or self important informers.

As noted previously, there are no hard and fast rules for the deployment or even the employment of specialists in an intelligence unit. But one managerial principle should remain uppermost in the commander's mind. He must have a comprehensive plan as to how he will use the specialists after the most tempting and immediate targets are dispatched. If he has no permanent, continuing use for specialists, he had best not hire them in the first place. They are probably too expensive to employ as nonspecialist analysts. Even if they were so used, they would probably soon grow restless and move on to greener pastures.

The imaginative intelligence unit commander with nonrecurring requirements for studies in depth or the occasional analysis of highly complex problems can sometimes avail himself of other community resources. Most major municipalities have more than one law enforcement agency. It is not impossible that where two or more agencies are working together in full faith and confidence, they could share the costs of finding one highly specialized analyst between them. Or an accountant, say, might be agreeable to entering into a retainer relationship with one or more of the agencies. Such arrangements are obviously not as satisfactory as having the full-time services of such a person, but they may be all that can be defended from a cost standpoint—and they do have the advantage of keeping an analyst experienced in intelligence work on tap.

A variant of the retainer relationship is the use of contract employees or consultants when particular needs arise. This, of course, may be costly and is often time consuming for the agency that wishes to let a contract. Much depends, of course, on the rigidity of local laws governing the letting of such contracts, hiring temporary employees, and best-source agreements. Generally speaking, this kind of arrangement is most satisfactory when there is a specific objective task at hand that either requires special skills unavailable within the agency, or that, if tackled by the incumbent staff of the agency, would

seriously disrupt normal working routines over an extended period of time. Some obvious examples are: the redesign of an intelligence unit's existing filing and retrieval system, a long-range study of travel patterns of leading criminal figures as a means of determining the nature of illegal activities, a survey of real estate ownership fronts in a given section of a major city. Not to be forgotten, of course, is the kind of research which may not be directly related to criminal acts, but is needed to provide strategies for countering organized crime. For a State or municipality lacking a loan shark statute with teeth, a study of the effectiveness of different loan shark statutes in other jurisdictions might have more long-range impact than many activities more traditional to intelligence units. Such a study might best be done by an attorney or law professor under contract or on a consulting basis with the intelligence unit.

#### Use of the Academic Community

The resources of local or regional universities should be exploited for specialized personnel assistance whenever the budget permits. Surprising pools of talent can be tapped by the imaginative unit commander if he is willing to spend some time exploring such schools, particularly those with modern departments of criminology, management, public administration, systems sciences, sociology, etc. Concerned scholars working in fields that at first glance seem to have little connection with law enforcement intelligence can be identified working in a variety of disciplines. They may be found on the permanent faculty or in the ranks of graduate students preparing advanced degree dissertations.

Approaching the campus is a delicate matter if the intelligence commander has not already established contacts or friends who can pave the way for him. He had best not blunder into the dean's office looking vaguely for advice as to who is undertaking specific kinds of research that might be usefully employed by an intelligence unit targetted on organized crime. This may arouse all manner of latent and not so latent suspicions as to his real motivations and create an atmosphere of hostility that, even though unjustified, deters scholars, who would otherwise be interested in his needs, from contacting him. One ideal way to begin a dialog with a portion

of the academic community is to follow the professional literature, say on criminology or management, and select a local author whose work may be relevant to criminal intelligence or police administration and write him directly about his research. There are countless ways to bring about a discreet encounter with members of the academic community, of course, but the essential matter to keep in mind is that, no matter what tactics are used, they must be above suspicion. The purpose of the visit must always be explicit and unchallengeable: a search for intellectual assistance for a law enforcement problem of gravity and delicacy. Only a few scholars would rebuff such an approach out of hand.

Having identified what appears to be a talented scholar (or scholars) on a local campus, the unit commander may find that he can avail his unit of the services of a graduate student or two on specific projects that threaten to consume too much of the time of his permanent staff. Some match between the graduate student's principal field of interest (or a subject related to his dissertation topic) would be ideal, but such a convenient arrangement would probably turn up only rarely. Nevertheless, if all goes well, and the student or students in question find the part-time work experience for the unit rewarding, the seeds for a more permanent relationship in the future may have been sown. Establishing an academic internship would involve an agreement between the law enforcement agency and the university to permit a graduate student (or for that matter, even an advanced undergraduate) to satisfy some of his course requirements by work he is assigned within the intelligence unit. It might even be possible to extend this principle to the preparation of a study which, on the one hand, the unit needed done, and which, on the other hand, the university would accept as an input to the student's dissertation.

All such arrangements would necessitate a serious thinking through of the implications involved by the unit commander. He must, as a primary obligation, protect the integrity and security of his unit. However, if he demands clearance procedures as strenuous as those required for permanent personnel, he may discourage good young scholars from getting a taste of the law enforcement profession. He may in the process lose a promising candidate for placement

as an experienced specialist in his intelligence unit. Clearly, he must apply a rule of reason.

First of all, the unit commander will be better able to harmonize these two quite different concerns if he has what might be called "compartmentalized projects" in the planning pipeline. This simply means that discrete studies of a limited set of data that can be set aside from the other collections and from the daily routine of the office, would be assigned to an inexperienced scholar to tackle. Or such persons could be given an investigative assignment almost wholly devoted to public sources, such as library reference materials, newspaper files, etc.

One example of such a study would be a statistical analysis of telephone toll records. This would seek to determine the time and frequency with which calls are made from a known number (the analysts would not even have to know the name of the person in whose name the phone is registered) to other phones outside the city; that is, phone calls that would show up as toll calls. This could be useful where a new telephone number of interest to the intelligence unit has been discovered. The telephone number analysis might be an initial effort from which leads could be developed in other cities. Numbers frequently used in adjacent suburbs would be of greatest interest, and could lead to a request for surveillance by the agency in whose jurisdiction the new telephone is located.

In such cases, only a minimum background investigation of the student would be necessary and the risk of compromise of official materials (if any) would be measurable. Where such limited studies cannot be isolated from the normal working routine of the unit, the commander must, if he is to protect his unit, undertake a far more extensive background check, even for such a temporary employee. In the long run, of course, if the young scholar is tempted to enter intelligence work, the background investigation will have more than paid for itself. In essence, then, much will depend on the assignment that the intelligence unit commander is able to delineate for the interested, part-time scholar.

A final word is necessary on the intelligence unit/university connection. So far the discussion has centered on the simple problem of obtaining, or borrowing, intelligent minds from the campus to assist in intelligence functions, and hopefully, to attract some of these minds on



a permanent basis. There is a great deal more that a healthy relationship with a strong and civic-minded university faculty can do for the intelligence unit. It might, once confidence and respect is reciprocal, become involved in the training process of intelligence officers and analysts. Training is a particularly difficult problem for most intelligence unit commanders because few police academies offer more than a few hours of instruction on the subject. (See chapter V for full treatment of training in intelligence.)

As the specialties needed for analysis of organized criminal activities become more abstruse, unit commanders will virtually have to hand tailor their own courses—and this can often be done best by employing the resources of a university faculty, or indeed by funding course work at the university for particular members of the unit. Usually arrangements of this latter sort will require considerable give and take between the university officials and the law enforcement agency—for example, an agreement to waive prerequisite courses for police students.

One or two intelligence units around the country have moved even further than this with their university contacts. They are experimenting with brainstorming sessions in the company of trusted and respected academicians. The sessions are informal, usually consisting of the unit commander and his immediate subordinates sitting around a table discussing their knottiest intelligence or management problems. Often the guest plays the role of devil's advocate by proposing ways and means to meet the difficulty—ways and means that may be highly unorthodox by traditional law enforcement standards. The purpose of these sessions is not necessarily to have the professor lay out specific solutions to specific difficulties. It is rather to stir the thinking of law enforcement personnel, who may be becoming wedded to old habits and comfortably familiar approaches to intelligence or management difficulties—difficulties that are resistant to traditional methods.

### THE PROBLEM OF THE NONBADGED EMPLOYEE

In some law enforcement agencies, where there is a longstanding bias against employing nonsworn personnel in other than administra-

tive and purely housekeeping functions, the sudden arrival of "civilian" personnel may be resisted for some time. Resistance will not only come from badged personnel in the intelligence unit who may feel their temple has been desecrated, but also from higher command echelons suspicious of civil service employees diluting the discipline of the agency's sworn officer ranks. If there is any considerable degree of disparity between civil service compensation and benefit rates and those of the sworn officers, the hostility to mixing might become severe and even emotional.

Despite the potential frictions inherent in intermixing sworn officers with civil service analysts, the game is worth the candle—if for no other reason than that few law enforcement agencies have as yet the skills on their sworn officer rosters that would enable them to combat organized crime with modern analytic techniques. The techniques of civilian analysts can lead the organized crime intelligence unit into fields of investigation hitherto untouched by traditional police officers. Even more importantly, it can turn the focus of an intelligence unit away from exclusive attention to assisting the street investigator toward direct support of the mission of the agency head. This redirection of emphasis may take some time, but it can be accomplished if well disciplined minds stay at the task and are spared the normal interruptions of traditional enforcement duties.

Encouragement and rhetoric will not by themselves bring off a successful combining of the sworn officer and the civilian analyst in a single shop. The supervisor must assist in the process to insure that the marriage is more of a happy one and a less of a shotgun affair. It will have to be his leadership genius that puts together teams of analysts and investigators as suggested in chapter III. This will be a direct confrontation technique that can succeed only if the analysts rapidly prove their mettle. There are other devices he can use to ease the introduction of civilians into the midst of a professional law enforcement body. He could, for example, insist that the newcomer be administered his or her civil service oath in the assembled presence of all future colleagues—as a way of emphasizing that even civilians must be sworn.

But in the longer run he must work to overcome institutional problems that cannot be

ameliorated by ceremonies. If there is apprehension among the officers that civilian "whiz-kids" constitute a threat to established members of the badged force because of the educational advantages, then he must seek by every means possible to upgrade the educational requirements and levels of his sworn personnel. If he merely gets agreement for raising entrance requirements for sworn officers to the college degree level, say, he will continue to encounter resentment from those sworn officers currently in his shop who did not enter the service with a degree. So he must work to make it possible that officers already on board (and who wish to do so) be given free time for educational opportunities. There are Federal moneys available for systematic upgrading of such personnel. If he neglects this phase of his personnel program, he may simply be transferring the resentment of his on-board sworn personnel from the civilian analysts to the incoming highly credentialed rookie patrolmen. Finally, he must deal directly and aggressively with any present or prospective imbalance between compensation levels of sworn officers and civil service analysts. He must become an advocate for the promotion of deserving officers who are doing work parallel to that of more highly paid civil servants—or vice versa. Once again, and particularly in light of the peculiar differences between civil service and police officer ratings and salaries, this will not be an easy problem to solve. But whether ultimately he succeeds or not in bringing about some measure of equity is less important than that he demonstrate to all troops that he is trying.

### **THE SPECIAL NATURE OF STAFFING THE INTELLIGENCE UNIT**

The message should be coming through clearly that the intelligence unit command is the officer more responsible than any other for the successful amalgamation of the work of different types of subordinates work. He may or may not get help from the personnel bureau on this potentially thorny problem, but in any case, he will have to acquaint himself with the regulations of the local civil service commission if he is to operate effectively. It may be that in certain jurisdictions more frictions will surface over differing levels of benefits and job security than over inequities in compensation. These seem-

ingly intractable problems may not be as worrisome as they would appear at first glance, as long as all hands understand the differences in detail and are not permitted to harbor resentments over imagined inequalities.

Over the long run, the intelligence unit commander will probably find that the most sensitive point from a managerial perspective is his freedom to terminate the employment of unsatisfactory civilian members of the team. In some localities civil service regulations operate to provide virtually perpetual job protection, and it is in these jurisdictions where the most elaborate selection procedures will be necessary. The commander will rarely have the luxury of disposing of the services of an analyst "who has simply not worked out well" by transferring him or her to another element of the agency. There may be no civilian openings or even slots in other parts of the agency. He must either make a special training effort to increase the specialized skills of on-board sworn personnel or become a proponent of autonomous status for his agency or department, separated from the civil service system with full hiring and firing powers vested in the agency head. Such systems are ideal for law enforcement agencies which are critically vulnerable to the corrupting practices of organized crime, but they may be far off in the legislative future of some jurisdictions.

If the agency is fortunate enough to be moved into such a status by local legislative or executive authority, additional responsibilities fall upon the intelligence unit commander, however. He will have to exercise great restraint in recommending the removal of any of his civilian personnel. Should he move precipitately without an iron clad case for incompetence or malfeasance against a civilian employee, he may risk involving the agency in a civil suit. This may itself be worth the gamble if the employee is of little or no use and cannot be readily transferred. But under circumstances where the agency has recently been switched to an autonomous status within the jurisdiction, almost certainly after stiff resistance from political supporters of the civil service system, a new hue and cry will surely be stirred up. At the worst, things will be legislated back to the status quo ante—and, of course, the chances for getting another crack at autonomy will have been forfeited for some time. This worst-case situation is mentioned here only

as a reminder of the importance of being right about acquiring new civilian analysts the first time; that is, at the point of hiring, not of firing.

### **Career Considerations for Intelligence Personnel**

The intelligence unit commander soon recognizes that the personnel management problems he encounters are likely to be quite different from those of other elements in the law enforcement agency. Mention has already been made of the special situations that can be created in those jurisdictions where there is a mix of sworn and civilian personnel in the same shop. But there are more pervasive career peculiarities his subordinates will have to face that spring from the nature of the work itself and the premium placed on continuity in the intelligence profession.

First of all is the circumstance that, by and large, unlike most law enforcement personnel, intelligence professionals rarely enjoy concrete triumphs in the conduct of their duties. A vice squad officer may anticipate personally arresting noxious individuals and subsequently testifying in the proceedings which may remove them temporarily from society. Not so for the intelligence professional. A patrolman may be quick-thinking and an evenhanded approach to a street brawl satisfy himself that he has headed off a dangerous conflagration; he may be told as much by his precinct captain. Not so for the intelligence professional. A district attorney may savor his name in newspaper headlines the day after the major criminal figure he has prosecuted is found guilty of conspiracy charges. Not so for the intelligence professional. Yet, in the first and last of the examples above, the intelligence professional may have contributed, if only indirectly, the essential input to the vice squad's tactical plan or to the prosecutor's brief.

The point is, obviously, that the relationship between the painstaking work of the investigator or analyst and the ultimate unraveling of an organized criminal network or the indictment of a gang leader is seldom evident. Intelligence activity, in other words, may rarely have a recognizable outcome that is personally satisfying and rewarding to the professional. Instead, small pieces of information are pieced together to make a portion of a larger picture. Other officers, other law enforcement agencies, may contribute

other portions of the picture until there is enough for a warrant, an arrest, an indictment. The arrests and indictments are almost always made by somebody else, usually at a time and place unknown to the intelligence professional. Intelligence is often, in short, an anonymous business, and it certainly is a business where success cannot be measured statistically or by headlines, or by the awarding of medals of valor. Three months spent on a study of racketeering in the wholesale laundry business has little glamor potential compared to the highly expert and highly publicized detective work which leads to the apprehension of an axe murderer.

With this gap between the pace of intelligence activity and actual apprehension of criminal offenders in mind, it is up to the unit commander to devise other ways of satisfying the psychic needs of his subordinates. One practical and obvious approach is to keep himself thoroughly informed about the uses to which the intelligence produced in his shop is put. This may mean no more than reporting back to the analyst that the study he produced was taken home by the chief to read. Or it may be that in talking with a junior attorney in the prosecutor's office, he learned that a decision had been made to build a case against crime figure X or criminal activity Y, based on his investigator's efforts. He cannot assume that his people will naturally know these things because he does. If he assumes this, he will only demonstrate that he doesn't know very much about the vast differences in human personality. So, he must be, by himself, a sort of feedback loop—articulating as best he can the connection between a piece of analysis, an investigation of some months past, or a study and the consequential event which takes place somewhere else far removed from the intelligence unit. He must go further; he must make sure that his superiors and fellow officers elsewhere in the agency understand this connection, and that they appreciate the process involved.

Finally, the unit commander may discover that the experienced personnel under his command are so highly specialized that their advancement in the agency may be jeopardized. In many agencies they can be caught between two conflicting bureaucratic imperatives: (1) to advance significantly in the agency an officer must have a variety of career experiences, such as

patrol, traffic, narcotics, planning, etc.; and (2) intelligence work is so specialized that few officers do it well, and those that do had best be kept where they are, because experience counts, etc. For the civilian analyst, of course, movement from one division to another in a large agency may be an impossibility altogether. Some commanders, when they recognize these seemingly intractable facts of bureaucratic life, tend to accept them philosophically and tell themselves, "Well, all intelligence people are queer ducks anyway; they probably wouldn't give up what they are doing if they could all be commissioners." This is too fatalistic an approach.

An intelligence unit commander should have an aggressive personnel policy even if it must operate under different conditions from the rest of the agency. He should, despite the cost to his own unit, encourage the best of his officers to make a run for glory; he should press hard for an occasional assignment *out* of intelligence for his best people; if an officer is once in awhile moved onwards and upwards, he will become a missionary for good intelligence support wher-

ever he goes in the agency. Although the skills depart, the gain may be important. But to those who remain, probably longer than comparably bright officers in corresponding divisions elsewhere in the agency, he also has an obligation.

There are two basic things the unit commander can and must do for such subordinates. First of all, he must fight hard for high ranks or positions in his shop. Here the case must rest on the wits of the men and women involved. It cannot rest, as noted before, on arrest statistics or even the numbers of organized crime leaders apprehended in the jurisdiction. Months may go by without a score. So, it has to rest on the realities; that is, that the officers and analysts involved are an exceptionally talented group and could probably be doing much better for themselves elsewhere in the agency or in other professions. To use this argument with any effective impact on his superiors, of course, he must be confident that his selection policies have indeed produced an exceptional team. Second, he must bend every effort to insure that within the intelligence unit, the career of an officer or a

FIGURE 12.—Criteria for selection of intelligence unit staff

<i>Essential</i>	<i>Highly desirable</i>	<i>Desirable</i>
1. Integrity— Honesty Personal candor Realistic about self	1. Flexibility— Nondogmatic Broad range of interests Openminded	1. Perseverance— Not easily discouraged or frustrated
2. High intellectual capacity— Alertness Inquisitive mind Imaginative	2. Special motivation— Draws satisfaction from problem solving Particular desire to be intelligence officer	2. Planning skill— Good manager of time
3. Analytical aptitude— Thinks logically Capacity to synthesize Capacity to hypothesize	3. Articulate— Writes well and concisely Speaks well and concisely	3. Self-discipline— The "self-starter personality"
4. Meticulousness— Thorough Pays attention to detail Precise in handling data	4. Resourcefulness— The "digger" type "Where there's a will, there's a way"	4. Cooperativeness— Capacity to work well with others
		5. Fast learner— Quick response capability

*Essential characteristics.* Should be considered just that; the candidate who appears weak on any one of the characteristics should probably not be appointed.

*Highly Desirable-Desirable characteristics.* Should be considered as complementing the other qualities, and thus not all of them are necessary for successful careers in intelligence.

Trade-offs are possible within each "bundle" of Highly Desirable and Desirable characteristics, and between the two "bundles."

A less well developed capacity in one category can be made up for by great strength in one or more of the others. Forceful and skillful management can offset some weakness in the secondary characteristics. Subsequent training can be applied in some cases to turn a weakness into a strength.

civilian analyst is as varied as possible. Not only does this help to still the overly restless spirit, but also it prevents hardening of the intelligence arteries. Where possible, analysts and investigators should occasionally exchange roles. An officer who has done several long investigations on gambling can be switched to a narcotics problem. The desk-bound civilian analyst who has mapped a large conspiracy for months or

even years can be sent to participate in the training of middle level officers from all elements of the agency. A sergeant who has worked long and hard perhaps can be given a year off to complete university work for his degree. Depending on the size of the unit, the opportunities for flexible deployment of intelligence professionals are there. It is up to the commander how fully he exploits those opportunities.

# Chapter V

## TRAINING AND INTELLIGENCE

*Appreciation of value of intelligence to law enforcement agency requires three-pronged training effort:*

- *General patrol force.*
- *Personnel assigned intelligence unit.*
- *Command level.*

*For patrol forces, general intelligence training program should focus on:*

- *Dispelling mystery of intelligence.*
- *Soliciting cooperation of non-intelligence officers.*
- *Accuracy and conciseness in field reporting.*

*For intelligence officers, training program should focus on:*

- *Current and potential activities of organized criminals, and role of intelligence in fighting them.*
- *Official corruption as an essential element of success of organized crime.*
- *Analytic technique as basic tool of intelligence unit.*
- *Need for effective report writing capability.*

*Command level training should focus on theme: what intelligence can do for command level.*

- *Training for this level most demanding of all—problem agency head being willing to give time to subject.*
- *Focus on relations between intelligence inputs and agency decision/strategy making; both a substantive and a management problem.*

### INTRODUCTION

If intelligence means anything to most people, it is a mysterious mixture of sleuthing, intuition, dangerous looking chemical experiments, and anonymous agents appearing (and disappearing) magically in the right places at the right times. Television images have created impressions that are both misleading and, worse, miss the point completely. The real point, of course, is that

intelligence is as much a product as a technique. To obtain the product "intelligence," some or all of the dramatic collection techniques so favored by TV script writers may be necessary at one occasion or another. But concentration on these techniques obscures the end result, which should be a careful, measured judgment about some situation, some person, or some allegation. If no judgment evolves, there is no point whatsoever to the antics of video's star performers.

So it is in real life law enforcement. Collection techniques are familiar to most veterans of police departments and prosecutors' offices. However, fascination with these techniques has tended historically to deflect attention from efforts to improve the ultimate product. A good training program for intelligence against organized crime should begin with a recognition of this longstanding myopia. Accepting the fact that the end product has been neglected raises in turn a fundamental premise about the state of intelligence in many law enforcement agencies: What is needed most is a general reorientation, from the top down, on the character and usefulness of intelligence—not simply another training course.

Although agency heads and their subordinates every day come to rational judgments on the basis of information presented to them, few understand they are thereby fashioning the intelligence end product themselves. Not understanding this, they are unlikely to insist to their subordinates that the process could be improved or their own use of intelligence extended. Drawing conclusions based on analysis of assembled information is a simple description of how a policymaker—or decisionmaker—uses intelligence, and at the same time is an essential part of the process. He is the consumer. Training has concerned itself very little with the consumer and therein lies the need for a revamping of existing training assumptions and directions.

### THE THREE LEVELS OF TRAINING

General reorientation of a law enforcement agency to an appreciation of intelligence requires a three-pronged training effort, that is directed toward: (1) the general patrol force; (2) the personnel assigned to intelligence responsibilities; and (3) the command level.

The largest (general patrol force) category of training programs should focus on a better understanding of what the intelligence process is and where the inputs of non-intelligence officers can be inserted into the process. For the second category, that is, those training to go into intelligence either as investigators, analysts, or information control personnel, very practical instruction is necessary—how to collect, evaluate, collate, analyze, etc. But for the command level, the main objective should be to demon-

strate what intelligence can do for management and what assets the intelligence unit should have at its disposal to do the necessary job of strategic support for the decisionmakers. All categories, of course, should receive a good dose of instruction on the nature of organized crime.

But each category presents a different problem in development of program and course presentation. The first two of these tiers may be dealt with fairly directly; that is to say training programs for them—although perhaps quite different in content from what has traditionally been offered on the subject—can be fitted into existing curriculums and facilities. The command level category presents an entirely different kind of problem. There are few recognized ways that the command levels of law enforcement agencies can be trained. In fact, the general assumption of most agencies is that the command level will dictate the tone and general philosophy of the training programs offered, and that it does so out of a large fund of wisdom and experience acquired through long service. Far from needing training for itself, the assumption goes, the command level designs training requirements for subordinate levels.

But if training programs for subordinate levels of intelligence against organized crime are to have a meaningful impact; if they are to be designed so as to be supportive of strategic thinking as well as of operations, then the role of intelligence must be more clearly understood than it now is at top command positions. The practical problem remains: By what mechanism can training at this level be provided? There is no satisfactory answer that can apply to all sections of the country or to all local jurisdictions. It might be possible sometime in the near future for regional entities of, for example, a professional police association, to sponsor annual short programs, possibly with some Federal funding, for command level personnel of the municipalities and counties in the region. In some States such a training program might be given annually by the State police academy, or its equivalent. Finally, if a local jurisdiction has a strong training program on organized crime, it might experiment on a one shot basis with a 2- or 3-day course tailored to command level students, piggybacked on its regular program for somewhat lower level law enforcement officers.

This chapter will include suggestions as to what might go into a command level training program for intelligence on organized crime in full recognition that such a course or program may be a practical impossibility for many agency heads and their staffs. But it is necessary to include such material, first because a few may be able to exploit it, and second to demonstrate that three distinct clienteles for training can be identified and each must be handled differently.

How specific training cycles are broken down to accomplish the aforementioned objectives, or how many hours of instruction are required for each student clientele group cannot be defined for all jurisdictions, but some suggestions as to relative weightings of the various components of the different courses are suggested in figure 13, below.

### TRAINING FOR THE NONINTELLIGENCE OFFICER

The objective of any course (or portion of a course) designed for the patrol force or other non-intelligence-assigned peace officers should be to prepare them to understand and contribute to the intelligence process. Most police academies now allow for an hour or so on the subject of organized crime; only a few make more than passing reference to intelligence. Indeed, those that do touch on this subject usually only con-

centrate on field report writing as an input to the intelligence process. It is little wonder that many law enforcement officers have no feeling that intelligence can or should concern them in any direct way. If their agency has an intelligence unit, it is usually wrapped in such a cloak of secrecy that they are discouraged from finding out more about the subject. The image of the intelligence unit quite often is one of an inaccessible fortress of filing cases inhabited by odd-ball officers and civilians mysteriously pushing paper instead of making arrests.

### Intelligence Is Not a Mystery!

Clearly, then, any general training program for law enforcement officers must have as one of its first goals the clearing away of the mysteries surrounding the concept of intelligence. There is, of course, very little that is secret about the process itself—for the most part only the contents of the filing cases are sensitive. Once this is understood by law enforcement officers, the distance between the intelligence unit and the rest of the agency personnel should begin to shorten.

Perhaps the best way to achieve this is to have an officer of the intelligence unit address the rookie class, or whatever training or retraining program is underway, in exactly these terms. He should emphasize that the methods of collection, investigation, analysis, etc., employed in his unit are not at all the mysterious rituals some have imagined them to be. In fact, he should, where possible, offer the class a case study of how intelligence has contributed to the unraveling of an important criminal conspiracy. A local case comparable to the automobile supply store caper described in chapter II would be appropriate. This kind of presentation should emphasize the laborious aspects of making matches between what had been thought to be unconnected people, or places, or businesses, etc. The actual methodology should be described so that the students can judge for themselves how simple but painstaking much of intelligence work is.

Once the aura of mystery is removed from the intelligence process, the training course should deal with ways to solicit the cooperation of non-intelligence officers, particularly those in patrol assignments. A number of approaches are possible here, but arousing the awareness of the aver-

FIGURE 13.—Suggested weighting of subjects in intelligence training courses

	<i>Relative weight</i>
<i>Training for the non-intelligence officer:</i>	
What intelligence is .....	2
The intelligence process	
How the agency head uses intelligence	
Techniques of observation .....	1
Field reporting .....	1
Introduction to organized crime .....	1
Other topics .....	X
<i>Training for the intelligence officer:</i>	
Intelligence theory .....	1
Organized crime .....	4
The intelligence process .....	4
Report writing (field and analytic) .....	1
Technical training .....	2
Other topics .....	X
<i>Training for the command level:</i>	
Intelligence, management, and strategy .....	4
The intelligence report .....	1
Understanding methodology and process .....	2
Organized crime .....	3
Hardware .....	1
Other topics .....	X



age law enforcement officer should be the main emphasis. He should be encouraged to think of the precinct or beat he serves as a source of reportable information. To direct his thinking this way, some assistance can be offered. He must be urged to view the area he covers less as a geographic whole and more as a composite of human interactions, each of which has a specific meaning and purpose. As one who daily visits this area he witnesses some, at least, of these interactions. He should study them to determine, if possible, their significance.

For example, if an officer is assigned to an area in a city where the commercial activity centers around the garment trade (an activity about which we assume he knows little), his first reaction would probably be that he has a hell of a traffic problem on his hands. He will encounter great numbers of trucks hurriedly unloading and loading often at several doors on a single block. The streets may be full of handcarts holding racks of clothing and knots of men on the sidewalks in deep discussions impeding pedestrian movement. Confusion is the principal impression. If he makes an effort to understand the flux all about him, he will soon discover that suppliers' trucks do arrive and unload according to rather rough daily timetables, that local manufacturers save transportation costs by moving new clothes to nearby retail stores by handcart, that larger clothing firms sell off unpurchased stock to discount houses, also using handcarts, and that clothing is bought, sold, transferred, etc., often on the basis of oral agreements made on the street between neighboring businessmen or in favorite coffee houses or bars.

Other things may then come clear to him. He may note that certain trucks rarely unload on the open street, but seek out alleys for the discharge of their deliveries, even if they cannot get as close to the store they are serving. At the larger establishments he may observe that certain truckers do not wait their turn to unload their goods, but automatically go to the head of the lineup of trucks which have arrived earlier.

At this point, he should be beginning to ask himself why these things are so. He will, in other words, have learned how patterns of activity define the nature of his neighborhood, and

he will have observed breaks in the pattern that suggest human interactions are in play which may have considerable importance to him as a police officer—and, possibly to the intelligence unit. Once he begins to see his precinct in this way, the peace officer will automatically store in his mind, patterns of activity and the rhythm of people's movements. He will have begun to understand the dynamics of his beat, his perceptions will sharpen and in time he may come to recognize the meaning of unusual activities and changes in normal patterns. At that point he will have grasped the essentials of being a good observer. Next he will have to school himself to become a good reporter of his observations.

### Field Reporting by the Peace Officer

Good reporting techniques not only have to be taught; they have to be inspired. Persuading a busy police officer to pass on information for which there is no immediate operational necessity is not easy. In fact, the impetus for doing so probably will have to come from within the individual officer. No amount of exhortation will drag it from him, unless he, personally, is interested in what he sees about him and feels it may have value to others. It is for this reason that an effort must be made to induce the police officer to think like an observer. This approach may tickle his imagination; simply appealing to him to record the unusual that he sees on his beat will not.

But instruction on good report writing can and should be presented as a prime objective of the general law enforcement officers' training. Conciseness, thoroughness, and accuracy are the principal qualities to get across. Style and grammatical perfection are less important at this level than pointedness. The student should be cautioned to read his own practice report from the point of view of the recipient. If he learns to do this, he will avoid missing the target. For example, let us say that the instructor constructs a simple scenario about which the students are obliged to write a one-paragraph report.

The scenario can be put together by pictures clipped out of magazines plus a few words added to each picture. The scene is the beat which all the students are asked to imagine as their own. They are further

asked to imagine that they are familiar with all the low-level underworld characters and the places (a tavern) that make up the scenario. The instructor pins a picture of Joe Jones on a board; the class is told that Jones is well known in the neighborhood of the Tiny Tavern; his principal claim to fame is that his girlfriend, Louella Z, is an intimate associate of Doris X, the mistress of an important mobster, Billy Y. All these people are pictured on the instructor's board, as in the Tiny Tavern. The imaginary event which takes place is that the patrolman observes Jones entering the Tiny Tavern with Doris and after a half-hour stay, departing with her.

The first point which the instructor will want to get across by use of this exercise is that the report written on the scenario be as useful to the recipient as possible. In practical terms this means it should be *complete*, down to the last detail. In other words, the reporter must not assume that simply because *he* knows all about the local characters—who enjoy a certain notoriety on his beat—that anybody else up the line will recognize the significance of the relationships between them.

The student should also learn that his reports will not receive much attention unless they come down hard and early on his main point. He cannot hope to get his message through if it is buried in a mass of detail or only partially relevant material. So he must be trained to present the main thrust of what he has to say at the beginning of a report and let the supporting factual material follow. His report on Joe Jones, for example, should probably run something like this:

“At 4 p.m. on June 6, I observed at 1200 Central Blvd., Joe Jones, a local hoodlum, enter the Tiny Tavern with Doris X who is the mistress of Billy Y, West-Side mobster. Doris X is a close friend of Jones' girlfriend, Louella Z, but has not been observed before alone in Jones' company. The two departed for unknown destination after a half hour.”

If the students omit the relationships in writing their practice reports, they will have provided headquarters and the intelligence unit with what may be no more than indifferent gossip about street characters. If the students fail to men-

tion Billy Y (although he was not directly involved in the scenario), the whole episode will have little meaning for headquarters. Direct, pointed reporting technique *can* be learned; but drilling is necessary.

### Introduction to Organized Crime for the General Officer

Of course, it does little good to encourage the general police officer to act as an extended collector for the intelligence unit if he does not have an effective understanding of organized crime. Several course hours should be devoted to this subject, if only to depict the variety and complexity of the criminal underworld and suggest areas for his observations. He should know, for example, that certain businesses and service industries are particularly susceptible to organized crime penetration; he should know what activities of organized crime have recently been recorded in other cities.<sup>1</sup> He should understand that he has an obligation to familiarize himself with the known criminal figures in his precinct and to learn as much about them as his precinct commander can tell him. If he becomes an active reporter, he should know where and how he will have ready access to the intelligence unit.

### Understanding the Role of the Agency Head

Finally, some time in the general patrol officer's course should be committed to the command obligations of the agency's leadership. While this subject is not strictly intelligence, it is directly related to the intelligence function. A good lecture devoted to “a day in the life of the agency head” should be part of every general training program. It should emphasize the policymaking function of the highest level of command and describe the interconnectedness of policymaking, planning, and intelligence support for these two responsibilities. Not only is such a presentation useful and desirable for its own sake, but it also helps to clarify the strategic role intelligence plays in a law enforcement agency—a concept not fully understood by many fledgling officers.

<sup>1</sup> The pamphlet, “Police Guide on Organized Crime,” published by the U.S. Department of Justice, contains a list of 20 indicators suggestive of the presence of organized crime.

## TRAINING OF INTELLIGENCE OFFICERS

For those personnel designated as organized crime specialists in such fields as narcotics, vice, etc., quite specific training is called for. (See figure 14, page 91, "Two-Week Training Course for Intelligence Analyst/Investigator.") Where the general officers training program need extend only to a broad understanding of the nature of the intelligence process and some exercises in report writing, courses for organized crime specialists should emphasize professional development heavily, particularly methodology. The intelligence process should, in fact, be the heart of the training. The reasons for such an emphasis are simple. The intelligence process, which consists of a continuous series of inter-related intellectual activities, is not familiar to most people. It requires a mental discipline—a habit of mind and energy which, although not unique to the law enforcement profession, must in great part be learned rather than developed out of job experience.

Manual skills requiring practice to develop dexterity can be learned fairly rapidly, and once learned, remain more or less constant at a level determined by physical factors and the quality of the training involved. Thinking habits or mental processes develop more slowly. Or, it may be more accurate to say that the introduction of new ways to use mental processes is resisted by old, familiar comfortable habits of thought. Thus, the suggestion that the end product of the intelligence process should be an analytic judgment of some sort or another may be perfectly well understood when the point is made, for example, in training lecture. But a subsequent classroom exercise in which the students are asked to produce end products may turn up nothing better than simple summaries of the exercise. This is not student sabotage at work; it is, rather, a consequence of old habits overcoming the effort of a novel idea to establish itself as an accepted part of the mental process.

A bright law enforcement officer can master the fine technical (and even dexterous) detail of a new long-range camera in a few days. It may take the same officer many months to adjust his thinking habits and develop mental disciplines to which he has not been accustomed. Thus the first guideline for the intelligence officers' course

should be one which recognizes the disparity in learning speeds. Much more course time should be spent on the development of a deep understanding of the intelligence process—and the personal adjustment necessary to its demanding discipline—than to the more traditional subject matter, such as new hardware, surveillance technique, and the like. This is not to say that one is more or less important than the other—only that the former takes longer to be assimilated—even for the quickest mind.

### Intelligence Theory and Organized Crime

An introduction to the intelligence officers' course should begin with a few—probably no more than 5 or 6—hours devoted to a discussion of intelligence theory as it relates to organized crime. These will not be easy concepts to get across. Considerable attention should be given to the role of intelligence in the battle against organized crime. The students should see it as defining the scope of organized criminal activity with increasing precision and developing points of focus for intensive investigation leading to the ultimate decision that an attempt should be made to build a case. This phase of the introduction would of necessity involve some exploration of both indications intelligence (or warning or danger signals) and strategic intelligence (report on existing or potential pattern of activities). Also required would be a discussion of the different uses made of indications, tactical, strategic, and evidential intelligence. (See chapter II, page 11, for a discussion of the four types of intelligence.)

The distinction between the pure intelligence function and operations would be treated as an essential means of preserving objectivity. This should lead directly to a discussion of intelligence as a staff function of the command level and its use by those making strategy or doing the planning for the law enforcement agency. A critical point that should emerge from this discussion is that intelligence supports the strategists of the agency. It does not and should not arrogate to itself the planning or decision function of the command level. On the other hand, it should be thoroughly responsive to the needs of the command level for guidance on contingency questions. In practice this means the intelligence officer should be prepared to answer

the question: "What would be the consequences, if we did this?" Or, "If we adopted such and such a strategy against a particular criminal organization?" (Chapters II and III contain considerable material on contingency intelligence support.)

The reason for enunciating this doctrinal point and laying such stress on it must be clear to the instructor. He should be largely concerned at this point in the training course that the intelligence unit come to be understood as filling a special, even unique place in the law enforcement agency—and that if its members do not understand the unique relationship the unit has to the command level, they will be unable to serve the command level objectively and professionally. For once the intelligence unit presumes to propose or dictate strategic moves, it will lose its independence. It will be sandbagged and second-guessed by the larger components of the agency; it will no longer be the supporting staff arm of the agency head, but a claimant for power, battling for its view against unequal odds. Its effectiveness will be destroyed.

### **The Target: Organized Crime**

The next portion of the intelligence officers' training should be a fairly generous one devoted to the target itself—organized crime. If it is to have impact, it will have to concentrate on an area that is not normally the substance of such courses—organized crime involvement in legitimate business and its interest in penetrating government.

Depending on the location of the training course, the instructor will have more or less of a problem overcoming the it-can't-happen-here syndrome. He may, of course, be dealing with examples that are far removed from the jurisdiction in which his students operate. But if his presentation is well prepared and carefully supported by facts, records of court transcripts, etc., he should have little trouble. The best answer to the it-can't-happen-here sceptic, of course, is to ask the students from their general knowledge of the metropolitan area they serve, to compose a scenario descriptive of how it could happen here. This kind of group exercise can be an extremely useful tool—not only in testing the imaginativeness of the students, but in blunting the scepticism of the doubters in the group

by exposing them to the wider knowledge and perceptiveness of their fellows.

Probably the best way to conduct such a session is to permit a picture to grow naturally from inputs by individual students. To get things started it may be necessary for the instructor to prearrange with a student, who is known to have some knowledge of organized criminal activity in the area, to be the kick-off man. The instructor could start a list of three columns on a blackboard: "current manifestations and indicators," "potential weak spots," and "probable type of future criminal activity." Thus, the kick-off man might remark that he was personally aware of a gambling ring covering at least two distinct sectors of the city. This would be entered in the first column as would a followup remark by another student that he had been told by one of his informants that bootlegged cigarettes from out of State were now to be found in dispensers throughout the city. Persistent provocative questioning by the instructor might elicit the comment from yet another student that once the new harness track was finished in the neighboring county, a new flood of criminal and semi-criminal interests would probably develop. The track management might be suggested for listing under "potential weak spots." From that point the instructor could simply weave students' suggestions back and forth under the appropriate columns until something of a composite hypothetical picture emerged.

### **Official Corruption**

Emphasis on corruption techniques of organized crime against government officials is at this stage of training only the first introduction of a theme that should be woven throughout the program. That theme is, clearly, the susceptibility of any law enforcement agency to penetration by organized crime. The whole question is enormously important for future careerists in intelligence work and is probably the most sensitive single part of any training curriculum. Precisely how it is handled will depend on local conditions, the integrity record of local agencies and a number of other factors. It is a subject which should be considered at great length, not only by the course planner, but by the highest command levels of the agency involved in sponsoring the training. There may be merit in

importing an outside speaker, preferably one who is free to discuss the difficulties experienced along this line by a particular police department or prosecutor's office. Dramatization of the impact of corruption on a city might be one approach. John Gardiner's "The Politics of Corruption" is a good source for such a presentation.<sup>2</sup> A discussion led by the head of the internal affairs squad—or the agency head itself—might be another.

The question of how to cover integrity questions within training programs is one beyond the scope of this manual. Most law enforcement agencies have a specific policy for treating this subject in recruit training programs. Usually this takes the form of the familiar "free cup of coffee speech." What is under discussion here, however, is a far more sophisticated approach, in which a real effort should be made to detail the pernicious techniques of organized criminal figures to entrap law enforcement officers, or place them unwittingly in positions from which illegal obligations can be extracted later. An audience of intelligence officers would be an excellent forum for a discussion—perhaps conducted by an attorney—of systematized approaches to anticorruption measures.

### Organized Crime Beyond the "Mafia"

The second principal area essential to the organized crime portion of the intelligence officers course is that pertaining more specifically to the target group. A fundamental objective should be to stretch the students' thinking beyond the traditional ethnic image of organized crime. In many jurisdictions, and even at high levels in these jurisdictions, there exists the comforting notion that organized crime is not much of a problem because no major "family" member is involved in criminal activity locally. This attitude ignores the whole range of criminal conspiracies that spring from different ethnic groups, or are not ethnically homogeneous.

Perhaps the best perspective for the instructor organizing materials on this subject is to think of the metropolitan area from which the trainees are drawn as a composite of social opportunities for crime. Crime clearly exists in the jurisdiction—to what extent is it tied into networks with

direction and discipline imposed by command levels? To what extent have old-fashioned street gangs grown up to be the nuclei of self-perpetuating criminal conspiracies? Do several loosely held together bands of criminals cooperate with one another for specific ventures or in particular districts of the metropolitan area? If the answer to any of these questions is "yes," there may be a severe organized crime problem in the city, or the beginnings of one, without any participation or interest by a "family" member whatsoever.

Similarly, the intelligence officers must be encouraged to think beyond the traditional types of criminal activity hitherto long associated with organized crime, such as gambling, narcotics, fencing, loan sharking, and the like. White-collar crime, securities manipulation, credit card fraud, new forms of extortion, sophisticated rackets involving the physical security industry—these are the fields where organized crime may be moving next. They are largely ignored by training courses today, because they are not yet understood as real threats in many jurisdictions.<sup>3</sup>

Clearly, no one intelligence officer's course can provide a thorough training for coping with these potential danger spots in the local jurisdiction. What it can and should do, however, is provide him with the tools for understanding the complexity of the city he serves and rouse him to think about the possibility that organized crime may penetrate the city's economic or political life at an unconventional point. The faculties of local universities, particularly the departments of sociology or urban affairs, may be helpful to the course planner in this regard. The overall purpose, of course, will be to remove the traditional blinders that limit the thinking of the students to the more notorious activities of organized crime as dramatized in such literature as "The Valachi Papers" and the many volumes on the "Mafia."

### Emphasis on Analytic Technique

As noted earlier, the major part of the intelligence officers' course should be devoted to the intelligence process, and in particular, analytic technique. The process must be thoroughly

<sup>2</sup> A short documentary film based on this book is available from the Westinghouse Broadcasting Corp., New York, N.Y.

<sup>3</sup> See particularly the pamphlet written by Herbert Edelhertz and published by the National Institute of Law Enforcement and Criminal Justice: "The Nature, Impact and Prosecution of White Collar Crime," May 1970.

understood, even to the point of giving the students simulated investigative reports and putting them through the individual steps—collection, collation, evaluation, analysis, reporting, dissemination, and reevaluation. This is a laborious training technique, but if it results in identifying clearly for the participants both the uniqueness of each step and the interrelatedness of all steps, it will have been worthwhile.

The most difficult single subject within the process to clarify will be analysis. Since almost all intelligence problems are one of a kind, no single set of guidelines can be offered to the students, although a few self-testing questions are applicable to all analysis; that is to say, there are questions which the analyst should ask himself about all data that comes his way that may be helpful. By asking (and answering) these questions the officer who would be an analyst does not achieve overnight mastery of the analytic process. But he will be getting closer to an understanding of what is expected of him as an analyst.

Beginning with two or three scraps of raw information, which point to the existence of criminal activity in a certain field, the analyst must learn to ask himself: "What other information would I *like* to have to better complete the picture? What other information am I likely to be able to obtain relatively rapidly and economically—this is, what information can I get that will be worth the effort? Given additional information, do I perceive a new dimension in the problem? What is the critical element in the problem? Can I match any of the materials on hand with other information in storage (files or computer) in such a way as to broaden my understanding of the whole problem? Assembling all the pieces, that is, the original two or three scraps of information, the newly collected information (if it was decided more would be desirable) and the stored matter that impinged on the other pieces of data, can I now reconstruct the problem? Is what results a clearer picture than before I started the process? Can I draw from this new overall picture a significant judgment of some kind? How confident am I of my judgment; have I indicated the degree of my confidence in my judgment statement? If the world-be analyst asks himself all these questions during his exploration of the materials he has on hand, he will begin to get a feel for the analytic

process. He should, of course, be put through these paces on a number of different kinds of problems. (An example of an analytic problem to give trainees can be found on page 88.)

### Sophisticated Analysis Problems

More sophisticated analytic techniques should be described to the class and, if possible, field exercises conducted using some of these techniques. Subjects such as the identification of real estate ownership, hidden corporate management, gathering evidence of skimming operations, etc., involve highly technical knowledge, but an introduction to these areas may stimulate the students to reach out for new techniques, or even one day to perfect analytic techniques of their own in other fields. Instructors who are responsible for this type of training should probably themselves be exposed to the U.S. Internal Revenue Service Special Agent Basic School, which contains quite intensive training in techniques of financial investigation. Some knowledge of accounting is necessary for this course. IRS regional offices occasionally make available other training programs for State and municipal investigators.

The course director who wishes to push his students to the limits of their imaginative powers may also want to acquire professional assistance from a local university faculty. Many faculties contain specialists in problem-solving theory. Such men may be located in departments of systems analysis, psychology, and even philosophy. The introduction of this discipline to an intelligence officer's course would not be for the purpose of converting the students into instant psychologists. It should rather be thought of as additional stimulation for those about to plunge into the analytic world. An imaginative academic from one of these disciplines might provide insights to the students for thinking through problems rather than having them tie themselves to set formulas for the resolution of intelligence puzzles.

Much of the mystery behind the so-called problem-solving discipline now popular on some campuses clears away when it is understood as largely a matter of hypothesis formation and testing. (See chapter II for a discussion of this technique as applied to analysis.) Whereas the academic approach usually includes a good dose of mathematical formulas, they are not necessary

for a basic understanding of the technique. The professor recruited from the local campus had best be advised that he should offer only the most rudimentary essence of his technique to the intelligence officer's class. He will have contributed significantly to stretching the imagination of the students if he can persuade them that systematized ways of breaking down problems which contain unknown factors are possible and profitable.

An exceedingly simple example might be a good point for introducing intelligence officers to the analytic process and problem solving in general. Any expansion or elaboration of this simplest concept will be possible only when each student thoroughly grasps the fundamental idea and is confident enough to extend himself a little further. The simple example is the Fujiyama concept. This concerns the Japanese father and his son traveling by train from Tokyo to Osaka. Out of the right-hand window the famous snow-capped Mount Fujiyama suddenly appears, its top covered as usual with heavy clouds. The father says to the boy, "You can see most of Mount Fujiyama, son, but not the top. Tell me what you think the top looks like." The son, a studious little boy, draws a picture of the mountain with its cloud cover on a small pad of paper. He then draws the same picture of the mountain, but removes the clouds. Then, he extends the sides at the same pitch until they intersect. He gives this picture to his father as his answer. "Very good deductive reasoning, son," says his father, "but very bad answer. If you read more geography and fewer comic books, you would know this whole part of our country was once volcanic. Almost all the mountains around here are old craters and their tops are flattened out—they are not pointed as you have shown."

The class should be able quite quickly to grasp the moral of this story. Deductive reasoning alone cannot solve all problems when only some of the facts are known. In this case, total reliance on deductive reasoning lead the boy astray. A moment's research into any reference work would have offered the boy a better chance to be right. He made an intelligent hypothesis, but since things are not always what they seem to be, his assumption was badly mistaken. Without research, he could never have made an accurate hypothesis.

One final word on analysis is necessary. Noth-

ing can take the place of a young, dynamic organized crime intelligence unit analyst coming to the classroom equipped with the basic raw materials from which he has put together a major study or investigation. If he can spread these materials among the students and then describe, step by step, how he conducted the analysis and fashioned the final judgments which emerged from this process, he will do more to shed light on the analytic mysteries than any other participant in the program.

### **Report Preparation**

Report writing should occupy an important bloc of time in any intelligence officer's course. Report writing in this context has two meanings: investigative reports prepared in the field and submitted to headquarters, and the reports which are the end products of the intelligence process. These latter reports are those which are the culmination of sorting through raw information, collating those related pieces, analyzing the collection selected for study, and drawing some useful judgments from the picture so presented.

### **Field Reports**

The field report will probably be familiar to most of the students in an intelligence officers' training course. In fact, not much more instruction will be needed at this point in their careers than to reemphasize the necessity for clearly stating the who's, where's, when's, with what's, and how's. The fundamentals, such as short sentences, clear antecedents and the like, should have been mastered by most many years before. If not, this is hardly the course for dealing with them. On the other hand, a truly professional presentation on effective expository writing can often dramatize the need for correcting bad, old habits in an hour or two. One additional point which should be stressed at every opportunity is the need for including evaluation in field reports. Here the instructor must balance on the thin line between the general instruction "to tell only the facts" and the need at headquarters for knowing what the investigator on the scene believes to be the worth of the information he has passed on.

### **The Analytic Report**

The analytic report is another matter altogether. It is quite possible that not all partici-

pants in the intelligence officers' training program should receive extensive training in this activity. It is, after all, a highly specialized art and not everyone will do it well enough to satisfy an agency head. But for those who are selected to train in analytic drafting of intelligence reports, a few basic skills need to be emphasized. (See the section in chapter III on analysis and report writing.) One of these is structuring the report so that the findings are described logically and coherently. Another is conciseness and the elimination of contentious words and extraneous detail. Finally, a considerable amount of time should be spent on how to draw meaningful conclusions. No specific procedures can be offered in this regard. Pointed conclusions, after all, are the products of mental discipline, even more than mastery of the written word. Accordingly, the students should be guided to train themselves to draw out one or two, or possibly a few more, main points that constitute the basic reasons for having assembled the materials and written the report in the first place. These main ideas or themes should be grouped in a rough order of priority and melded into a paragraph or two. Ideally, a senior officer of the agency should be asked to present his views on what he needs by way of reports from his intelligence unit, and how such reports should be shaped to suit his tastes and work style.

The distinction between a summary and a conclusion should be stressed repeatedly and exercises conducted to illustrate the latter. The simplest method to accomplish this is to present the class with a series of single paragraphs describing some aspect of organized crime operations and request the students to compose conclusions for each paragraph. Take, for example, the following paragraph on loan sharking:

"If loan sharks experience their own version of a tight money crisis, they are not above 'getting to' a professional loan officer in order to use bank funds. Recently in New England a bank loan officer, who had enjoyed a taste of high living offered him by a racketeer, returned the favor by accommodating an individual referred to him by the racketeer with a personal loan of \$3,000. The borrower immediately paid \$600 or so to the racketeer/loan shark who had steered him to the bank and retained the balance

for his own use. During the course of the loan's term, the borrower repaid the \$3,000 to the bank."

A summary of this excerpt might read: "This paragraph tells how loan sharks sometimes are able to 'buy' support from bankers when their own operations are short of ready cash." A conclusion, on the other hand, might say: "Bank officers are sometimes susceptible to favors offered by organized crime figures. Thus, the banking practices of organized crime figures, particularly loan sharks, should be monitored as closely as possible." Other conclusions could be composed which would be equally appropriate, but the point that has to be made is that a conclusion is derivative. It adds a perspective or demonstrates a relationship that was only implicit in the original text. Above all, it tells the significance of an item.

### Technical Training

It must be assumed that personnel assigned to the intelligence officers' training program will have undergone basic training in investigative techniques. Indeed most will probably have had several years in detective or other investigative activity learning their trade by doing. The intelligence officers' training program should not, obviously, occupy the time of the students with these matters, but should be used as a vehicle to demonstrate newly developed techniques in such areas as surveillance, photography, electronic eavesdropping, and the like. These demonstrations optimally would include field exercises in the use of new equipment or new techniques, as well as discussions of their applicability in certain circumstances. In other words, hardware should be related to actual or potential situations wherever possible. The training of highly technical specialists, such as electronic eavesdrop operators or accountant analysts will probably require resort to special in-service courses offered by the local police academy, or even Federal training, such as the basic agent's school operated by the Internal Revenue Service. However, at a minimum, the intelligence officers' training program has an obligation to make it clear to the students how such skills can be used to produce sound intelligence.



## Security Training

Security is a special problem for the intelligence unit and must be covered in the training course. (See chapter VI for a discussion of this problem.) The intelligence officer must be aware of why he is subjected to a much more thorough background investigation than that of his brother officers. He must understand why this is essential even though he may already have been a law enforcement officer, perhaps in the same agency, for several years.

The intelligence officer must understand the reasons for the rigid security requirements for the offices in which he is going to work and especially for the material in its files. He cannot even be completely free to talk to other officers in his own agency about some of the matters under consideration in his unit. He must understand the difference between dealing with unsubstantiated reports and allegations harmful to the subject persons, and dealing with official arrest records and "rap sheets." This is the obvious point in the course for a guest lecture by an attorney on privacy rights and intelligence.<sup>4</sup> Security should also be presented to the intelligence officers as a means for guarding an area which may be a target of organized crime penetration efforts. Effective security of the unit can only be achieved if the "why" of security is understood.

The intelligence officer must also be given special training in security when he is operating in the field. He will often be operating in difficult circumstances and must come to understand why his communications back to his unit must be guarded so as not to give away his operation or his own whereabouts to the criminal.

## Other Topics

The training program so far described for intelligence officers is by no means a complete package. There are many other subjects that could quite properly and rewardingly be touched on—for example, automated data processing and analysis, streamlining the collation function, new security concepts for the intelligence unit, plans for in-service training, intelligence and trends in the law, etc. What has been discussed at some

<sup>4</sup> For further elaboration see appendix A, "Intelligence and the Law."

length in this chapter is simply a minimum base upon which other topics could be added as particular local needs demand or opportunities arise. Even as a minimum base, however, the proposed training program represents a quite sophisticated challenge for the training officer. It may in fact be somewhat beyond the capabilities of any given staff on board in police academies. Clearly, even the most progressive police academies are going to need outside help in organizing and presenting some of the proposed subject matter.

It may be desirable to contract out parts of the program or even all of it, to a university professor or research organization. Finally, in some jurisdictions it may be possible to arrange for the intelligence officers' training program to be conducted entirely outside the academy at a site selected by a contractor. This option might be preferable to any of the others, since it would tend to dramatize the newness of the techniques and approaches under study. On the other hand, the contractor would have to be chosen with great care since intelligence theory and practice is not a particularly widely known or understood discipline.

## COMMAND LEVEL TRAINING

Command level training is the most demanding obligation of all. It will necessitate severe intellectual retooling for students and instructors alike, with all the psychic hazards this implies for the latter. The training content should have a single major theme: what intelligence can do for the command level. Minor themes would usually cluster around several topics related in some way to the main theme: breakthroughs in intelligence techniques, new strategies of the organized criminal, managing the intelligence process, recent court decisions and intelligence limitations, etc.

A good starting point might be to offer a lecture or discussion by a prominent officer from a national intelligence agency. Such a speaker would be asked to emphasize how he uses the intelligence which comes across his desk daily, how he defines what intelligence he wants available to him each morning, and what accommodations he makes in terms of his personal timetable and competing requirements to keep himself informed. Obviously, this approach is

proposed to dramatize a quite personal involvement in the intelligence process as something of service first, to the agency head, and secondly, to the investigator developing a specific inquiry. Such a presentation would only have impact if the official were able to demonstrate that he used intelligence directly and strategically. Its value as a reorienting device would come as he described how he was able to draw from his intelligence unit specific reports or briefings that assisted him in making better decisions about significant policy problems. Since there can be no substitute for the reality of the particular world in which each of the students lives and operates, the next step might be an informal session requiring them to adapt the speaker's system of intelligence usage to their own situations. This could be followed by a general critique of the various suggestions made by the course participants.

### "War Gaming"

Another technique for provoking new thinking on intelligence as a tool of supervisors is to involve each course participant in a "war game exercise." A scenario describing certain phased penetration moves of organized crime in a given city would be presented, and roles, such as police chief, prosecutor, intelligence unit commander, organized crime boss, etc., assigned to the various students in the course. The purpose would be less to find a school solution to the game than to construct later a list of the intelligence products that would have been useful in the course of the exercise. A postmortem of this type could arouse in the students a recognition of the intelligence resources they should develop with their own commands. The scenario would have to be carefully prepared, however, so that it posed a situation of some degree of reality. Too fanciful a game would only produce cynicism or derision.

### Writing the Intelligence Report

Anything training device which would have special meaning to the command level would be to assign each participant the task of preparing a weekly intelligence report for the agency head. The students would be given factsheets describing the previous weeks' events as they related to organized crime developments, newspaper stories, status accounts of various studies underway

in the intelligence unit, and a selection of recent investigators' reports and data received from other agencies. The task would be to compose something of value to the policymaking level of the agency. There need be no attention to such things as style or grammar in this exercise, but each student would be required to defend his selection of topics, format, and the overall thrust of his report against the criticisms of his peers and the course director.

Clearly, the variations possible in this sort of a training program are limited only by the imagination of whoever designs it. But in all cases the objective remains the same. It is to stimulate rigorous thinking about the relationship between intelligence and command level decisionmaking. Only the rare course director can describe this relationship with any degree of conviction or persuasiveness. On the other hand, a feeling for it may develop from the immersion into the process itself of those involved in decisionmaking.

The concept behind this approach is one which is reiterated throughout this volume: To appreciate the intelligence process and to be able to exploit intelligence effectively the component parts of the process must be understood thoroughly. Without this understanding, the command level officer will be unable to discern what he can do with the mass of paper coming across his desk, or will not fully grasp why he is being asked to acquire two additional investigators for his intelligence unit, or how he can measure the overall effectiveness of the unit, or offer any reasonable resistance to the public prosecutor who wants to "let up a little on hijacking investigations and concentrate on gambling." In effect, he will be more or less a helpless victim of the swirling events of the day, the routine preoccupations of all law enforcement agencies, and the seemingly mysterious expertise of his subordinates. Instead of being buffeted by all these forces, he should prepare himself to use intelligence for his own command purposes and to support him in controlling the assets at his disposal. The only way he can do this is to comprehend the intelligence process and its potential for contributing to the basic missions of the agency.

### Understanding Methodology and Process

So far the discussion has centered on intelligence as a product—that is, the informed judg-

ment resulting from the collection, evaluation, and analysis of varied scraps of information. The command level needs to have confidence in the process which converts raw information into these informed judgments. Moreover, and this point is critical for management, the command level must come to recognize that in a real sense it is responsible for setting the qualitative standards of the agency. Shoddy intelligence will result in bad decisions or faulty strategy or unrealistic plans. Therefore, training at the command level should aim at clarifying the evaluative and analytic elements of the intelligence process, not only so that the component parts of the process are fully appreciated, but so that the command level can assert its responsibilities for quality control at points where it may expect to make some impact. (See chapter II for a fuller discussion of managing the process.)

A significant portion of any command level training program, then, should be devoted to evaluating techniques and analytic methodologies employed in the intelligence process. The command level will not, of course, be deeply engaged in these matters itself. Instead, the training should provide insights which senior officers in command positions may find useful in querying the validity and soundness of the judgments offered to them by their intelligence apparatus. This portion of the training will have served its purpose if it provides the top levels of the agency with the capacity to ask tough questions about the way in which intelligence judgments are developed.

If the above sounds more like management training than intelligence training, that is because good intelligence results only when there is sound management of the information flow, and it certainly cannot afford to be passive about what it receives as an end product. The section of the training program devoted to analysis and methodologies should be sufficiently detailed so that it lifts the analytic process out of the realm of mysteries performed by experts and makes it, if only roughly, meaningful to top management. Such exposure should provide the command level with a far more sophisticated view of what an intelligence unit can do if the necessary funds and talents are available to it. It is important, therefore, that this portion of the course not be a mere representation of what is going on in the local organized crime intelligence unit, but that

it bring in the most innovative and even experimental approaches in use wherever they may be found. This, in turn, will normally require the appearance of speakers from other intelligence units or from Federal law enforcement agencies.

### **The Command Level and Organized Crime**

An innovative approach should also be used in that portion of the command level course concerned with organized crime itself. The emphasis should be on trends in the activities of organized criminal syndicates from a variety of urban points in the country. Since most law enforcement agencies suffer to some degree or another from "localitis," this approach may provoke some scepticism. It is always easier to say of one's own jurisdiction, "Well, *that* can't happen here," than it is to admit that, although you don't think it could happen here, it might, and if it did, you wouldn't necessarily know about it. For this reason it would be desirable to draw examples of organized crime activities from cities of a size and complexity comparable to that which the students serve. The training officer charged with preparing this part of the course may be hard put to come up with a variety of criminal activities from distant points. There is no better answer for this than to do careful homework well in advance. This may include a newspaper clipping file on organized crime stories, or even subscription to a clipping service on the subject. Regional contacts habitually used by the local agency can be tapped for this purpose and possibly the larger law enforcement community networks such as LEIU or an association of police chiefs.

### **Training Priorities and Hardware**

There need be no set program for a command level course set down in these pages. The few opportunities for training at this level will be very long in terms of man-hours away from the operational desk, so there will almost always need to be a high premium set on staking out training priorities. A good guide to follow would be that presented in this chapter:

1. Exploring what intelligence can do for the command level and how.
2. Understanding the intelligence process, particularly its methodology, and specifi-

cally some review of the latest analytic techniques.

3. Trends in organized crime activities throughout the country.

If there is still some time available after those broad subject areas are covered, then some consideration of new hardware application for surveillance, electronic detection, etc., could be introduced. Ideally this sort of instruction should be reserved for the technical experts, but as a practical matter, the budgetary aspects of hardware acquisition may be such that the command level may be obliged to become immersed in the subject. This is the level, after all, which will have to defend proposals for costly acquisitions. It had best know intimately what it wishes to obtain for the intelligence unit.

### OTHER TRAINING PROGRAMS

In chapter IV on staffing some suggestions are made for special training programs for the active intelligence officer and analyst. Nothing further need be added here save to remark that as organized crime changes its character, the skills necessary to combat it may be absolutely different from those now employed. The intelligence unit commander must remain flexible in the face of requests by his subordinates for specific specialty programs of training. Moreover, he should (budget permitting) encourage subscription to the professional journals of a variety of disciplines, and attendance by his subordinates at professional society meetings and conventions. These are where the newest ideas are floated; where reports of methodological breakthroughs are made, and where new uses for unfamiliar skills may be spotted. All of this, of course, is as much a part of training as actual course work.

### TRAINING TECHNIQUES

Scattered throughout the foregoing discussion of training for different levels of law enforcement officers and analysts have been suggestions concerning certain useful techniques: seminars, written exercises, "war gaming," etc. None of these untraditional approaches should be entered into lightly. They all require highly individualistic teaching skills, considerable preplanning, and, in some cases, access to a variety of unfamiliar materials and facilities.

But even within the traditional training framework, certain guidelines are useful to follow. Factsheets are better than lectures. Or put another way, lectures that are simply a recitation of factual data are deadly. A potential guest speaker who is a VIP in law enforcement circles is not thereby a great speaker. Find out about his oratorical talents as well as his reputation. He may do better in a discussion setting. Don't use outdated training films, the students will suspect that you are trying to use up time, or are lazy, or both. Effective field exercises use up enormous amounts of instructor's time, both prior to and during the exercise. Care should be taken that the result is worth the investment.

### Untraditional Training Techniques

Where budgets are relatively generous and training officers are generally free of other duties, new techniques of teaching should be attempted. Presumably the intelligence officers to be trained will be among the more resourceful and thoughtful personnel in the agency. As such they would probably make a good group on which to test new training approaches. Small group problem solving, for example, is a method which not only provides a gauge of intelligence and practicality, but can also measure in a rough way such things as leadership potential and personal volatility or flexibility. Similarly, open-book projects where the students are given a list of sources and a time limit against which they must construct a small and finite piece of analysis can be used as a method of judging mental dexterity, sense of priorities, and the ability to keep cool under pressure.

All these—and many other devices which could be used—should have one element in common. They should be learning experiences. That is to say, they should be monitored closely by the training staff with certain specific objectives in mind. The first objective would be to get across the idea that there are no school solutions to the problems or exercises in question. This, alone, should do a great deal to instill in the students the notion that good intelligence is often the product of a disciplined and imaginative mind, rather than an elephantine memory. Another objective of careful staff monitoring is to set up a critique or evaluation session at the end of each problem or exercise. It should not matter

in courses of this kind whether an individual did well or did poorly. What matters is that he learned how to do whatever the assignment as well. Accordingly, if he has done poorly, the critique should be modeled in such a way that he learns what he has done ineffectively, recognizes his deficiencies, and appreciates what to do about correcting them. The critique is not in this sense a corrective discipline, but an exploration with the student of those areas of the training he has not understood and an effort to strengthen his understanding then and there.

The approaches outlined in this chapter will require a considerable wrenching around of traditional law enforcement training programs. Training the trainers will be a large task in itself. For this, special arrangements may have to be made, such as sponsoring the education of a few training officers at a variety of institutes or Federal training schools for specialists. Such an investment will yield good returns if it produces *one* training officer capable of sparking student officer enthusiasm for trying new approaches to intelligence methods.

### **SAMPLE PROBLEM: TO DEMONSTRATE AND TO TEST ANALYTIC TECHNIQUE**

The following example explains what the instructor would give to the student and what action would be required of the student. To the greatest extent possible the problem should be so structured that there need not be a school solution but an approach that encourages the student to follow his own line of thought. The instructor must be ready on his part to evaluate different approaches to the problem, and to point out to the student where he might have requested other kinds of information. This is a problem to test technique rather than to test the ability of a student to follow a particular analytic path.

#### **Phase I**

*Instructor gives information to the students:*

The student is handed a piece of paper on which there is information purported to have been turned in by a reliable informer.

1. A woman by the name of Jane Doe was seen with Harry Jones. (Harry Jones is a known criminal, suspected of being in-

involved in hijacking. He is a lower level captain in Central City's West Side syndicate.)

2. The two had dinner at the Eating Club and Harry paid for a very expensive evening.

3. Jane Doe was dressed expensively and was wearing what appeared to be real diamonds.

4. They arrived at the Eating Club in a white Cadillac. The license number was NY 61245. Jane Doe was driving.

The investigator handling the informer added his own views, stating:

1. Jane Doe was a new woman for Harry.

2. From the nature of the outing, Harry must have received a substantial increase in his cut of the proceeds from whatever operation he was involved in.

3. Harry was never reported before eating at the Eating Club which is Central City's most expensive restaurant.

*Students are asked to respond to the report by:*

1. Developing an hypothesis to explain what the dinner date might mean and why it took place.

2. Make a list of five questions giving in order of priority additional information they believed immediately necessary to better understand what Harry might be up to. The student must also pinpoint where he thinks the information can be found.

#### *Sample Student Responses*

*Student 1: Hypothesis:* The meeting had no significance other than what it appeared to be, namely a dinner date to which Harry Jones had taken a new girl friend.

*List of questions:* (Student didn't think further questioning was worthwhile.)

*Student 2: Hypothesis:* The new girl friend and the expensive surroundings together indicated some change in the pattern of operation for Harry Jones. It could be that Harry's reported hijacking activities were beginning to go into high gear. This report should be considered as an alerting item and more information should be sought on a high priority basis.

*List of questions:*

a. Who is Jane Doe? Query the files.

b. Who is the registered owner of the Cadillac? Query the license bureau.

c. What is the status of hijacking on the West Side? Query files.

d. Who is involved in ownership of the Eating Club? Query liquor license bureau.

e. What has been the pattern of Harry Jones' activities over the past year? Query the files and the general police records.

#### *Instructor's Reaction*

*To Student 1:* This is a legitimate hypothesis but seems to be out of keeping with the potential meaning of the change in pattern for Harry Jones. Because of his rank, if for no other reasons, there should have been, at least, one round of further questions to determine who the girl was and what Harry has been doing recently.

*To Student 2:* This was an excellent hypothesis and one that could be tested rather quickly, at least, as to its general thrust and whether further activities should be focused on Harry Jones.

## Phase II

#### *Instructor gives new information to students:*

The instructor can give only the answers detailed below, and then only if the instructor feels that the student asked a valid question obtainable from a logical source.

1. Intelligence files—biographic.

a. No information on *Jane Doe*.

b. *Harry Jones* has a record of arrests for various crimes including armed robbery but not for hijacking. As informer report in his file states that he is newly in charge of hijacking operations for the West Side syndicate. The report is evaluated as probably true and the informer as being reliable.

2. Intelligence files—functional.

a. *Hijacking:* Substantial and increasing amount of hijacking on the East Side Dock areas. Small amount of hijacking on West Side Docks, beginning about 6 months ago.

b. *Restaurants:* According to unconfirmed reports, the Eating Club is owned by one of the criminal syndicates, some members of which have connections in Midamerica City.

3. *Auto license records*—license reported issued to Jim Roe, a resident of the East Side of the city.

*Each student is asked to respond to the new information by:*

1. Update, change, or write a new hypothesis based on the new information he obtained from the instructor. (Each student may have a somewhat different data base since all may not ask the questions necessary to get all available information. As stated above, the instructor should only give out the information that is now required and logical sources from which it can be obtained.)

#### *Sample Student Responses*

*Student 3: Hypothesis:* The presence of Jane Doe was a cover for a meeting in the Eating Club between Harry Jones and others unknown. It was probably an organizational meeting perhaps to bring Harry Jones together with the Midamerica City people who reputedly were owners of the Eating Club. The goal would appear to be to expand hijacking operations, especially focusing on means to unload the "hot" goods. It would appear that the Midamerica City connection might be the answer to the fencing problem.

#### *List of questions:*

a. Who is Jim Roe? Query the files.

b. What information is available on fencing of the hijacked items from either the East or West Side? Query the files under "Fencing." Also the burglary squad.

c. Who are the real owners of the Eating Club? Query corporate license office of the state.

d. Who are the known associates of Harry Jones? Query the files.

e. Who is Jane Doe? Check telephone company, credit bureaus, city register, voting registration, drivers license registration.

f. Query Midamerica City the following:

1. Any record on Harry Jones?

2. Any record on Jim Roe?

3. Any record on Jane Doe?

4. Any reports in intelligence files on hijacking that connects activities (including fencing of "hot" goods) between the two cities?

5. Any record of criminals holding ownership in Eating Club?

*Student 4: Hypothesis:* The dinner date represented out of town persons getting in contact with Harry Jones through the good offices of Jane Doe. The idea was to take over control of

the city. The outside element was using both the woman and money to buy Harry. The meeting portends a possibility of a gang war and an increase in crime as Harry attempts to prove to his new leaders what a tough, effective crook he really is.

*List of questions:*

a. Send urgent queries to all major cities in the area seeking answers to the following:

1. Any reports on criminals or others in their jurisdiction who were reportedly involved in hijacking in Central City or in the disposal of stolen goods therefrom?

2. Any reports in their files on Jane Doe, James Roe, Harry Jones?

3. Any reports on criminal gangs that appear to be attempting in any way to develop relations with any persons or groups in Central City?

b. Query the Federal agencies on Jane Doe, James Roe, and Harry Jones.

c. Query the Federal agencies on any reports having to do with hijacking in Central City and any link up between persons or groups in Midamerica City and Central City.

*Instructor's Reaction*

*To Student 3:* The hypothesis seemed reasonable in light of the information and would serve as a good guide to probing the problem further. It did not try to run away with the development as though it were a major threat. It might become such but the information available at the moment did not appear to support the Harry Jones operation as a major affair.

*To Student 4:* This hypothesis seemed to be running too far ahead of facts. It led the student to put too much pressure on a series of other law enforcement agencies to produce information. Finally, there was nothing in the information available to suggest that Harry Jones would be capable of taking over the city and thus worth such an effort by outsiders.

### Phase III

*Instructor gives additional information to students:*

The instructor can give only the answers detailed below and then only if the instructor feels

that the student asked a valid question obtainable from a logical source.

1. Intelligence files—biographic.

a. *Jim Roe* has no arrest record but is reported to be a principal captain in the organized crime syndicate that controls the East Side. A reliable informer report links *Roe* with a criminal group in Midamerica City.

2. Intelligence files—functional.

a. *East Side gang-syndicate:* This group has as their attorney *Sam Law* and their leaders appear to use the *Corner Bank*. An informer reports a rumor that the fence for the East Side gang is in another city, some say Midamerica City. Another informer report, unverified, states that *Jim Roe* has bragged about his plan to take over the city.

b. *Fences:* The West Side gang is reported using a legitimate company as a front for getting rid of their hot goods. Apparent owner is a woman, *Janet Joe*, from Midamerica City.

c. *Banks:* Information derived during an investigation on another case indicated that the majority ownership of the *Corner Bank* appears to be held through a front. Actual owner not known.

3. County Records. Ownership of *Eating Club* gives every appearance of being in noncriminal hands.

4. Intelligence files—Midamerica Police Department.

a. *Jane Doe* has no arrest record. She was the wife of *Bill Doe* who was convicted of being a fence and subsequently died in prison.

b. *Bill Doe* had a record of a number of arrests for robbery and for acting as a fence. He had one prior conviction for fencing. He reportedly worked with one of the syndicates, the North Side gang, which in the six months before *Doe's* arrest was reportedly becoming involved in hijacking.

c. *Jim Roe* was born and raised in Midamerica City. He had several arrests and one conviction for auto theft. He reportedly was a friend of *Bill Doe* and was seen with members of the North Side gang but is not thought to have been a member of the gang.

*Each student is asked to respond to the new information by:*

1. Updating, changing, or writing a new hy-

pothesis based on the new information he obtained from the instructor.

The sample problem ends here. However, the exercise could go on for several more phases. At each phase there should be answers that lead to nowhere, and others that are suggestive of totally different hypotheses. The goal is to test the capabilities of the students to put facts together and to construct a pattern, both tentatively to explain the events, and to guide the investigators in their search for additional facts.

FIGURE 14.—Two-week training course for intelligence analyst/investigator

<i>Subject</i>	<i>Hours</i>
<b>I. The Theory of Intelligence</b>	
A. Support Function in Law Enforcement .....	1
1. Support to the policymaker or agency head	
a. Strategic intelligence	
b. Contingency questions	
2. Support to the operational objective	
a. Tactical intelligence	
B. The Objectivity of Intelligence .....	1
<b>II. Organized Crime</b>	
<b>A. Traditional Patterns</b>	
1. Gambling (bookmaking, policy, casino operations, etc.) .....	2
2. Loan sharking .....	1
3. Prostitution .....	1/2
4. Narcotics traffic .....	1
5. Labor racketeering .....	1
6. Hijacking .....	1

<i>Subject</i>	<i>Hours</i>
<b>B. Nontraditional Patterns</b>	
1. Infiltration of legitimate business .....	1
2. Business manipulation .....	1
3. Real estate .....	1
4. "Skimming" .....	1
5. White-collar crime .....	1
C. Official Corruption as a Principal Objective .....	2
D. The Organized Crime Figure of the 1970's .....	2
<b>III. The Intelligence Process</b>	
<b>A. Collection</b>	
1. Field reporting .....	1
2. Surveillance .....	1
3. Informants .....	1
4. Undercover men .....	1
<b>B. Collation</b>	
1. Information control techniques .....	1
2. Automatic data processing .....	1
C. Evaluation .....	1
<b>D. Analysis</b>	
1. Problems in analytic technique .....	1
2. Problem solving .....	4
<b>E. Dissemination</b>	
1. Exercises in finished report writing .....	2
<b>IV. Operational Techniques</b>	
A. Investigative Aids .....	4
B. Electronic Equipment .....	2
C. Photography .....	2
<b>V. Special Field Problems</b>	
A. Investigative .....	12
B. Analytic .....	24 1/2
<b>VI. Intelligence and the Law</b>	
A. Trends in Judicial Decisions .....	1
B. Privacy Arrangements .....	2
C. Security .....	1
Total .....	80



# Chapter VI

## SECURITY AND THE INTELLIGENCE PROCESS

*Security, a special problem for intelligence unit due to:*

- *Sensitivity of information in files.*
- *Likelihood its personnel are prime targets for efforts to corrupt.*
- *Need for protection of rights of privacy.*

*Effectiveness of intelligence unit's operation depends on trustworthiness of its personnel:*

- *Assurance of trustworthiness requires probing of past and present actions of candidate for employment—especially financial status.*
- *Periodic updates required to insure that no adverse change occurs.*
- *Polygraph is useful in evaluating personnel, especially where any question of individual's integrity.*

*Steps must be taken to insure office spaces and, especially, files are protected at all times against access by unauthorized persons.*

*Protection of personnel while on information-gathering operations requires:*

- *Security of communications.*
- *Anonymity of the person in appearance and in vehicles used.*

### INTRODUCTION

Security is a special problem for the intelligence unit—security of personnel, office and files, and operations. Security is a particularly sensitive concern for two principal reasons: the delicacy of the subject matter in the unit's files, and the intelligence unit's attractiveness to organized crime as a general target for penetration or corruption. Security's place in the daily business of an intelligence unit must be fully understood or it will become an end in itself. Some intelligence officers are like the elderly librarian who is only happy when she has recalled all books on loan, and has every volume in its rightful

place on the shelves. She thereby achieves total control in a fluid operational situation, but, of course, loses all sight of the basic purpose of the library. Similarly, in the intelligence unit the purpose of security must be understood lest it impinge on the basic objective of the unit.

What are the purposes of security in an intelligence unit? They are to insure that: (1) Information on file is protected against access by unauthorized persons, and (2) information and reports circulated within the agency and distributed to other law enforcement agencies are protected in a manner commensurate with their sensitivity and, in no case, allowed to pass into the hands of unauthorized persons. There are,

also, some subsidiary objectives: (1) Enhancing the morale of the law enforcement agency as a whole by providing strong resistance to corruption, and (2) encouraging the flow of raw intelligence from the rest of the agency because of confidence in the security level of the intelligence unit.

To achieve these objectives, the intelligence unit must take steps to insure that all members of the unit are trustworthy and are in no manner acting as an agent for organized crime or any other lawless element. The unit must adopt physical security methods which ensure that the files are located in such a way that only authorized personnel have access to them. Steps must be taken to ensure that the area cannot be penetrated easily at times when no personnel are on duty. Personnel should apply rigorous security precautions in the performance of their duties. This applies generally to operations in a dangerous area, either in plain clothes or as an undercover agent. It applies specifically to the use of radio communications where there is always a risk of giving away their location or other information which would help to identify them.

Finally, it is important to understand that the security system has an important role in protecting the right of privacy of individuals. Much of the information in intelligence files has to do with allegations, unverified reports of activities and associations, and other matters which are not necessarily evidential. For example, the investigator cannot always be sure what the relationships are between a number of people observed individually entering a given location, allegedly for the purpose of holding a criminal enterprise meeting. The problem is even more complicated where a public place, such as a restaurant or tavern, is involved. Who is engaged in a conspiracy, and who is simply a hungry or thirsty member of the public? In many cases information secured from observations of this kind can never be presented in court. On the other hand, it is essential information for an intelligence unit that seeks to develop an understanding of the operational patterns of organized crime. Thus, the intelligence unit personnel and their commander must be fully aware of their responsibility to maintain a security system not only against potential penetration by organized crime, but also against inadvertent leakage of unsubstantiated information that might be damaging

to the person involved, whether or not that person has a criminal record.

These are the security objectives, then. They may be better understood if a list is made of objectives for which a security policy should *not* be reaching.

1. The intelligence unit must *not* use security to exclude authorized persons from reading or learning its findings. Intelligence is not produced for other intelligence officers (except to the extent it is essential for developing further analyses), but for the consumer beyond the intelligence unit. Once the consumer's need to know is determined, and found appropriate, the intelligence material must be made available to him. The intelligence unit must perfect guidelines for passing reports outside of its control. Such guidelines will generally concern the reliability quotients of recipients. But the end purpose of determining levels of reliability is to insure that the appropriate people receive and read the reports, not to prevent them from being read.

2. Security must *not* under any condition be used to conceal an intelligence unit's employment of illegal techniques, such as electronic surveillance where it is not permitting according to the statutes of the particular jurisdiction. In such a case, security would simply be contributing to a more disastrous showdown when, as is inevitable, the use of illegal means is revealed.

3. Security must *not* be used to conceal reports either from the jurisdiction's political leadership or other official representatives who are not members of the law enforcement agency, or to prevent documents from being used by a public prosecutor even though the sources of the documents are highly sensitive. Nor should security be used to conceal or cover up mistakes or corrupt activities by members of the unit or the agency.

4. To summarize, security *should* be used to the end of preventing disclosure of material to unauthorized persons, and to prevent unauthorized persons from gaining access to the files with the potential of misusing the information.

Security in any organization, whether it be military or diplomatic or police, focuses on three aspects. There is, first, the necessity to assure the personal security of the organization's staff. Secondly, there is the development of means for protecting records and facilities used by the agency. And, finally, there is operational se-

curity; that is, when communicating and when in the field on an operational problem. These various facets of security are discussed below.

## PERSONAL SECURITY

Any intelligence unit must be assured that its own members are themselves trustworthy, that they are what is known as good security risks. The security of a person can only be determined by probing his actions in the past, attempting to determine how he will react under certain circumstances, and by assessing the current associations and social patterns he maintains. While the background investigation is not a perfect system by any means, the experience of the Federal Government suggests that it is not only an effective approach to establishing the loyalty and integrity of an organization's staff, but it is the only method available.

### The Background Investigation

A background investigation should probe all aspects of a person's life, both professional and personal. The background investigation should seek to detect indications of lack of character or integrity in either context. A person who lacks integrity in his personal life—that is, in his dealings with his friends and family—will have a tendency at some point to act without integrity in a professional matter. It should be remembered that no one has a right to a position in public office, every citizen must fulfill the requirements established for that office before being considered. The character and integrity of an applicant are basic requirements, and, as pointed out above, they are especially important when associated with a position in intelligence.

Whether or not the intelligence unit has responsibility for performing the investigations of its own new personnel, it must be aware of the principles which guide such an investigation. (See appendix F for suggested guidelines to direct an investigation.)

*First of all*, it is essential that the investigator carefully evaluate all information reported on a subject. The simple statement, "It was alleged by a previous landlady of the subject that he was an undesirable tenant because his noisy parties—where, moreover, she suspected wild 'goings-

on'—caused complaints by the neighbors," is next to useless, unless evaluated. How did the investigator gage the character of the landlady? What was the relationship between the subject and the landlady? Had they had other differences which might explain in part her attitude towards him? Had the investigator checked with the neighbors about her allegations? Did the investigator attempt to trace down any of the associates of the subject during that period to satisfy himself about the subject's social life? In short, evaluation and careful checking out of derogatory information are basic elements of fairness, which should be the investigator's prime tool.

*Second*, it is essential that an investigator include information he develops in evaluating sources of derogatory information. In the example cited above, it is insufficient for the investigator merely to report negatively that he was unable to substantiate the landlady's allegations. Such a statement can be interpreted as meaning that in the absence of other evidence there is at least the possibility that the landlady's criticism reflected accurately on the subject's life style. If, on the other hand, the investigator details the steps he took to substantiate or discredit the landlady's testimony, then he has implicitly included elements of evaluation in the picture.

The recipient of the report can judge against the details of denials or agreements by the neighbors and associates of the subject how the landlady's accusations should be measured. This is perhaps an obvious point, but is one often missed by field investigators. It is missed because there is a longstanding tradition in many law enforcement agencies of dispassionate objectivity in conducting personnel investigations. This is a fine rule, indeed a fundamental rule for an agency that prides itself on integrity. But too often a narrow interpretation of what the rule means leads to ugly distortions. Thus, some supervisors fail to make the distinction to their investigators between dispassionate reporting of all the derogatory facts and the injection by the investigator of his own sense of fairness. The investigator who reports on the irascible landlady may be fully satisfied himself that she is a vindictive old bag, but if there is no latitude in his reporting system to allow for such an observation, then he is forced back into giving a distorted, albeit objective, report on his subject.

*Third*, the investigator must not allow fairness to preclude his consideration that the subject might in fact be a rogue as suggested by the derogatory information. This is the basic reason for careful checking of derogatory information. If an investigator is unable to satisfy himself that one dangerous allegation against a subject can be explained by the malicious character of the source or a strained relationship between the two individuals, he is justified in recommending further investigation into the allegation. If nothing further turns up which corroborates or negates the charge, then the subject himself should be asked about it.

Such a procedure is delicate and should best be undertaken with some care and preplanning. A formal but not unfriendly atmosphere for such a confrontation is best under these circumstances. Very often the subject's responses will give the investigator new leads to trace down; sometimes his personal reactions and facial expressions will reveal either genuine righteous indignation or some consternation mixed with guilt. In those jurisdictions where it is legal, polygraphing the subject (with his agreement) about the allegation can be useful. (See page 97 below for a discussion of the use of the polygraph.)

In the last analysis, if doubt still remains in the minds of the unit supervisor or the investigator, the subject may be told that unless he can help refute the allegation, his candidacy will be foreclosed. This may be looked on as putting the monkey on the applicant's back, but given the position he is hoping to assume, this is hardly unjustified.

In the background investigation, in addition to a search of the normal records of schooling, clubs, previous employment and family, questions should be asked concerning the candidate's financial dealings and his associates. (See figure 15, page 96, for a sample financial questionnaire). The financial dealings are important, if for no other reason than the negative one of determining whether the candidate is in financial difficulties which might make him susceptible to an offer of a bribe by someone intent on learning information about the intelligence unit's operation. A similar circumstance obtains where the person is conducting his personal life in such a way he might be open to the use of blackmail to cause him to betray a trust.

## Update of Background Investigation

It is important also to have a specific program for updating background investigations. Updating is necessary simply because people do get into trouble, even though up until the particular moment of transgression, they had nothing negative on their records. The update can be conducted at routine intervals for every staff member or, if in a large unit, a detailed investigation can be done on a spot-check basis; every fifth man, for example.

Updating should focus on two areas in particular. One is the financial status of the subject. The investigator should seek any evidence of significant change, either in terms of greatly increased spending habits or of substantial borrowing. The source of income which supports the increase in spending should be reported and the motivations behind the substantial increase in borrowing should be explored. In the first instance, income without an apparent source could mean a payoff. In the second instance, heavy borrowing could mean either a payoff or the development of a situation in which the subject could become susceptible to an offer of help (see figure 15, page 96, a sample financial questionnaire).

The second point of focus of an update should be on social life. Here again, any significant change without apparent cause should be investigated. In particular, a careful look should be given as to whether the subject's social group includes anyone on the fringes of organized crime. Similar care should be shown if the subject appears to be involved with a group that does not fit in with the pattern of his other activities, especially in terms of his income.

But, as important as is the updating of the background investigation of the intelligence unit's personnel, prior announcement of such a requirement is even more important. This is essential to prevent unwarranted concern that the update has been triggered by the revelation of negative information about a specific person. The periodicity of the updates should be specified; that is, whether they are to occur at one, two, three, etc., year intervals. Every person newly applying for a position in the intelligence unit, whether by transfer from elsewhere in the agency or from outside, should be told that the update is part of the requirement for service in

FIGURE 15.—Sample financial questionnaire

Name \_\_\_\_\_

Date \_\_\_\_\_

1. *Bank accounts*

Do you, your wife, you and your wife jointly, and/or your children have a:

checking account Yes \_\_\_\_\_ No \_\_\_\_\_

savings account Yes \_\_\_\_\_ No \_\_\_\_\_

safety deposit box Yes \_\_\_\_\_ No \_\_\_\_\_

If so, give the name of the bank and the type of account and the name of the person in which the account appears:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

2. *Charge accounts*

List the companies with which you, your wife, you and your wife jointly, and/or your children have charge accounts or credit card accounts:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

3. *Income*

Do you receive income from any other source than your agency salary?

Yes \_\_\_\_\_ No \_\_\_\_\_

If you do, give the source and amount:

\_\_\_\_\_  
\_\_\_\_\_

Does your wife, you and your wife jointly, and/or your children receive any income? Yes \_\_\_\_\_ No \_\_\_\_\_  
If so, give the source and the amount, indicating the name of the person receiving the income:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

4. *Property*

List all major items of property (real estate, automobiles, boats, etc.) owned by you, your wife, you and your wife jointly, and/or your children, giving the type of property, original amount paid, remaining indebtedness if any, and the address (in case of real estate):

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

List all stocks and bonds owned by you, your wife, you and your wife jointly, and/or your children, giving the company, the number of shares, and the date and cost per share when purchased:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

I certify that the statements I have made are true, complete, and correct to the best of my knowledge and belief.

Signature \_\_\_\_\_

the unit. Notification of this practice should be included in the initial interview when the requirements for acceptance by the unit are being described.

If the unit is sufficiently large so that the spot check method is employed, this, too, should be understood as a natural consequence of employment in the unit. There might be some merit in involving the rank and file members in the lottery selection of those to be investigated. Such a system would remove the arbitrariness of present background investigation procedures where candidates for investigation are chosen secretly and the investigations carried out and concluded as surreptitiously as possible. This procedure would have the further advantage of committing all members of the unit to active participation in the arrangements for deterring corruption. It could be an important building block in putting the agency on a footing where pride in the integrity of the personnel takes precedence over pride in personal loyalty to colleagues, right or wrong. But even where the spot check system is used, those not having the full field investigation should still have to fill out the financial questionnaire.

None of the foregoing is meant to imply that the unit commander should not have full authority to order a background investigation of one of his subordinates at any time. He, after all, is responsible for the overall integrity of his unit. If he suspects that one of his colleagues is "turning sour," he had best not wait until the routine updating background investigation comes up or take a chance that his suspect will be picked in the next background investigation update. For if he waits, he cannot be confident of the trustworthiness of his unit. He may be exposing the agency as a whole to serious damage.

### Polygraph

In those jurisdictions where it is permitted, the polygraph can be of great assistance in evaluating the integrity of a prospective staff member. (See chapter IV for a detailed discussion of staffing practices.) By its use, the unit can make sure that the subject is not hiding some past action that might cast doubt on his capability and, especially, on his honesty. It can be used to resolve doubts raised by an unsubstantiated derogatory report. In such cases, there may be

no alternative but to ask the subject about the truth of the allegation. If he is attempting to conceal his past actions, he can deny he ever did such a thing. Then the interrogator (and, especially the unit commander, particularly if he is really interested in getting the subject on his staff) is in a dilemma. The use of the polygraph, operated by experienced and well-trained technicians, can help resolve this dilemma.

The polygraph can be used at the time of the initial check and also at the time of the recheck or update. But, in either case, it should be the announced policy of the intelligence unit to require submission to this test. The prospective member of the unit must be told what to expect—whether the polygraph is used as a matter of course on all applicants both at the time of initial acceptance and at the recheck, or whether it is only used to check derogatory statements, as discussed above. The prospective staff member, by knowing in advance that he may be subjected to the polygraph need not feel personally offended when the test is given. More importantly, he probably will not apply in the first place if he has something he is attempting to conceal which he knows might keep him from being accepted as an intelligence officer.

It should be recognized, however, that, even though legally acceptable in the jurisdiction, the use of the polygraph may produce difficulties. One such difficulty could arise if it is used only by the intelligence unit. Agency personnel from other units might fear their careers would be jeopardized if by transferring to the intelligence unit they had to submit to the polygraph. The local police union or the civil service commission might consider its use by only one element of the agency as discriminatory and thus work against its being used at all. On the other hand, integrity standards for the intelligence unit should be as high as any in the agency—if not the highest. Use of the polygraph could symbolize the special personal requirements demanded of members of the unit.

### Security Training

It is important that special attention be given to security during the training of new personnel selected for the intelligence unit. They must be thoroughly indoctrinated with the requirements for security, why it is important, and the often

tragic results that can result from a breach of security. They should understand that people from their own unit, especially those working as undercover men, or their informers, can be put in jeopardy by security failures. (More specific data on training can be found in chapter V.)

## PHYSICAL SECURITY

The objective of physical security is to insure the personnel of the intelligence unit that no unauthorized persons will have access to their working quarters. The members of the unit should feel free to work with their material and discuss their cases and studies with one another without fear of compromising sensitive information. They should also be confident that the integrity of the information in their files is secure. No unauthorized persons should ever be allowed to use the files.

### The Office

To achieve the above objective, steps must be taken to restrict entrance to the area occupied by the intelligence unit to its own personnel and those formally accepted as being trustworthy. A log should be kept of all nonunit people that enter the intelligence unit's areas. (See figure 16, page 99, for a sample logsheet to record visitors.) There must be physical means to allow the intelligence unit to identify all persons before they can come into the area. In particular, there must be barriers and a specific recognition procedure that controls access to the working area of the unit. Furthermore, the file room must have additional controls, a controlled area within a secure area. (See figures 17 and 18 at end of chapter, pages 103 and 105, for sample office layouts.)

During the normal working day, one person should always be responsible for recognizing and admitting persons to the intelligence unit area. There should also be a person to watch over the files during this same period. At night, if no one is on duty, the room must be secured by some type of electronic or mechanical means that will trigger an alarm if anyone attempts to penetrate the intelligence unit area or, especially, the file room. The alarm should ring in the command center of the agency which presumably will be staffed 24 hours a day. (See the sample intelli-

gence unit office of the end of the chapter for a description of the several security measures that should be taken.)

### The Files

The files themselves, if in hard form, can be kept in ordinary filing cabinets. There is no need to have safes or special lock devices if the room itself can be secured as discussed above. If there is a problem in securing the room, then it would be well to have files with locking devices. In any event, where there is sensitive material, it should be placed in a separate area and stored in a safe. Sensitive material would be that containing informants' names; any information on corruption of members of the department or local political figures; or material given to the unit by other departments which they have classified as sensitive. Ordinarily the container of sensitive material should be located in the intelligence unit commander's office, but if not the lock combination should be available only to him or perhaps to one or two other senior members of the unit.

### Restricted Materials

The criteria for sensitivity of files or information are at base subjective matters; that is to say, some purely personal judgmental factor enters into most decisions as to whether a file, or a document, or an item of information is to be given special, protective handling. It is not good practice to have only two classifications of material—that which is sensitive and that which is not. Such a system works well when all personnel engaged in the clarifying process are dedicated to a free and full exchange of intelligence and are confident of the techniques for storage and evaluation employed in their unit. Their confidence is probably directly related to their substantive knowledge of what is in the files and how cautiously analysts have marked certain pieces of information as to source, and how precisely they have allotted evaluative weights to the contents. Unless this confidence is strong, however, the natural reaction of unit personnel will be to over-restrict the information in their files. Whether conscious or not, the guiding policy of the unit will be: When in doubt, restrict the information. The obvious solution for this state





of affairs is to build unit confidence by removing as much doubt as possible from the filing and classifying systems in force.

A useful means to build confidence is to move to a more sophisticated classifying (and this may mean, in turn, storage) system. Instead of relying on the simple dual category system of restricted or nonrestricted, a unit can introduce a range of sensitivity labels, or perhaps somewhat better, it can assign certain indicators to files or documents which characterize their contents in more than one way.

For example, documents containing unsubstantiated information about an individual could be assigned a color tab indicative of the fact that the material has not been corroborated. If the document in question concerns a matter suggestive of official corruption, another color could be added. If, further, the official corruption touches on a law enforcement agency, a third color could be included and so forth. Given combinations of colors appearing on the edge of a document or file would immediately warn as to the sensitivity quotient of the contents.

A supervisor faced with the choice of passing or not passing files or documents that otherwise would be helpful to a neighboring agency, could, with this system, make discriminating decisions far more easily (and helpfully) than if he has to rely entirely on an analyst's decision that the material in question is sensitive. Naturally, the most sensitive materials the unit commander will keep to himself, probably in his own safe. One residual benefit of moving to a color code system for contents sensitivity is that it will require a wholesale ransacking of existing files—presumably those dating back to a certain arbitrary fixed date, thus giving the unit one more review of its stored assets and the sensitivity level heretofore assigned to them.

### Security and the Computer

For the unit that has its own computer, there are special problems. Over and above the security of the unit's area discussed above, the computer and its data must be protected from penetration and harm. The first concern must be for the consoles through which the computer's information are queried and inputs made. Whether there is only one console or there are a series of remote stations, access must be controlled to only

those authorized. When further control of access to sensitive information is deemed necessary, computer programs may be coded so as to restrict retrieval to those who know the code. Not only to insure security but also proper evaluation of inputs, it is best that all inputs be inserted into the computer by the intelligence unit rather than directly from outstations. In other words, the computer should be programed to refuse outstation inputs. In a like manner, protection of data in the computer can be assured if no outstation can query the computer directly for intelligence information.

Other security problems concern the protection of the computer data bank from overt, unauthorized attempts to destroy or to modify existing information. Special care is required since data in the bank often requires review and correction. It may also require purging where the subject of the information is found to be incorrectly identified or, for example, where a suspect is released from judicial proceedings without conviction.

Finally, the computer room must be protected from unauthorized entry which could lead to the destruction of the machinery and/or the data filed on tapes or disks. Some member of the staff must have the explicit responsibility at all times of recognizing and admitting persons to the computer area. This becomes a particularly acute problem when the intelligence files are placed on a nondedicated computer; that is, one which is owned by another department and serves several elements of the jurisdiction's administration. (For a more detailed discussion of the problems associated with the use and protection of computers, see appendix B.)

### Security and Privacy

A major function of a security system of an intelligence unit in a police department is that of protecting its information from misuse. The privacy issue when it relates to intelligence files is a more difficult and urgent problem than it is in relation to routine police records, the so-called rap sheets. In the case of intelligence records, much of the information will be unverified and, therefore, will contain allegations, references to associations, and even include analyses of potential activities; routine police records are official documents. Much of intelligence material may

never be tested in the courts. Many whose names are in intelligence files will never be subject to arrest. Thus, it is critical that the security system of an intelligence unit protect the flow, storage, use, and distribution of information from persons not required to know about it, or from those like a hireling of an organized criminal group or someone who is seeking information in order to defame a private citizen.

The security of the system, in particular, must apply to the answering of requests for information from other units. Intelligence information should under no conditions be extended or given to non-law-enforcement agencies, including such operations as credit card bureaus, banks, employment agencies, personnel departments, etc. Care will have to be taken on a case-by-case basis to avoid giving such information to those law enforcement agencies that have a record of not handling such material in a protected manner. Secondary disclosure can be as damaging to the individual as disclosure by the primary agency. (For further discussion of privacy, see appendix A, "Intelligence and the Law." For a discussion of practical control procedures, see chapter III.)

### **Organization of the Office for Security**

To insure the implementation of security policy, it is essential in the intelligence unit that someone be given specific responsibility. He should be charged with making sure that physical security is maintained as designed, and that new personnel coming into the office are briefed on both physical and personal security. He must be responsible for seeing that the SOP worked out for security is implemented. In order to emphasize the importance of security, it is suggested that the task of security officer be rotated among the members of the intelligence unit. This way all become aware of the importance of the problem, and the additional responsibility is also equally shared.

### **OPERATIONAL SECURITY**

Security also has a definite role in the operations of the intelligence unit. The intelligence investigator must take measures to insure that his operations, that is, his specific activities at a particular time and place, are known to as few persons as possible. The investigator on a search

for indications of new criminal developments will want to have his efforts remain completely unnoticed, if at all possible. The analyst does not want anyone outside of the unit to know of his concentration on the development of a particular pattern of criminal activities about which he has as yet no hard evidence but sufficient indications to be relatively certain.

To maximize security of the unit's personnel, the office phones should be checked periodically to be sure that no wiretap has been put in place. The office should also be swept electronically to insure that no electronic eavesdrop devices are in place. If possible, the office should be given one or more nonagency listed phone numbers for use by its own personnel (as well as by informers).

Once in the field, the safety of the investigator can be enhanced by use of unmarked cars with nonofficial licenses. The cars should be stock models with no identification in the engine area which might reveal official ownership. Two-way radios should be concealed in glove compartments. There should be no antenna other than that used for the normal car radio. The colors of the cars should be popular but subdued so that they will not be readily distinguished. Second hand rather than new cars are preferable. Where funds can be made available, consideration should be given to the use of rental cars by investigators. Portable radio transmitter/receivers can be used in place of the fixed installation.

Security should be observed in communications from the field to the office (and vice versa). Wherever possible, investigators should use telephones—public phones if possible. Calls should be made directly to the intelligence unit, bypassing the agency switchboard. It makes little sense to check out intelligence officers specifically for integrity and then to handle their reports as routinely as investigators in the detective bureau.

Where radio must be employed, the intelligence unit should use a different frequency from the rest of the agency. Codes should be available that are also different from those used by the other units of the agency. The code may be simple, limited perhaps to the subject of investigation, the investigator, and the activities being reported. Coded names, letters, and numbers can be changed periodically. Since most of the intelligence unit's operations will be investigative rather than of an enforcement nature, it is imperative as a matter of security (both for the

operation and for the safety of personnel) that day-to-day operations be kept within the unit. Only where it is deemed absolutely necessary (or where the unit is acting jointly with or under orders of another unit in the agency) should other elements of the agency know of an on-going operations activity. Disclosure of such operational information should be carefully restricted to the specific activity. This care is required because of the known interest of organized criminals in penetrating the ranks of law enforcement agencies. It should become part of the SOP of the intelligence unit that it always operates as though other elements of its agency were penetrated. Obviously, this element of the SOP itself should be held closely so as not to antagonize brother officers.

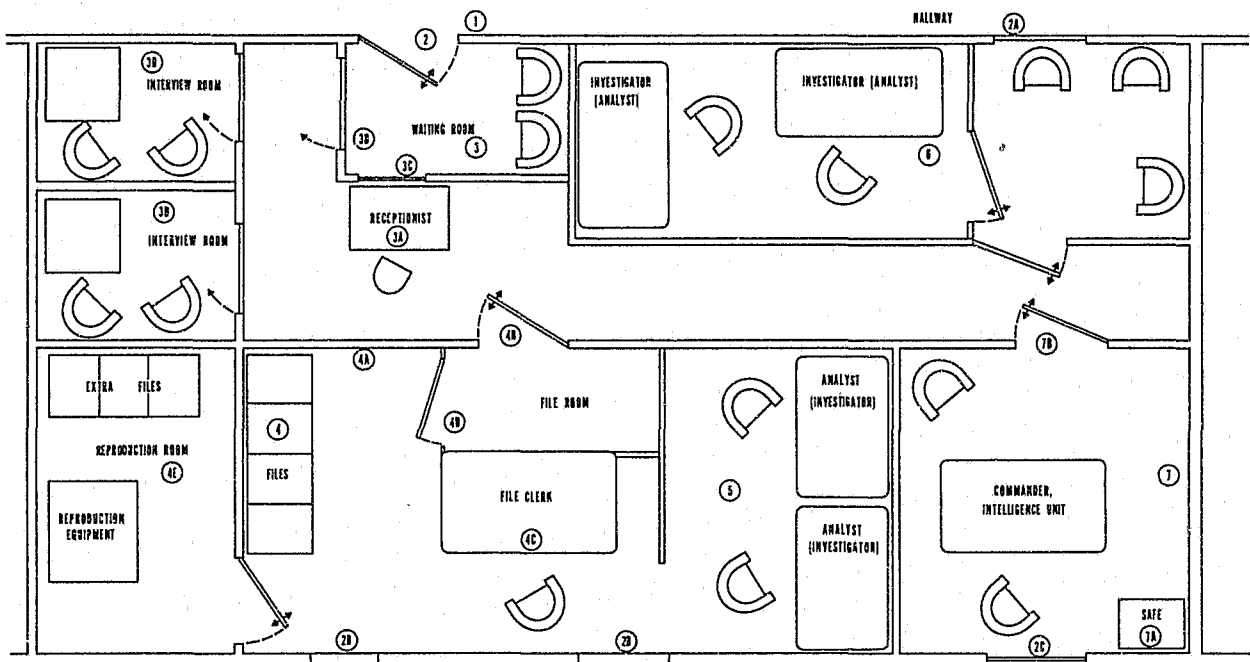
The commander of the intelligence unit must also take care to provide for the security of his own personnel when they are on operations where they may come in contact with known criminals. If personnel from other elements of the agency, or from other law enforcement agencies, should see and make reports of these contacts, it could cause false accusations to be made against the investigators involved. The commander may choose to have his people operate in pairs, or have another officer cover the person doing the investigating.

## THE RESPONSIBILITY OF THE UNIT COMMANDER

As in most functional areas discussed in this manual, the effectiveness of the intelligence unit's security system rests almost solely with the unit commander. Here again, the intelligence unit is set apart from the rest of the agency. As in training and staffing, the unit cannot rely on the normal operational guidelines to cover its security needs.

Thus, in most cases it will be the responsibility of the unit commander to develop the security rules for his unit. He must see to the arrangement of the offices. He must press to have his space secured in a different manner than any other in the agency. He requires special cars, and his communications require special consideration. His men must undergo a more rigorous background check and this may in turn cause problems in the normal operation of the personnel division of the agency. But all of these actions and policies will probably have to be initiated by the unit commander, and he will probably have to keep pushing to get some or all accepted. Even when these procedures are accepted as part of the operating routine of the agency, they will still be unique and thus require his particular attention to insure that security is effective.

**FIGURE 17 - A SAMPLE SECURE OFFICE LAYOUT**

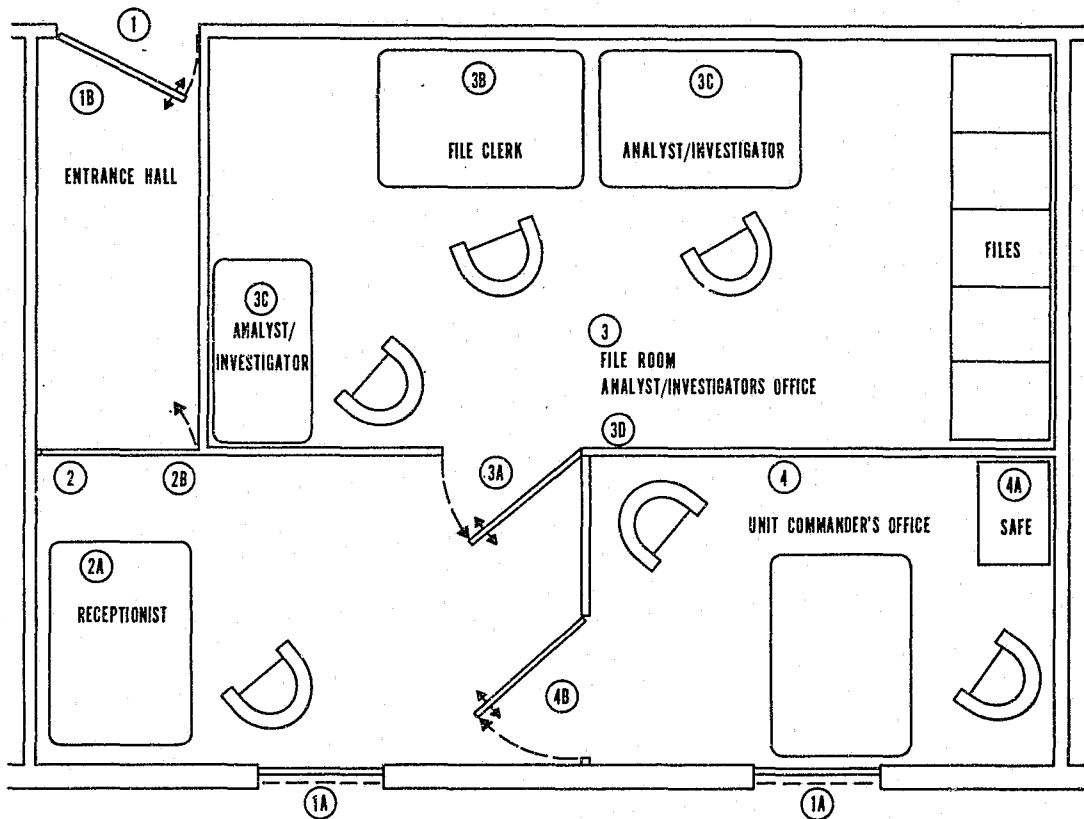


A sample office layout which demonstrates the physical security principle discussed above is shown in the figure shown above. The numbered items on the layout are explained in the text which follows.

1. If possible, the intelligence unit should always be housed above the ground floor. This adds the protection of whatever door guards are at the agency's entrance, and discourages potential walk-ins. It also minimizes the possibility of break-ins through windows that are not sealed.
2. The intelligence unit should be housed in an area with only one entrance which is under 24-hour-a-day control. If the office is closed at night, the door should be wired to give warning of an unauthorized intruder. The warning device should be connected to whatever desk (or area) in the agency that has 24 hour duty personnel. If the unit is in a building separated from the agency, or the agency does not have 24 hour duty personnel, then the warning system should be connected to the nearest police unit which does have around-the-clock operations.
  - 2a. If it is felt necessary to have other emergency exits for use in case of fire, they should be barred against entrance from the outside and wired to give an alarm if they are opened from the inside.
  - 2b. All windows in the area occupied by the intelligence unit ideally should be sealed.
  - 2c. However, if some windows are left unsealed, for example, in the commander's office, they should be secured against entrance from the outside by the use of bars, and an electronic device to give warning if the window is being tampered with.
3. There should be an entrance area which is closed off from the rest of the intelligence unit's space. This can serve as the waiting room for visitors and for persons to be questioned. It can also be the receiving point for mail and other documents, thus making it unnecessary for messengers to have access to the intelligence area. The point should be reemphasized: the fewer non-intelligence personnel permitted into the intelligence unit's space, the less opportunity there is for inadvertant or planned acquisition of data to which the intruder has no business.

- 3a. During the hours that the office is open and manned, there should be a person on duty to control access to the office. In smaller units, a receptionist can also be responsible for other duties such as handling the document and message log, answering the telephone, typing, newspaper clipping, etc.
- 3b. Access to the intelligence unit's space is through a door electrically controlled by the receptionist.
- 3c. The receptionist should be protected by a glass panel. However there should be a pass-through for the receipt and dispatch of mail and messages that are carried by non-intelligence unit messengers.
- 3d. Adjacent to the entrance but behind the controlled access door, there should be provision made for interview rooms. They should be individual rooms (they need not be large) to protect the privacy of the person who has come to give information. They should be so placed (as is shown on the diagram) also to protect the activity, files, and layout of the intelligence unit's office from the non-cleared person.
4. Files of information and reports of the intelligence unit must be kept in an area which can be physically separated from the balance of the intelligence unit's space and where access can be controlled.
  - 4a. Where possible, the walls of the file room should be made fire-resistant, if not fireproof.
  - 4b. The single access door should be wired so that when no personnel are on duty, an alarm will sound in the agency's command center if the file room is violated. During duty hours the door can be left open, but access should be only with the approval of the file clerk (or his temporary replacement should he be called away).
  - 4c. If at all possible, the file clerk (and possibly analysts who work closely with him) should be the only person allowed access to the files themselves. When materials are required by investigators (or analysts not given access) or by other elements in the agency, they should be requested from the file clerk. He should find them in the file, and, if the material is to be handed out, make a record of who has taken them and for what reason. Sensitive material should be clearly marked and given only to those specifically authorized by the unit commander.
  - 4d. To assist in the control efforts, access to the files should be denied by a gate electrically controlled by the file clerk.
  - 4e. Any provision for reproduction equipment (ZEROX or other make) should be controlled. One way, as shown on the diagram, is to place it within the area controlled by the file clerk. The room can also be used for additional files.
5. If the file room can be made large enough, it can be used as a secure area in which analysts can work. In this way, sensitive material does not have to be taken from the file room. Furthermore, if these analysts are given access to the files, there is little reason for them to take material from the file room.
6. The investigator and/or the analyst-investigator teams should be given office space which can be separated off, if only in cubicles, not only as an effective working area, but also to provide better security for the materials used and people interviewed. Compartmentation is a traditional tool of the intelligence trade used to reduce the possibility of a major penetration into sensitive information. The separation of some analysts from others makes certain that the materials that apply to each case will be kept separate. This separation can be applied in the sample to the analyst-investigator teams in that single teams can use spaces 5 and 6.
7. The intelligence unit commander must have a private office. He probably will have papers that he wishes to keep under his personal control. He will need to confer privately with visitors from within and without the agency because of the sensitivity of the material being imparted to him.
  - 7a. It is suggested that a safe be available to the commander in his office. This will insure the compartmentation of highly sensitive material and information that is for the knowledge of the commander alone (or for those members of his staff that he determines are to be apprised of it).
  - 7b. Efforts should be made to increase the degree of soundproofing of the walls and door of the commander's office to insure that his privacy is, in fact, maintained when the door is closed.

**FIGURE 18 -- A SAMPLE OF SECURE OFFICE LAYOUT -- SMALL UNIT**



The sample layout for a small unit follows the pattern and principals set down for the larger unit, as shown in Figure 17. The layout in Figure 18 was designed for a three to five man office, counting all personnel that might be included.

1. If possible, the intelligence unit should always be housed above the ground floor. This adds the protection of whatever door guards are at the agency's entrance, and discourages potential walk-ins. It also minimizes the possibility of break-ins through windows that are not sealed.
  - 1a. If the windows are left unsealed, as shown, they should be secured against entrance from the outside by the use of bars, and an electronic device to give warning if the window is being tampered with.
  - 1b. The intelligence unit should be housed in an area with only one entrance which is under 24-hour-a-day control. If the office is closed at night, the door should be wired to give warning of an unauthorized intruder. The warning device should be connected to whatever desk (or area) in the agency that has 24 hour duty personnel. If the unit is in a building separated from the agency, or the agency does not have 24 hour duty personnel, then the warning system should be connected to the nearest police unit which does have around-the-clock operations.
2. There should be an entrance area which is closed off from the rest of the intelligence unit's space. This is to keep control of person's entering and to minimize visitors who are not admitted seeing the layout of the office. The point should be reemphasized: the fewer non-intelligence personnel permitted into the intelligence unit's space, the less opportunity there is for inadvertant or planned acquisition of data to which the intruder has no business.

- 2a. During the hours that the office is open and manned, there should be a person on duty to control access to the office. In smaller units, a receptionist can also be responsible for other duties such as handling the document and message log, answering the telephone, typing, newspaper clipping, etc.
- 2b. Access to the intelligence unit's space is controlled by the receptionist with the aid of an electrically operated gate.
3. Files of information and reports of the intelligence unit must be kept in an area which can be physically separated from the balance of the intelligence unit's space and where access can be controlled.
  - 3a. The single access door should be wired so that when no personnel are on duty, an alarm will sound in the agency's command center if the file room is penetrated. During duty hours the door can be left open, but access should be only with the approval of the file clerk (or his temporary replacement when he is called away).
  - 3b. If at all possible, the file clerk (and possibly analysts who work closely with him) should be the only person allowed access to the files, and if the material is to be handed out once found, make a record of who has taken it and for what reason. If duplicating material is to be used, this should be controlled in the same manner. Sensitive material should be clearly marked and given only to those specifically authorized by the unit commander.
  - 3c. If the file room can be made large enough, it can be used as a secure area in which analysts can work. In this way, sensitive material does not have to be taken from the file room. Further-more, if these analysts are also given access to the files they can double for the file clerk if there is no other substitute.
  - 3d. Where possible, the walls of the file room should be made fire-resistant, if not fire-proof.
4. The intelligence unit commander must have a private office. He probably will have papers that he wishes to keep under his personal control. He will need to confer privately with visitors from within and without the agency because of the sensitivity of the material being imparted to him.
  - 4a. It is suggested that a safe be available to the commander in his office. This will insure the compartmentation of highly sensitive material and information that is for the knowledge of the commander alone (or for those members of his staff that he determines are to be apprised of it).
  - 4b. Efforts should be made to increase the degree of soundproofing of the walls and door of the commander's office to insure that his privacy is, in fact, maintained when the door is closed.

## Appendix A

# INTELLIGENCE AND THE LAW

New legal restrictions on some areas of intelligence operations are beginning to develop. These restrictions are generally based on the Constitution of the United States, and thus impinge or may soon impinge on State law. Although the courts have traditionally insisted on the elaboration of detailed legal regulation on certain aspects of the criminal justice system (such, for example, as the introduction of evidence), collection of domestic intelligence data, and the subsequent storage and dissemination of this data, have only recently begun to engage the attention of the courts and of legislative bodies.

This new interest in domestic intelligence gathering and its procedures springs from a number of recent developments:

1. Organized crime became a subject of national concern in the early 1960's; radical revolutionary movements in the late 1960's.

2. The various local movements for reform of criminal justice systems, together with important new constitutional decisions, have turned the spotlight on recordkeeping and data gathering procedures.

3. At the same time, there has been a significant jump in many localities in the volume and depth of criminal justice data collected and stored. More generous funding of State and metropolitan law enforcement agencies has meant that materials can now be collected and stored that would not previously have had high enough priority to qualify even for collection.

4. Finally, courts and legal theorists have enunciated a constitutional right of privacy. As yet, this concept is vague and imprecise, but as it becomes clearer, it almost certainly will affect intelligence procedures.

Law enforcement agencies, then, should anticipate that their intelligence activities will come under closer public (or, at least, judicial) scrutiny

than in the past. From this scrutiny may emerge detailed legal rules and standards of operation—either issued from the bench or prescribed by legislation or administrative orders. Questions of the constitutionality of domestic intelligence operations have already been raised in a few cases. The dissemination and usage of criminal history information—a much less controversial form of recordkeeping—is now the subject of legislative consideration in several jurisdictions and of a growing number of court cases. Congressional and to a certain extent public attention is also focusing more frequently on privacy problems—as, for example, the Senate Committee on the Judiciary hearings conducted by Senator Ervin in 1971.

The development of legal rules and standards for criminal justice intelligence systems reflects some public uneasiness about the potential hazards in such systems for civil and political liberties. The collection in secret of detailed information concerning the activities, habits, and beliefs of large numbers of citizens—whatever the form of criminal conduct in which it is believed they are engaged—involves substantial constitutional questions. Undisciplined collecting techniques and the indiscriminate aggregations of dossiers can, often unintentionally, undermine basic U.S. constitutional assumptions concerning a free society, tolerant of dissent and unorthodoxy.

Rules and standards for intelligence operations are beginning to develop, then, as deterrents to practices that threaten to abuse constitutional liberties. These rules and standards are not designed to cripple or eliminate completely the intelligence function as it relates to organized crime. Their emergence does mean, however, that every individual engaged in the collection, maintenance, and dissemination of intelligence



data should be aware that he is working in an area of high constitutional sensitivity. Detailed legal rules and standards defining the conduct of the intelligence officer and limiting certain of his procedures, will help him to safeguard important constitutional values. Scrupulous observation of rules and standards may also be the best guarantee in the future for the continued existence of the intelligence function. The purposes of this essay are to describe the direction in which the law in this area seems to be developing, to identify guidelines for the conduct of intelligence activities that have already emerged, and to suggest additional methods and standards of operations responsive to that direction and those guidelines.

## I

It may be useful to look backwards first and examine the rules which have traditionally governed the collection of domestic intelligence information. By and large there have been few. Legislatures, both State and Federal, have rarely treated the subject in any explicit fashion; judicial bodies have not often pronounced on abuses. Consequently, both private persons and official agencies have on the whole been left to ask such questions and collect such information as they believed to be proper.

The principal exceptions to this permissive state of affairs have been in connection with the fourth and fifth amendments. The courts have sought to prevent arrest and interrogation techniques that have the effect of forcing individuals to provide evidence incriminating to themselves. These restrictions have been extended beyond testimony given in formal courtroom proceedings to a wide variety of circumstances in which an individual is compelled to offer evidence that might, directly or indirectly, assist in his criminal prosecution. For example, the privilege against self-incrimination has provided the basis for the unconstitutionality of reporting requirements in the Federal gambling and firearms tax statutes.<sup>1</sup> The privilege's requirements have been extended beyond the courtroom so as to encompass all interrogations that occur while the interrogated person is in official custody.<sup>2</sup> Many lead-

ing commentators have recently argued that in these and other areas the privilege has been extended well beyond its proper scope.<sup>3</sup> In practice, however, many rules and practices have been permitted which might be thought inconsistent with the constitutional protection against self-incrimination. Thus, although some reporting requirements have been invalidated under the privilege of self-incrimination, others, no less hazardous in terms of potential prosecution, have been validated.<sup>4</sup> Until relatively recently, a claim of the privilege could be commented upon to the jury by prosecuting attorneys, often to the serious prejudice of defendants.<sup>5</sup>

The fourth amendment's blanket protections against unreasonable searches and seizures have also been extensively elaborated by State and Federal court rulings, and the controlling decisions are familiar to all law enforcement agencies. Finally, special statutory regulations have been imposed in many jurisdictions for collection methods regarded as involving particularly delicate privacy considerations. Wiretapping and electronic eavesdropping are the principal examples of such regulated methods.

Traditionally, more comprehensive restrictions have been imposed on the dissemination and *usage* of information than have surrounded its *collection*. Federal courts have for many years excluded the introduction of evidence obtained illegally, or as a consequence of leads unlawfully obtained.<sup>6</sup> This doctrine has been extended to prosecutions in State courts, and would appear to be relatively well rooted in the nation's judicial subsoil. In addition, there is the very considerable problem of civil liability for improper circulation of defamatory materials. While it is true that Government officials acting without malice have been protected from liability in cases where they have in the course of their official duties disseminated defamatory information, the threat of civil action nevertheless remains a potential weapon against officialdom for the private citizen who feels himself wronged.

<sup>3</sup> Friendly, *The Fifth Amendment Tomorrow*, 37 *University of Cincinnati Law Review* 671 (1968).

<sup>4</sup> *Cf. Shapiro v. United States*, 335 U.S. 1 (1948).

<sup>5</sup> *Griffin v. California*, 380 U.S. 609 (1965).

<sup>6</sup> This is known, aptly, as the "fruit of the poisoned tree" doctrine. See, for example, *Nardone v. United States*, 308 U.S. 338 (1939).

<sup>1</sup> *Marchetti v. United States*, 390 U.S. 39 (1968); *Haynes v. United States*, 390 U.S. 85 (1968).

<sup>2</sup> *Miranda v. Arizona*, 384 U.S. 436 (1966).

## II

Over the past 40 years the Supreme Court of the United States has drawn from the first, fourth, ninth and 14th amendments a series of important limitations on the purposes for which and manner in which government may collect information from and about its citizens. The Court's efforts have been premised chiefly upon the belief that such restrictions are imperative for the effective exercise of political and civil rights. The Court has recognized, for example, that "inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association."<sup>7</sup>

The essential point is that the public exchange of ideas must remain "uninhibited, robust and wide-open,"<sup>8</sup> and that this is possible only if the activities and beliefs of large numbers of individual citizens are not cataloged and assessed by Government agencies. The political argument that follows from this line of judicial thinking is that if government were permitted unrestricted opportunities to collect information about its citizens, unorthodoxy might be discouraged by notoriety, and even the mildest eccentricities might be noted for official evaluation. Society might be left relatively more homogeneous, controlled, and rigid.

The restrictions upon information gathering and dissemination which are developing from these assumptions have been described by some jurists and legal theorists as flowing from a right of privacy implicit in the Constitution. Few legal commentators agree on what the right of privacy means and what it entails. Now however, there is clear authority that such a right is included in the Constitution.<sup>9</sup> The broadest interpretation is that it constitutes a right of personal autonomy, that is, an individual's freedom to develop his personality and interests without fear of governmental interference. It would be difficult to imagine a more abstract or far-reaching doctrine. Nonetheless, a number of State and lower Federal courts already have accepted such an interpretation. Courts have on this basis held unconstitutional statutes requiring motor-

cyclists to wear helmets. They have ruled that schools and other institutions cannot regulate the clothing and hair styles of students and employees. A great variety of attacks, some of which already have been successful, have been made on statutes regulating sexual conduct exercised in private by consenting adults.

A narrower interpretation of the right of privacy—and a more concrete one—holds that an individual, in the absence of overriding social needs, has the right to control the dissemination to others of information concerning his behavior, beliefs, associations, and characteristics. This is the meaning of privacy suggested by many of the leading legal commentators.<sup>10</sup>

It is too early to identify the specific terms of the constitutional restrictions upon domestic intelligence activities that are coming or may come as the right of privacy develops. Many important questions have not been addressed by courts or legislators. There is, however, substantial evidence that these restrictions will follow certain general lines of development, which may be summarized as follows:

First, it is clear that the constitutional right to privacy is not absolute. Protection of individual rights as a desirable purpose of society must be balanced against competing social interests. Among the factors to be weighed in the balance are the degree of the intrusion for the police purpose at hand and the availability of alternative methods to serve the same purpose. A permissible intrusion is, in other words, one that strikes no more widely or deeply into personal affairs than is essential for the achievement of a proper public purpose. This is a process of measuring and balancing competing social purposes, none of which may be assessed with arithmetical precision.

Second, privacy rights are more likely to be upheld by the courts where the rights in question approximate more traditional and familiar rights of all individuals. For example, courts generally will be disposed to scrutinize most carefully intrusions violative of personal freedom when the individual or individuals involved are potential targets for criminal prosecution. This in turn will impose obligations on organized crime intelligence units to balance the social purpose of

<sup>7</sup> *NAACP v. Alabama*, 357 U.S. 449 (1958). See also *Gibson v. Florida Legislative Investigative Committee*, 372 U.S. 539 (1963).

<sup>8</sup> *New York Times v. Sullivan*, 376 U.S. 254 (1964).

<sup>9</sup> Cf. *Griswold v. Connecticut*, 381 U.S. 479 (1965).

<sup>10</sup> See, for example, A. Westin, "Privacy and Freedom," (1967).

an intelligence operation against the privacy interests of the target personalities.

Third, officials will be permitted to intrude on the privacy interests of citizens only for purposes clearly related to constitutional responsibilities. Idle or marginally useful inquiries will be impermissible. This does not mean that it is sufficient that the overall purposes of the agency or intelligence unit are constitutionally acceptable. The question instead will be whether each intrusion—indeed, each element of data collected—is reasonably related to government's constitutional responsibilities. Stated as baldly as possible, intrusions will be limited to those absolutely imperative for the effective performance of the law enforcement's agency's responsibilities.

Fourth, the methods by which data are collected will increasingly come under closer scrutiny. It may be that methods which the courts find to be unnecessarily intrusive will be subjected to severe restrictions. Data obtained by such methods may be excluded from formal presentation in proceedings involving the individual's rights or property. This would represent merely a short extension of the judicial rule that excludes as evidence any information collected by illegal means.

Fifth, certain judicial holdings, particularly *Griswold v. Connecticut*, 381 U.S. 479 (1965), suggest that "special zones of privacy" may be created. These would be physical or geographical areas, such as the home, in which any intrusion would be particularly suspect. The exact legal prescriptions against intrusion that might emerge from the recognition of such special zones under the law are not yet clear.

Sixth, procedural requirements may be established for the collection or dissemination of various classes of data. As the significance of such collections becomes more widely understood, proposals may be made that information gathering agencies take various steps only with the prior approval either of a magistrate or of a higher administrative officer. The purpose of such restrictions would be to submit intelligence decisions to the review of relatively independent and disinterested governmental officers. Such requirements have of course already been established for the collection of information by electronic surveillance and electronic eavesdropping.

Seventh, the constitutional right to privacy may well take shape as a "consensual doctrine."

That is to say, an important presumption underlying the right to privacy would be that the disclosure of information about an individual rests on the prior consent of that individual. The principal standard for the propriety of collecting or disclosing personal data would be the express, or, at least, the implied consent of the subject of the data. This, of course, would be a standard not easily met by criminal justice intelligence systems. The recognition of such a standard in the law would *not* mean that intelligence systems that fail to satisfy these standards would be outlawed. It could mean, however, that the intelligence unit that collects or discloses information about a given individual, without his consent, would be obliged to demonstrate to a court's satisfaction the necessity for bypassing the normal standards.

Eighth, rights of access and challenge by individuals to data collected about them are likely to become increasingly familiar aspects of intelligence files and data banks. The establishment of such rights corresponds to the concept of consensuality. They also represent reliable and inexpensive guarantees of data accuracy. As such rights become more common, and their significance more widely understood, any failure to include them—as will necessarily be the situation with respect to criminal justice intelligence systems—will stimulate demands by the courts for explanation and justification. As with the concept of consensuality itself, the intelligence unit that denies rights of access and challenge may find that the evidentiary burden is placed upon it to justify its data collection and storage activities.

Ninth, it is likely that privacy interests will receive special attention where they intersect with, or are necessary for the protection of, constitutionally protected civil and political liberties. In particular, courts may give special protection to privacy interests which support constitutional rights of speech and association. This was, for example, the basis of *NAACP v. Alabama*, cited above, in which the Court protected from disclosure various NAACP membership lists. This emphasis upon privacy interests where they are essential for the protection of other constitutional rights merely reflects the preferred position traditionally assigned by the courts to civil and political liberties.

The possible developments described above

certainly do not constitute any comprehensive guidelines for the governance of criminal justice intelligence systems. They are intended to indicate only the direction in which the law now is going. As noted earlier, many questions—including those of the greatest practical importance—have never been directly addressed by courts or legislators. Nonetheless, these guidelines suggest various methods and standards of operation essential for every criminal justice intelligence system. Those methods and standards of operation are described in the section which follows.

### III

This section will identify methods and standards of operation responsive to the legal rules which appear to be developing with respect to the collection, storage and dissemination of domestic intelligence data. For convenience, the section will be divided into various subsections, each concerned with a separate aspect of the operation of criminal justice intelligence systems. Each section contains a common problem: the balancing of conflicting social interests and values in a fashion consistent with limitations imposed by courts or legislatures interpreting constitutional guarantees. The impact of an intelligence system upon the constitutional rights of those about whom it collects information ultimately depends upon the whole of the system's operations: the categories of individuals included in its files, the persons and agencies to which it disseminates information, the provisions it makes for verification and purging, the adequacy of its security arrangements, and so on. The balance of this section will be devoted to an examination of each of these aspects.

(i) *The scope of the intelligence system's activities.*—The issue here is essentially whether intelligence systems should be closely restricted to organized criminal activities, in the sense of racketeering enterprises, or whether instead they may be extended to all situations in which groups of persons are thought to be persistently engaged in pernicious activities. The important practical question is whether organized crime intelligence systems should be broadened to include civil disorder files and other records concerning groups who are thought to be engaged in subversive or dissident activities.

This question has frequently been thought to be one merely of administrative convenience—a problem of the most efficient use of available resources and storage space. In fact, much more serious problems are at issue. Civil disorder files involve constitutional questions of the greatest seriousness. Although these questions are only now beginning to reach courts and legislators, it is clear that such files offer palpable dangers for the exercise of political and civil rights. Merely the collection of such information may discourage the exercise of rights guaranteed by the Constitution. If such files were intermingled with organized crime intelligence records, the constitutional problems implicit in the former would inevitably attach to the latter. Moreover, the political and public acceptance of organized crime intelligence systems would be eroded by the controversy that might surround civil disorder files. As a matter both of ordinary prudence and of sensible administration, intelligence files relating to organized crime and racketeering activities should be maintained entirely separately from civil disorder records.

(ii) *The persons to be included.*—In part, this question merely repeats those discussed above, for it is imperative that organized crime intelligence files should not be broadened to encompass information concerning the political and other activities of unpopular or unfavored groups of citizens. But it is also important that conscientious efforts be made to prevent the collection of information concerning citizens about whom there is no reasonable basis for a charge that they are involved in organized criminal activities. This, admittedly, is a goal more easily stated than achieved. However, since every system should include mechanisms for the prompt and, so far as reasonably possible, the complete evaluation of data entering the system, the least substantial entries can be readily eliminated. Information that seems plausible, but cannot be verified should *not* be disseminated, or, if disseminated, should be rigorously restricted to the law enforcement intelligence community and accompanied by clear warnings that it is not yet substantiated.

The essential point is that organized crime intelligence units should target as precisely as possible on known or suspected participants in syndicated crime. Where known racketeers are involved in otherwise legitimate businesses, it

may require extensive investigation to determine which business partners are criminal associates and which, if any, are unwitting, innocent business colleagues. Differentiating between the two becomes particularly difficult where some of the figures in question have no criminal records. Probably the best guideline here is the rule of reason. Where an associate is an intimate of a known racketeer, whose interests appear to be intertwined with those of the criminal, he should be the subject of an intelligence file. Where the connection appears more tenuous and the person in question has no criminal record, he probably should not. The line is a difficult one to draw, and some diminution of intelligence operations' effectiveness could result from drawing it too sharply. But a forward and liberal posture by the intelligence unit on this kind of question may sometime in the future protect the overall activities of the unit from judicial censure or even legally imposed restrictions.

(iii) *The data to be included.*—It is essential that organized crime intelligence systems should restrict the data included in their files to those reasonably relevant to preparation for prosecutions. Each intelligence system should assume a continuing obligation to evaluate each of the data elements it collects in light of this restriction, and to eliminate those elements which are found to be no more than marginally useful. In particular, the collection of data that are "unusually intrusive" should be permitted only if they are, after careful assessment, found to be necessary for effective intelligence operations. This evaluative obligation must be a continuing one; each system should periodically assess the information it collects to determine if there are categories of information which may be eliminated from its collection efforts.

Special attention should be given to data which may be tainted by the unlawfulness of its collection. The handling of such data is by no means an easy problem: in the first place, such information cannot easily be identified. Complex issues of law, perhaps involving ambiguous or changing legal principles, may often arise. It is unrealistic to expect that busy intelligence analysts can come up with fully accurate solutions to such issues. Nonetheless, the dangers of error are by no means trivial: information tainted by the unlawfulness of its collection may taint the information obtained through it, caus-

ing the inadmissibility in judicial proceedings of the entire chain of evidence.

Certain minimal safeguards are therefore needed. First, those responsible for the evaluation of intelligence data should be made aware both of the law's requirements and of the urgency of complete adherence. Second, legal counsel should be available to each intelligence unit, to whom doubtful questions should be promptly referred. Third, where the information has been obtained from another law enforcement agency, that agency should be required to offer an assessment of the legality of the information's collection. These devices do not provide any complete guarantees, but, if combined with continuing efforts to avoid the collection and dissemination of such information, they offer at least minimal protection against potentially quite serious errors.

(iv) *Data purging.*—For more than one reason intelligence unit commanders should commit themselves to periodic purgings of the materials in their data systems. The mere entry of a data element into a storage system is often enough to confer authenticity on the data for years to come. Or, to put it differently, data systems deepen institutional memories; once in the system, a fact, a name, an allegation, a report, rarely gets out, even if it is not totally accurate, or if it is false. Periodic purging, then, becomes a matter of maintaining the accuracy of the files or stored materials. At the same time, the elimination of false or inaccurate data on individuals contributes to the protection of the civil rights of the subjects. The intelligence function, which necessarily depends for its success upon the correlation of information obtained over time from a variety of sources, can be purged only with great difficulty and with some risk that "the missing piece" in some future puzzle will be eliminated. But ambitious purging schedules can, potentially at least, jeopardize the chance of making successful future correlations. Accuracy and a sound constitutional approach suggest that purging on a fixed timetable should be a required procedure for all units.

(v) *Dissemination and use of intelligence data.*—The potential dangers to privacy rights and other constitutional interests are related to the kinds and effectiveness of the limitations that organized crime intelligence impose upon the dissemination and usage of their data. Although

the mere collection of personal information may be regarded as creating privacy and other constitutional problems, the severity of those problems rapidly increases as the information is more widely disseminated. A series of restrictions upon such dissemination is imperative if important constitutional problems are to be avoided. (See chapter III for a discussion of restrictions on dissemination.)

Above all, the dissemination of organized crime intelligence data should be restricted to criminal justice agencies with a clear need to receive them. This suggests that the "information buddy system"—the customary device by which information is given only to those in whom the information's collector has personal confidence—is an important and useful limitation, albeit a haphazard one, within the criminal justice community. But sound practice also suggests that many members of these informal buddy systems—trusted newspapermen, legislative aides, employees of non-criminal-justice agencies, private investigators, and others—should be excluded. Some of the information collected by organized crime intelligence units is highly sensitive, and some of it, if released, could have significant political and social consequences. Careers, election campaigns, employment opportunities and personal lives might easily be wrecked. To permit the dissemination of such information—which may be wholly or partly unreliable, which may be less than fully verified, and which may represent only part of the relevant data—at the option of an administrative official, without the intervention or assessment of any court, presents significant dangers for individual rights.

There are various possible limitations. First, at a minimum, dissemination outside the criminal justice system, whether formal or informal, should be prohibited without the approval of the intelligence unit's highest official. This approval should be given only after consultation with legal counsel. It might well be made contingent upon the further approval of appropriate officials outside the intelligence unit itself. Good procedure would also dictate that official records be kept in the originating agency of all materials disseminated outside of its control.

Second, the intelligence unit should be prepared for the possibility that such disclosures will ultimately result in a judicial ruling by

which the individual involved in the disclosure will be permitted access to the system's files concerning him. The unit should further anticipate that civil remedies, including monetary damages, may be provided for cases of abuse. Such remedies now exist for many situations, but they are, as a practical matter, of little assistance to injured citizens, and it should be expected that they will ultimately be made more effective. Yet another possible consequence might be the creation by statute of a requirement that such information may be released outside the criminal justice community only with the prior approval of a judge or magistrate. This would, in other words, extend the warrant system to such disclosures.

These possibilities in turn suggest a demand with which all information systems may shortly be forced to deal: the demand that information systems should permit rights of access and challenge to all those persons whose names are included in their files. There is a clearly discernible trend to impose this requirement on most large-scale information systems in business, credit bureaus, etc. Exempting intelligence systems will inevitably provoke demands for explanation and justification. The justification for exemption that can be offered by organized crime intelligence systems is persuasive and effective, provided that intelligence data are held within the criminal justice community and used only for investigative and prosecutorial purposes. To the extent that such data are released outside criminal justice agencies or are used for other purposes, it will be exceedingly difficult to justify withholding them from the individuals involved.

(vi) *Data classification.*—Precisely as effective intelligence operations require a systematic evaluation of the reliability of the information collected, so such an evaluation contributes to the protection given to the rights and interests of the individuals involved. The point again is that individuals interests are directly served by the care and professionalism of an intelligence system. (See chapter II for material on classification.)

(vii) *External councils and advisory groups.*—One of the most common proposals for the governance of intelligence systems is the provision of an external group to provide policy guidance and direction. Such groups, particularly where intended to perform only advisory functions,

cannot realistically be expected to impose significant restrictions upon the activities of any intelligence system. The administrators of the system will know too much and the advisers too little; the administrators will have time and opportunities for preparation and the advisers will not.

Nonetheless, these objections need not mean that such groups are altogether without value either to intelligence systems or to the public. For the intelligence system, they can offer an opportunity to test ideas and suggestions against a sample of well-informed and interested outsiders. If used wisely, such groups might help to avoid many serious policy errors. Moreover, the existence of such a group might significantly encourage public acceptance of intelligence systems. For the public, such groups could provide a mechanism for the transmission of relevant information in two directions: public fears and complaints could be communicated to the system's administrators, and general information about the system's activities could be communicated from the administrators to the public. The usefulness of such groups should not be exaggerated, but they offer at least some assistance in the governance of agencies that are both controversial and potentially dangerous.

(viii) *Personnel and physical security*.—These questions are discussed in detail in chapter VI, and it is necessary here only to observe that an adequate security system, including careful clearances of system personnel, directly and significantly contributes to the protection of individual rights and interests.

(ix) *SOP's*.—Finally, many of the procedures and guidelines suggested in the preceding paragraphs are clearly less than precise. In some

jurisdictions there will be legal requirements for implementing few, if any, of them. But one purpose behind the design of these procedures and guidelines is to forestall possible legal action in the future against the individual officers or files of an intelligence unit. In this connection it is well to remember that evidence of institutionalized procedures is often considered favorably by the courts as a demonstration of good "faith and reasonableness." In other words, an SOP incorporating these procedures and guidelines should not only be in force, but be available to all personnel of the intelligence unit, as well as to the public.

#### IV

The rules and standards of operation described above are not intended to be exhaustive statements of the law's demands, or possible future demands, upon domestic intelligence systems. The point to be kept always in mind is that the law has only recently begun to provide rules for the governance of such systems, and it is not yet possible to offer clear guidance as to the form and content of the rules which ultimately will be developed. Nonetheless, whatever the rules that ultimately appear, the important fact is that privacy and other constitutional values should be a continuing concern of every organized crime intelligence system. A principal ingredient of the decisionmaking process with respect to such systems should be the consequences of any action or policy for individual rights and interests. If this concern is demonstrated by those who conduct such systems, the likelihood that they will attract and hold public confidence will be increased and the dangers they offer to political and civil rights will be diminished.

## Appendix B

# THE COMPUTER AND THE INTELLIGENCE UNIT

### INTRODUCTION

This appendix gives some general pointers about the use of a computer by an intelligence unit. It suggests the conditions under which an intelligence unit should consider committing resources to this purpose. It reviews the various uses to which a computer can be put—information storage and retrieval, collation, and analysis. This appendix does *not* attempt to develop or to suggest programs nor does it attempt in any way to probe the technical attributes of computers.

There is no doubt that when the intelligence process is computerized the intelligence unit will become more efficient. But this will have a cost. Resource planning and allocation must take into account a series of expenditures, including:

1. An initial cost-effectiveness study to determine the advantages it is hoped will accrue to the unit.
2. The development of the software or programs to determine how the bits of intelligence information will be available.
3. The large task of reviewing existing files to determine which ones and what contents of each should be put into the computers data bank.
4. The development of computer related information report forms.
5. Operational costs which will include:
  - a. A proportionate share of the cost of the computer.
  - b. A share of the cost of the computer-personnel, including: (1) computer operators; (2) programmers (contract or hire—to refine and to update programs through time to keep abreast of changing circumstances);

and (3) punchcard operators or typists to input data as it becomes available.

This appendix can offer little to assist in giving guidelines for the above cost analyses. Little has been published that will guide such calculations. It apparently must be done on a case-by-case basis. Computer companies or independent consultants in the field must be called upon to assist in making these studies and analyses.

There are mechanical aids other than the computer that are available to the intelligence unit. However, the discussion that follows focusses on the computer because the authors believe that it offers the most flexible and, thus, the most effective system in the long run. Whatever approach is adopted, it is recommended that from the first step taken to bring in mechanical aids, arrangements should be compatible with eventual conversion to a computer. This applies to the indexing systems adopted and the data input forms. In particular it applies to developing information element codes.

For those concerned that the computer will tend to run the unit, or cause unwanted information flow burdens, it must be remembered that the computer is a machine. Its output is bounded by the information put in and the instructions given to it through the programs that tell the computer what to do with the information in its storage tapes or disks. It cannot require that additional information be collected, nor can it make its own analyses. Its output can only show holes in the data bank and its programmed collation can only assist analysis. But there is no doubt that the presence of the computer, once its capabilities are appreciated, will have the effect of pressing the unit to gather



more information and to make the reporting compatible with the input programs.

### **CONDITIONS FAVORABLE TO CONVERSION TO COMPUTER**

Two major criteria should be kept in mind when considering the possibility of computerizing the intelligence unit:

1. The availability of a secure computer.
2. The level of existing or potential organized crime activity and the volume of information on it.

#### **Availability of a Secure Computer**

Because of the sensitivity of the information in the intelligence unit's files, security of the computer operation is essential. (See chapter VI and appendix A for a discussion of the problems of security and, especially of its relationship to privacy.) The security problem seems to rule out the shared-time approach when the computer being shared is not owned or leased by the law enforcement agency or by the jurisdiction in which the agency operates. In either of these cases the intelligence unit can potentially, establish adequate rules and procedures to achieve a requisite level of security. The specific problems involved in computer security will be discussed below in this appendix, beginning on page 118.

By themselves the information storage and data handling requirements of most if not all intelligence units do not seem large enough to support a computer operation. However, if an agency already has acquired a computer or is planning to do so for the handling of the general files and control of its patrol forces, then there should be active planning to get a "piece of the action" for the intelligence unit.

#### **Volume of Data To Be Handled**

However, before the conversion exercise is laid on, the intelligence unit commander should do an analysis of the amount of information his unit receives and how efficiently it could be handled with improved manual techniques, and most importantly, what is the projection of the organized crime problem over the next 5 years. The changeover from a hand-operated system to one that is computerized is a relatively costly operation. One approach is to review all files and

introduce into the computer all that have currently usable information. A more austere approach is to establish a cutoff date from which point forward all information will be collected in a format compatible with inputting the computer and retain and use the old files in their hard copy form. A compromise on the latter approach would be to combine the cutoff date with a review of old stored information as new cases develop. Where data from the old is relevant, it could then be put into the computer.

One point to be kept in mind is that because of the enhanced capability of the computer to handle, collate, and associate bits of information, the unit can handle (and will want) more information per investigation, activity, or suspected person. The use to be made of a more extensive flow of information in developing patterns of organized crime and more clearly delineating criminal participants is indicated by figure 19, page 119.

### **THE COMPUTER AND THE INTELLIGENCE PROCESS**

One practical way to examine the manner in which a computer may assist an intelligence unit is to review its application to the several steps in the intelligence process. As will be indicated below, the computer has a role in most of these steps. But as is also pointed out, the operation of the unit with a computer will have to be on a much higher level of sophistication than when it operates with hand "massaged" files. There will be more information available and a greater capability to use the information in the data bank to assist in analysis—in searching for patterns and for interrelationships between items of information of persons and activities. It would be most useful if some, and perhaps most of the members of the unit learn the mysteries of the computer so that they may exploit its capabilities to the fullest. Finally, the unit will have to guard against becoming inundated with printouts (or requests for same) or with request to produce interesting but not very useful sets of figures and correlations.

#### **Collection—Information Flow**

The unit with the computer will be able to handle a much larger flow of information. It can handle this information in a manner that

makes it much more readily available for use in a tactical sense. Investigators can request a printout of most recent information (tactical intelligence) and have it correlated with filed information without having to pull a series of hard copy reports and perform a time-consuming hand collation. Similarly the analyst can, day by day, obtain the assistance of the computer in his efforts to correlate bits of information and develop patterns of activities or organized criminals (strategic intelligence).

One decision that will have to be made is whether the totality of the remarks on a report, an electronic surveillance, or a court record will be inserted in the computer, be abstracted, or only be given as a source, with a referral to the complete report being held in its hard copy form. How this problem is resolved will have to be determined by each unit on the basis of its computer capacity, punchcard operators availability, potential developments in the organized crime threat, etc. Experience of other units should be sought on this problem, especially units of roughly comparable size and level of organized crime problem.

It will be essential that all data filed be coded for sensitivity. (See chapter II for a discussion of this problem.) Unless this is done there will be no way of separating sensitive from nonsensitive material when printouts are made of data in the computer. Since not each element of intelligence information has the same degree of sensitivity, it will be essential to have some system of classification, some system by which data inputs are given a sensitivity rating when they are put into the computer. While the bulk of information may not be considered sensitive, at least within the intelligence office, consideration must be given to its potential circulation to others. If it is not protected by code, the computer, when asked for all information on a person or subject, will put it on a printout that could become a serious breach of security or of privacy.

Equally important is the requirement that information put into the intelligence file be evaluated as to accuracy of the reporter and of the substance and that this evaluation be coded and attached to the data location. Once data is inserted into the computer it is time consuming to recall and develop an evaluation. But it must be evaluated either before or after or when

printed out all data will appear to have equal validity.

### Collation

The computer adds many dimensions to the collation potential. Through the use of appropriate coding of the bits of information as they are filed they can be associated with other bits of a similar nature and through programing associated with other types of information to present aggregations that can be used in turn to develop patterns, associations, and trends.

The most important area of improvement will be in cross-indexing. A single report from an investigator that contains information on several different persons, locations, and activities can be broken up and inputted in a manner which associates them with others of similar nature. The names can be checked to see if they are already on file. Similarly the locations can be checked. Notation that they were seen more than once in a particular location can be put in as a summary. The fact that the person was seen performing a similar (or different) activity can be recorded. But the point is that each separate bit of information is filed under its appropriate category. Unlike the hard copy or the index card, the subsequent user of the information in the computer does not have to bring out the hard copy with all the original information on it—some applicable and some not. Furthermore, the information can be gained from the computer in several ways, that is, by asking several different questions. It can be asked for by the name of the person, by the activity, or by the location. It should also be noted that with a computer there is no danger that someone will inadvertently walk off with a hard copy of a report and thus create a hole in the files.

Of course all of the above will not happen automatically. There must be a program written that will file the inputs in their correct location and will have them come out again, either as a unique piece of data or in proper association with like or associated bits of data. The unit must obtain the service of a programmer—as a new hire of a permanent employee, by training one of their own men, or by turning to a computer software company on a contract basis. Programing and file maintenance are not a one-time thing. As information begins to accumulate on a new area it may have some

significance for other files already in the computer. The programmer must come to understand the problem and develop the requisite instructions to give the computer so it will associate the new and on-file information and to give it back in the format most useful to the analysts and investigators.

## Analysis

The computer can offer great assistance to the analyst also. Through programming and through coding bits of information that are inserted into the data bank, the computer can do basic associations and correlations that the analyst, without the computer, must do himself laboriously (and may in fact overlook).

In particular, the computerized files will help in the development of new patterns and areas of operation by the organized criminals. In areas where they have already been operating but are enlarging their sphere of activity the computer can be called upon to associate MO's with people, with types of activities, with areas of operations, etc. Figure 19 which follows depicts a hypothetical file on hijacking. It is designed as an example of a data base that can be constructed and be made available relatively easily by using the computer. In new areas, the exploration of a particular function, such as laundries or sales of a new product such as detergents, or of new activities such as penetration of a union or theft and sale of securities, the data base describing the functional area of activity can be developed through programming the structure of new information to be placed in the computer (and the association of pertinent data already in the computer). Subsequently, as names and associations and activities are reported, they can be tested against the organized data in the file.

Figure 19 attempts to demonstrate the breadth and depth of information that can and should be available to the analyst on an area of organized crime. It also shows how, through programming, the basic data can be organized. The elements shown in capital letters on the first page of figure 19 are in a direct sense the totals and sub-totals. The data from the files when totaled in this manner can tell the questioner how much of a particular class of materials has been hijacked in a particular period, where, by what group (if known), what was the modus operandi used, the

value, etc. This is the raw material for developing hypotheses on how a particular group of criminals are operating and may indicate new areas where they might attempt their next strike.

The information on the right-hand side of the second and third pages of figure 19 is the input data. It would be highly desirable if the unit developed formatted pages to be used by the investigator or debriefer. These formatted pages would list the questions to be asked and would insure that the subject was covered and the desired information obtained. The questions themselves can be coded on the form which will assist the operator to input the information into the computer data bank.

Finally, by having the information organized to respond to predetermined or programmed questions, the analyst is aided in his probing the subject of hijacking—where is the point of focus in terms of goods, locale of action, methods, persons or groups involved, companies being hijacked, and how the stolen goods are ultimately disposed of.

## Security

Computer security means, first, protection of the data file against access by persons who are unauthorized, and second, the protection of the files against destruction and unauthorized inputs. It presents the same problem as the file drawers in the file room. But the problem is usually more complicated because of location, and what frequently the simultaneous use of the computer by other elements of the agency. The problem is often further complicated because the computer may be part of a system which includes consoles with input and retrieval capabilities sited at distant locations.

Computer technology has progressed to the point where it is presently feasible to design a computer system so that multiple users can concurrently access a common data base. In such a system each individual user can get only the information that he is allowed to see and any information entering the system is safeguarded from public disclosure. However, the degree of security will often be a result of the amount of funds available. The system designers must determine the value of the information and design safeguards that are commensurate with that value. In the paragraphs that follow, con-

FIGURE 19

EXAMPLE-SUMMARY PRINTOUT CATEGORIES AND INPUT INFORMATION

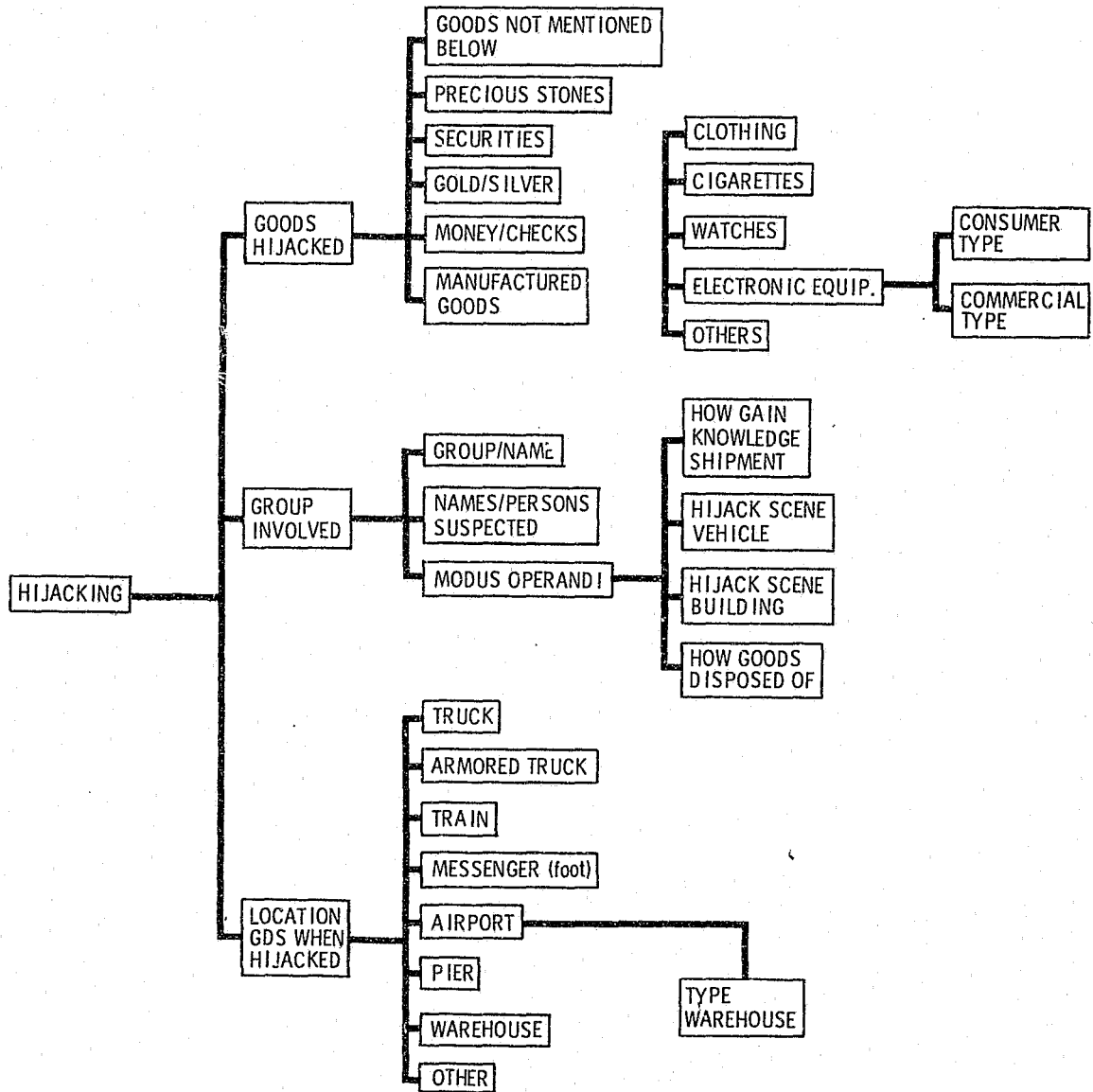


FIGURE 19 (continued)

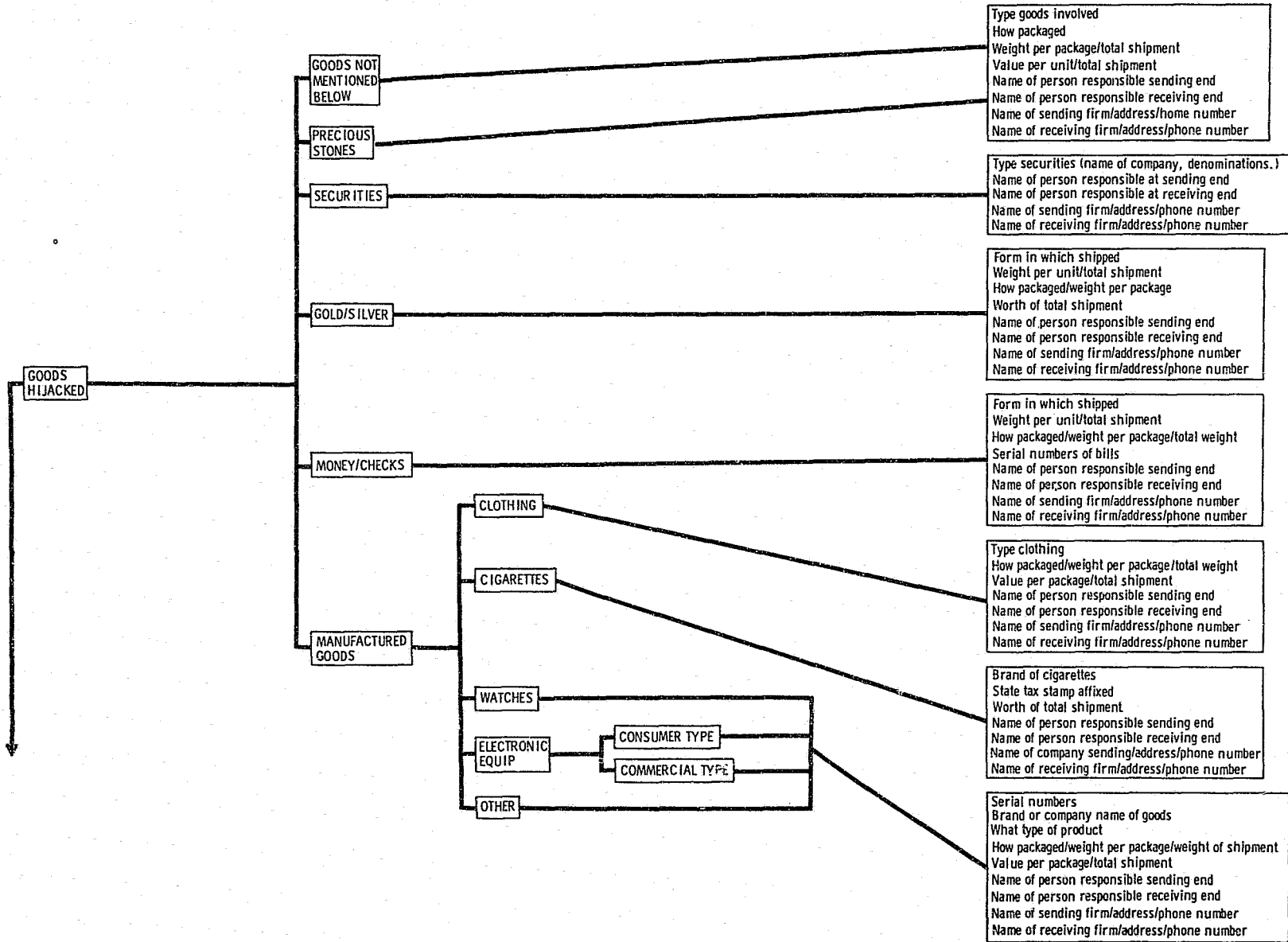
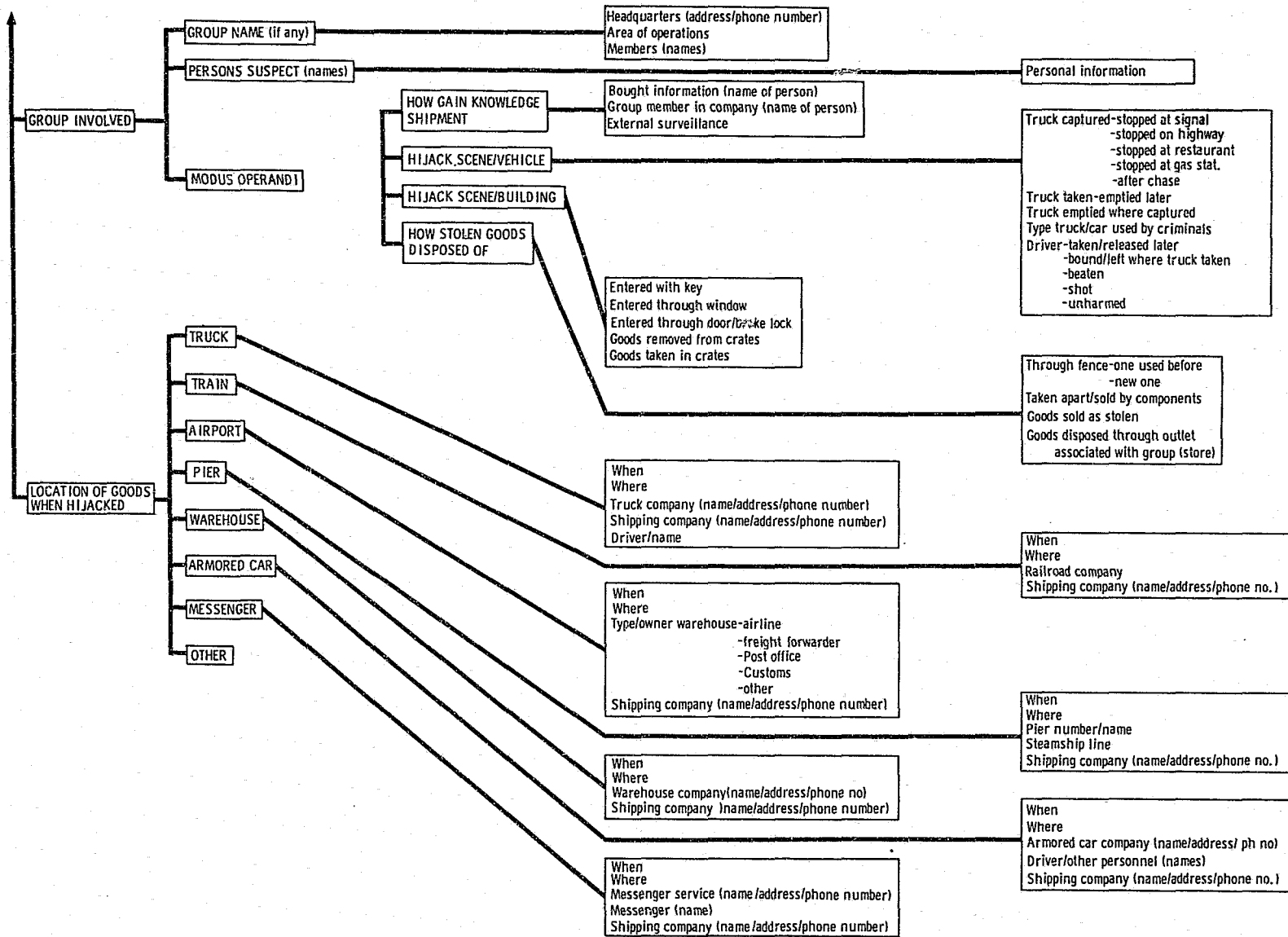


FIGURE 19 (continued)



sideration is given to the various areas the system designers should consider in developing security for a particular computer installation.

#### *Physical site*

The computer facility should be physically protected from intruders. This may involve no more than a guard at the door; it can also involve guards and double-locking doors with a TV camera in between. In the latter system the persons desiring entrance are held between two locked doors while they are identified by means of recognition over the TV circuit. The computer should also be located below the ground floor. This will prevent unauthorized persons from entering through windows and will also help alleviate electromagnetic radiation problems.

#### *Personnel*

All personnel associated with the operation and maintenance of the computer facility should be investigated. Ideally this will have already been done for any intelligence unit personnel involved. Since it will probably not be possible to give all personnel the rigorous check that the intelligence officers receive, it is essential that the unit have its own personnel in the facility at all times to protect its files from possible misuses by unauthorized persons. However, if it is impossible to have intelligence personnel in the computer facility at all times (that is all times when it is in operation) then every effort should be made to have intelligence tapes and disks locked up. This is possible if these files are not to be operated on an on-line basis.

With respect to security problems with com-

puter room personnel, there are several areas to be watched. A dishonest systems analyst can modify the software to enable specific users to program around security measures. A dishonest computer operator can copy a tape or reprint a listing. A bribed maintenance man can change the logic of the hardware so that a certain sequence of instructions will bypass the hardware protection. All of these types of security violations are difficult if not impossible to discover. The best way to foil the dishonest employee is to carefully review all system modifications after they are performed and to insist that the employees work in pairs.

#### *Security of the information in the computer data banks*

Security of the computer's data bank and of its operation is a complex matter and should be the subject on which help is sought from experts. The problems multiply in circumstances where the intelligence unit is sharing a computer with another element of its agency or another element of the government of the jurisdiction in which it is located. These are also increased where the decision is made to give outstation terminals the right to input and to request data directly from the data bank.

The cost of security should be taken into account when studies are first being made whether the unit is to switch to the computer. Costs will be involved in developing security programs, initially to control the input and output procedures including necessary control codes for permitting entry into the data bank, and in computer time as they check on the functioning of the security programs during operations.

## Appendix C

# SAMPLE DEBRIEF FORM AND LIST OF SELECTED SPECIFIC QUESTIONS

### INTELLIGENCE REPORT--DEBRIEF

Name of debriefer \_\_\_\_\_ Date and time \_\_\_\_\_

Name of officer or other person debriefed \_\_\_\_\_

Reason for debriefing \_\_\_\_\_

General questions to be answered:

Where did the event occur? \_\_\_\_\_

When did the event occur? Date \_\_\_\_\_ Time \_\_\_\_\_

Weather Conditions (if important) \_\_\_\_\_

What was apparent cause of the event? \_\_\_\_\_

Who was involved in the event? \_\_\_\_\_

Were there any unusual circumstances connected with the event? \_\_\_\_\_

#### Specific Questions To Be Answered

The questions asked relating to the specifics of the event, for example the modus operandi if it were a hijacking or loan sharking, should be directed to gaining all knowledge the person debriefed perceived at the time of the event (or knows about from other experiences). The debriefer should prepare a list of questions to this end before he meets with the person to be debriefed. An intelligence unit can develop a series of standardized questions relating to specific crimes, adding to them as events and successive debriefing indicate.

Attached are a series of questions that indicate

how the above suggested standard lists of questions might be started. They are drawn from a list prepared by Vincent Piersante, Michigan State Police.

#### SUGGESTED SPECIFIC QUESTIONS BY CRIMINAL ACTIVITY

##### *Corruption*

1. Are you aware of the acceptance or the offering of any gratuities or bribes for illegal or improper services rendered by:

- a. Law enforcement officers
- b. Attorneys
- c. Other public officials



2. Do you know of any prosecutions being "fixed" or dropped due to illegal agreements or activities by involved officials?

3. Have you ever observed a public official in the company of a known racketeer?

4. Do you know of any places that are hang-outs for known racketeers which are regularly frequented by public officials or police officers?

5. Do you know any payoff men?

6. Who handles payoffs for:

- a. Gambling
- b. Prostitution
- c. Narcotics
- d. Court Fixes

7. Do you know any hoodlums or racketeers who contribute to political campaigns?

a. Who, when and how much

#### *Firearms violations*

1. Do you have any information regarding racketeers or hoodlums who are known to travel with a gun on their person or in their luggage?

2. Do you have any information regarding the collection of guns by hoodlums and racketeers—any machine guns?

3. Do you have any information regarding any racketeers traveling out of State to purchase guns?

4. Do you know of any racketeers traveling on hunting or vacation trips where they are armed? If so, who, when, where and so forth.

5. Do you know anyone who keeps or stores weapons for the organization or its members?

#### *Gambling*

1. Do you know of anyone engaging in:

- a. Off-track betting (bookmaking)
- b. Numbers or policy
- c. Sporting events gambling
- d. In-house games of chance (this is intended for information and refers to barbuti, dice or poker games that are being cut by the operator for profit)

2. Do you know where one can:

- a. Place a bet
- b. Buy a number
- c. Buy a gambling ticket on a sporting event

3. Do you know the location of any book-making operation?

4. The names of those people operating the book.

5. Do you know of any persons engaging in or the methods used to transfer monies to a bank or drop point?

6. Do you know the location of the bank (be specific including a description of the physical layout, lookouts if any, and methods of entry)?

7. Do you know the number or types of vehicles used in these operations?

8. Do you participate in any type of gambling?

9. Could you introduce an undercover agent?

10. Do you have any knowledge relating to the transportation of gambling paraphernalia? (as bet pads, tip sheets, almanacs)

11. Do you know how the paraphernalia is shipped and from where?

12. Do you know of any wagering business which makes use of a wire communication facility including telephones? If so, were any of these communications interstate in nature?

13. Do you know any layoff men or set ups?

#### *Hijacking*

1. Do you have any information about any hijacking operation?

2. Do you know of any thefts from intrastate or interstate shipments?

3. If so:

- a. When did these thefts occur?
- b. From where was the merchandise taken (Acquire the name of the terminal, warehouse or platform where the theft may have occurred)
- c. Who are the persons responsible for the theft? (Complete description and vehicles driven)
- d. From what type of vehicle are thefts occurring?
  - (1) Trains
  - (2) Trucks
  - (3) Aircraft

4. Where is stolen merchandise being stored? (Get as complete a description of the physical layout as possible)

5. How is the merchandise sold or disposed of?

- a. Through a fence
- b. Direct to friends and associates
- c. Shipped out for disposal elsewhere

6. Do you know the location of any stolen goods either being stored or already sold?

## Labor

The following are areas to be explored which may develop information of the violations of the Taft-Hartley Act, the Labor-Management Disclosure Act, the Welfare and Pension Plan Act, as well as the Hobbs Act:

1. Employer or employer-representative payments to union officials;
2. Withholding dues from pay or employees and remittance to a union without written authorization from employees concerned;
3. Employer payment of dues from his own assets, that is, dues not checked off from employee's wages subject to written authorization;
4. Union officials with direct or hidden interests in companies employing members of that union or in companies which do business with the union;
5. Employers making purchases from union officials of articles and commodities at inflated prices;
6. Union officials failing to enforce contract terms with some employers;
7. Failure of union officials to process grievances of their members against certain employers;
8. Failure of unions to pursue organizational efforts relative to some employers in an industry that is generally organized;
9. Union officials permitting certain employers to pay less than union scale;
10. Union officials permitting certain employers to use less than the required working force on the job;
11. Union officials permitting employers to work employees in other than their own craft jurisdiction;
12. Known association of union officials with suspect individuals;
13. Direct or indirect control of unions by target or suspect person;
14. Shakedown of union member by union officials for job placement;
15. Cash collection of dues, initiation fees or service fees by union representatives from transient workers who may not be members of the union or only temporarily associated with the union;
16. Existence of fictitious employees on employer's payroll;

17. Nonworking and "no-show" union personnel on employer's payroll;
18. Union control of contract awards to companies, suggestive of collusive bidding arrangements;
19. Inducing employers to make political contributions;
20. Union contributions to candidates for Federal office;
21. Questionable loans made by union welfare and pension trusts to suspect initiates;
22. Evidence of kickbacks on loan arrangements from union welfare and pension plans;
23. Improper diversion or embezzlement of union funds;
24. Application of force or violence or the threat of such, against union members to deprive them of any of their rights as members;
25. Use of violence or threats against employers or firms being organized to gain a contract or to enforce improper terms;
26. Evidence of falsified information regarding financial reports required to be submitted by unions and welfare and pension plans;
27. Frequent changing of carriers of insurance in connection with pensions or welfare plans, suggestive of kickback arrangements on initial premiums.

## *Legitimate business*

1. Do you have any knowledge of any hoodlum or racketeer in a legitimate business either:
  - a. Owning the business directly
  - b. Owning the business through a "front" man
  - c. In partnership—openly or hidden
  - d. Managing the business
  - e. Operating the business
2. What specific business or businesses?
3. What are the locations of these businesses?
4. Are any of these businesses fronts for some form of illegal activity?
5. Approximately how many employees in each of the businesses?
6. Are any of the employees hoodlums or racketeers?
7. Do you know of any hoodlums or racketeers that are on the payrolls who do not work in the specific business?
8. Do you know of any tax violations occurring within a particular business?

- a. Not declaring all income
  - b. Failure to pay proper revenues for employees
  - c. Writing off personal expenditures as business expenses
9. Do you know of any falsification of other required reports to Federal, State, or local governments:
- a. Annual reports
  - b. Corporation reports
10. Do you know of anyone who has effected or tried to effect the operation of any business through the use of force, violence, robbery or extortion or threatened use thereof?
11. Do you know of any business establishments requiring a liquor license being operated by a front man and owned by a racketeer?
12. Do you know of any mob-connected taverns which acquire their liquor supplies from other than State licensed outlets?
13. Do you know of any business being operated by a hoodlum or racketeer that was acquired through loan shark payments?
14. Do you know the source of supplies and services for racketeer owned or operated businesses?

#### *Loan sharking*

- 1. Do you know of anyone involved in loan sharking, either as a lender or a victim?
- 2. If so, obtain:
  - a. Who is the loan shark
  - b. Who does he work for?
  - c. Who is the victim?
  - d. Who makes collections? (when, where and how)
  - e. What is the amount of the loan?
  - f. What is the rate of interest?
  - g. Have there been any threats of force used or implied, by whom?
  - h. Obtain the background of suspects, their vehicles, and so forth.
  - i. Do you know of any musclemen or collectors for loan sharks?

#### *Mafia-Cosa Nostra syndicate*

- 1. Are you familiar with an organization known as the *Mafia* or the *Cosa Nostra* or the *Syndicate*?
- 2. Do you know anyone who you believe is a member?

- 3. What makes you believe that this individual is a member?
- 4. Identify:
  - a. Occupation
  - b. Residence
  - c. Businesses
  - d. Criminal specialities
  - e. Familial connections
  - f. Criminal associates
  - g. Police and public official connections
- 5. Describe his organizational activities.
- 6. Does he have an in-State or an out-of-State residence?
  - a. How often does he use it?
  - b. What means of travel does he ordinarily use?
    - (1) In-town
    - (2) In-State and out-of-State
    - (3) Does he use a travel agency
    - (4) Does he visit Canada (give details)
- 7. Does he own an airplane or a boat?
- 8. Does he have connections with out-of-State or out-of-country members of the organization or any other criminals?

#### *Murder*

- 1. Do you have any knowledge about any murders being investigated?
- 2. Do you know of any deaths that appear accidental or natural, but were not?
- 3. Do you have any information about missing persons who may be dead?
- 4. Who are the musclemen?
- 5. Who are the enforcers or hit men?
- 6. Who do they work for?

#### *Narcotics*

- 1. Are you aware of any information relating to heroin, cocaine, marihuana, barbituates, amphetamines, or hallucigens?
- 2. Does the subject sell, use, or both?
- 3. What quantity is sold: Kilos, nickel or dime bags, or the number of pills:
- 4. What is the price charged per unit?
- 5. Have you ever purchased from the subject?
- 6. Could you introduce an undercover agent to the subject?
- 7. With whom is the subject associated?
- 8. What is the subject's answer of sale and delivery?

- a. Hand to hand
  - b. Use of a front man
  - c. Use of the telephone in the transaction
  - d. Subject acts as a middleman
9. What out-of-town associates does the subject have?
    10. Who is the subject's source of supply?
    11. Does subject have any prior arrests?
    12. Where does subject keep his supply of narcotics?
  13. Obtain from the source any information relative to subject's description, vehicle, residence, telephone number, etc.
  14. Are you aware of any members the medical profession, doctors or druggists, involved in the distribution of narcotics or drugs?

#### *Pornography*

1. Do you have any information about the manufacture, distribution, or sale of any pornographic material:
  - a. Motion picture films
  - b. Photographs
  - c. Books, pamphlets, or other printed material
2. Where is this material kept or stored?
3. What form of distribution is used:
  - a. Through fronts (as retail outlets)
  - b. The U.S. mail
  - c. Street men
4. Who are the people who handle sale and distribution of pornographic material?

5. Do you know the prices of the various types of pornographic material?
6. Where is the pornographic material manufactured?
  - a. A professional studio during off hours
  - b. Someone's home
  - c. Other types of buildings
  - d. Locations for outdoor shooting
7. What is the location of the studios in the case of films?
  - a. A professional studio during off hours
  - b. Someone's home
  - c. Other types of buildings
  - d. Locations for outdoor shooting
8. At what time of the day or night does the photographing take place?
9. What are the types of cameras or other equipment used?
10. Who are the models who pose for pornographic films? (get specifics as to description, age, address, and vehicles used)

11. Do you know of any regular customers of pornographic material?
12. Could you make a purchase of pornographic material or acquire samples as if for future sales?

#### *Prostitution*

1. Do you know the location of any houses of prostitution?
  - a. Who is the madame?
  - b. How many girls are in the house?
  - c. What is the cost?
2. Do you know any pimps?
3. Have you ever acquired the services of prostitutes for business purposes?

## Appendix D

# GUIDELINES: OPERATION OF AN INTELLIGENCE UNIT

### I. THE INTELLIGENCE PROCESS

*The intelligence process* is a continuous series of interrelated activities directed toward converting raw information into informed judgments. The products of each step in the process—collection of information, evaluation, collation, analysis, reporting, dissemination, and reevaluation—are essential ingredients of the end product, the intelligence report.

#### A. Collection of information

1. Collection of information must be carefully planned.
  - a. The collection effort by the intelligence unit should be directed against a specific target.
  - b. The collection system with the best chance of success should be given the primary responsibility for the task.
  - c. Collection efforts must be coordinated so as to avoid duplication.
  - d. Collection should be directed at gaps in the information; there is no need to prove a fact more than once.
  - e. Collection progress should be reviewed by the analyst at different phases of the investigation effort. In the early stages information can be general and indicative; in the latter stages precise evidence is needed.
2. The means of collecting information may be overt or covert.
  - a. Overt collection
    - (1) The *investigators* assigned to the

intelligence unit are an effective overt collection source.

- (a) The investigator develops the indications of criminal activity contained in information collected from one or more general sources.
  - (b) He checks the validity of reports obtained from informers.
  - (c) He works with the analyst to sharpen the target as the investigation progresses from a "looking into the situation," to the compilation of a study in depth, to a gathering of evidence.
  - (d) Throughout the investigation, he should promptly record his findings on suitable report forms.
- (2) *Information from nonintelligence units of the law enforcement agency*
- (a) The agency head must require that any information relating to organized crime, including gambling, narcotics, prostitution, usury, be passed on to the intelligence unit.
  - (b) All elements of law enforcement agencies—patrolmen, patrol cars, detectives, desk sergeants, etc.—should be encouraged to report to the intelligence unit any activity that relates to organized crime.
    - (i) Patrol units, where appro-

appropriate, should be assigned to note any activity around residences and businesses of major criminals in their area.

- (ii) They should report their findings on a special intelligence report form. (See Intelligence Manual, p. 17 for sample form.)
  - (iii) When appropriate, a representative from the intelligence unit should request specific help from other elements of agency and where indicated the personnel directly involved should be debriefed. (See appendix C of the Intelligence Manual for sample debrief form.)
  - (vi) All intelligence reports from other elements of the agency should be routed directly to the intelligence unit, although supervisors should be informed.
  - (v) The intelligence unit should press for time in the various training courses to describe the role of intelligence against organized crime.
- (3) Information from *other jurisdictions*
- (a) Because organized crime often operates beyond the city limits, the agency head should, if possible, establish relations with authorities in surrounding suburbs and in neighboring cities.
  - (b) Appointment of a liaison officer is frequently useful in expediting and controlling the transmission of data between different agencies.
- (4) Information from *sources other than law enforcement agencies*

(a) *Newspapers and articles* in journals should be examined for information on actions of members of organized crime both in and out of the agency's jurisdiction.

(i) Articles from newspapers and other periodicals can be clipped, filed, and cross-referenced, either by a member of the intelligence unit or a clipping service.

(ii) Abstracting articles<sup>4</sup> and journals should be considered as an alternative method.

(b) *Public records and documents*, such as trial records, grand jury commission hearings, and investigative hearings by state and federal legislators, are excellent sources of data, though usually they provide indicators rather than hard intelligence or evidentiary material.

(c) *Financial centers*—local stores, bonding houses, banks, insurance companies, telephone companies—can formally or informally provide useful leads. But privacy considerations and state and local laws must be kept in mind. (See appendix A "Intelligence and the Law," in the Intelligence Manual.)

(d) *Complaints*. Information is often revealed by a citizen voluntarily, but his report should be carefully checked out by the intelligence unit before it is accepted.

b. *Covert collection* is the acquisition of information from a subject who is unaware he is being observed or overheard. Its use is essential if successful prosecution of leaders of organized crime is to be achieved, but it is expensive in terms of manpower.

(1) *Physical surveillance*—observation of movements of suspects without

their knowledge—is most effective when used as a supplement to other types of covert collection. Although physical surveillance can lead to information on a suspect's associates, the places he visits, and his activities, this is not necessarily a useful technique for determining the purposes of a suspect's movements and the topics he is discussing.

(2) *Electronic surveillance* — where, legal, the use of electronic surveillance devices enables an intelligence unit to acquire evidence of a direct relationship between a crime leader and an illegal act.

(a) Organized crime leaders are becoming increasingly sophisticated. Methods and equipment must be adopted to these new circumstances.

(b) The material gathered should be carefully processed, preferably by specially trained personnel.

(c) Leads and indications beyond the case under investigation should be exploited, where this is legally defensible.

(d) The actual operation of electronic surveillance gear turned over to experts.

(3) *Informers*, individuals outside the police organization who are familiar with the operations of organized crime, are often a valuable source of information.

(a) Effective exploitation of an informer requires that the informer be convinced that his contact in the agency *always* deals with him honestly and discreetly.

(b) Money, the usual payoff demanded by informers, raises serious problems for many agencies.

(i) A fund for such purposes must be approved by the

political body which provides the agency with funds.

(ii) Safeguards against misuse of the funds, such as receipts, or the presence of an observer during the transaction, are highly desirable; if the informer will not agree, the risks of ignoring safeguards must be weighed against the value of the information likely to be obtained.

(c) "Management" of informers is an important aspect of an intelligence unit's duties.

(i) It is insufficient that only the individual investigator know the identity of "his" informer. A more systematic and desirable approach is the establishment of a central registry of the names of informers, handled with the utmost security and in which more than one officer may evaluate the worth of the informer.

(ii) Consideration should be given to upgrading informers by a judicious feedback of information which will help them to be promoted within their criminal organization. This obviously is a tactic which is both difficult and dangerous.

(4) *Undercover agents* are law enforcement officers who usually operate clandestinely on the fringes of an organized criminal group.

(a) To be effective the agent must have funds immediately available for entertaining, purchasing stolen goods, and drugs, gambling, etc.

(b) He also can be more effective if wired for sound, but the risks

involved must be carefully considered.

B. *Evaluation of intelligence* inputs is an essential part of the production of intelligence.

1. The validity of any report must be judged by the commander on the basis of the reliability of the reporter, as well as the substantive credibility of the report.
2. The commander (or his designated subordinate) should:
  - a. Seek to verify facts in the report by comparing them with other information.
  - b. Decide which leads in a report should be followed up.
  - c. Grade the worth of the reporter.
  - d. Before it is filed, mark on each report his evaluation of the reliability of both its substance and the reporter so that it can be of use for future reference.

C. *Collation*. Collation must be thought of as more than the simple storage of materials in files. It includes the sifting out of useless or irrelevant or incorrect information, the orderly arrangement of collected materials so that relationships between apparently disconnected data may be established, and a system for rapid retrieval of stored information created.

1. A *filing system* should provide for the quick retrieval of information on any one human subject or on a general area of criminal activity or on illicit businesses, phone numbers, licenses, etc. An extensive system of cross-reference and cross-indexing should be set up to allow pertinent material to be referred to under more than one category.
2. A *coding system* for filing should be adopted. A code, using colors, numbers, and letters either alone or in combination, can be set up to designate functional and activity files. It can then be used to indicate on a multisubject report how its substance has been filed and/or cross-indexed. The codes saves time when compared to using full subject titles and referrals.
3. The use of *mechanical aids*, such as auto-

matic data processing may be essential for larger agencies (see appendix B).

D. *Analysis*—is at the heart of the intelligence system.

1. The analyst must first assemble data, often scattered and incomplete, on the area under investigation
2. From these facts he attempts to develop a logical pattern or an hypothesis explaining the operation or activity under study. The commander of the intelligence unit reviews the hypothesis. He may have to require further collection, or decide the hypothesis doesn't stand up or to wait for further development.
3. A close working relationship should be maintained between the analyst and investigator so that the investigator can contribute his skills to the collection of specific information needed by the analyst.

E. The end product of the intelligence process is a finished *report*. It may be prepared in written or oral form. It may be quite brief, for example, a summary of the suspicious activities of a tavern owner to be given to the precinct commander where the tavern is located. It may be quite complex; i.e. a collection of documents prepared specifically for the highest consumer, the agency head or the prosecutor.

1. The report must be tailored to the needs of its principal recipients, the head of the agency or the prosecutor, or the enforcement elements of the agency.
2. It must be objective and dispassionately presented so that the decisionmaker can act on the basis of accurate information and sound analysis.
3. It must be structured so that the findings are described logically and concisely.
4. It must clearly separate positive information from hypotheses and inferences.

F. Dissemination of the intelligence report should primarily be the responsibility of the unit head.

1. The head of the agency must receive an intelligence report directly (or at least intact) to insure that he is fully informed



and that the message contained in the report is not distorted by opinions of other readers through whom it has passed.

2. Other recipients both inside and outside the agency should be selected on the basis of their need to know and the purpose of the report.
3. Security is important—especially in transmitting sensitive information or hypothetical analyses—but should not be the decisive factor in dissemination.

G. *Reevaluation*: The unit commander must continuously review each operation of the process so that he can detect weak points before they become major problems.

1. The commander must evaluate the quality of reporting, the collection system, and analysis (particularly in identifying new areas of criminal operations).
2. He must arrange for feedback from the agency head and other consumers on how useful the intelligence is.
3. He must develop tests to measure the effectiveness of the unit—its ability to produce quick analyses, to detect incipient criminal operations, to point out legitimate businesses which the syndicate may be beginning to penetrate.

## II. THE STRUCTURE OF AN INTELLIGENCE UNIT

A. The relationship of the unit to other components of the agency.

1. Traditionally the intelligence unit in law enforcement agencies has been looked upon as a clearinghouse or reference point primarily of use to the field investigator in developing his casework. This concept should be abandoned in favor of a two-directional unit that provides "strategic intelligence" to the agency head or prosecutor and "tactical intelligence" to the field investigator.
2. The intelligence unit should not be a part of the enforcement mechanism; it should not itself be operational. However, it cannot and should not stand apart and aside from enforcement responsibility.

a. It should examine—at the agency head's request, major pending enforcement tactical moves.

- (1) It should make available to the tactical planners all intelligence that might contribute to the success of the operation.
- (2) It should interpret the reliability of information being used by the tactical planners.
- (3) Where appropriate, it should appraise the potential value of the planned enforcement action.

b. The unit commander should make arrangements to exploit any intelligence collection opportunities during the operation itself.

B. Location of the intelligence unit.

1. The intelligence unit should be a staff organization. It should be insulated as much as possible from day-to-day police functions so that it can stick to its intelligence mission.

2. The unit should be directly responsible to the agency head.

a. The unit must be positioned to contribute to the decisionmaking responsibilities of the head.

b. The unit commander must make himself aware of the agency head's needs and tailor the unit's activities and his own reports accordingly.

c. Finished intelligence from the unit should be passed directly to the agency head to avoid the "filtering effect" of intermediate recipients.

d. The head must be immediately and directly informed of any internal corruption uncovered by intelligence collection.

C. The shape of the intelligence unit.

1. Each step in the process of intelligence should be considered and understood as a distinct activity, but the office should be so structured that a smooth continuing flow from one step to another is maintained.

2. Incoming information and reports must

be received at a central point and logged as a matter of course.

3. An information control system must be set up to insure the unit of solid professional standards. It must:
  - a. Route information to analysts within the unit who might find it useful.
  - b. File documents returned to the analysts for storage.
  - c. Protect sensitive materials from unauthorized circulation outside the intelligence unit.
    - (1) The section must see that sensitive documents go only to appropriate recipients and that receipts from outside recipients are obtained and recorded.
    - (2) It must record evaluative judgments on reports, carry through on purging the files of what has proven to be fallacious matter.
4. The principal substantive work of the unit will be done by investigators and analysts; if the unit is large enough these functions can be grouped in sections.
  - a. The analysts and the investigators should be encouraged to work together as a team under the supervision of the unit commander.
  - b. Where needed, specialists (economists, attorneys, sociologists, etc.) should supplement regular personnel.
  - c. Adequate clerical support should be provided.

D. The intelligence unit command.

1. The unit commander should:
  - a. Monitor all parts of the intelligence process.
  - b. Evaluate the products of the teams of analysts and investigators and decide which products should be pushed further.
  - c. Decide to whom all finished intelligence should be sent—and to whom it should *not* be sent.
  - d. Regularly report to the agency head on all intelligence developments in organized crime.

2. The unit commander should have the responsibility for intra-agency intelligence relations and in this role he should:
  - a. Ensure that all enforcement elements know what the intelligence unit is looking for, encourage all elements of the agency to pass along information and provide them with a simple reporting system.
3. The commander must establish contacts with those external agencies that may be valuable in terms of exchanging information and coordinating strategy.

### III. STAFFING THE INTELLIGENCE UNIT

- A. Three criteria should be applied to the selection of all levels of the staff: integrity, capability and personality.
- B. The most important personnel selection is that of the unit commander.
  1. He must not only be himself a symbol of incorruptability; he must also instill in his unit a sense of pride in the organization's integrity.
  2. He must be able to amalgamate the work of different types of subordinates.
  3. He must have a lively curiosity and imagination.
  4. He must have organizational ability.
- C. Ideally the unit should be autonomous, outside the local civil service system, with full hiring and firing powers vested in the agency head.
- D. Candidates for both analyst and investigator jobs should be personally interviewed and should be given appropriate testing.
- E. Analysts can be either nonspecialists or specialists.
  1. The nonspecialists (those who prepare reports, make appraisals, develop filing systems, etc.) should be selected on the basis of their intelligence, precision, and motivation rather than on their experience.
  2. Specialists with advanced training, such as accountants, lawyers, economists, should be used to meet specific needs, temporarily or on a long-term basis.

F. Investigators normally should be transferred into the unit from the detective branch.

1. They should be experienced.
2. They must be able to work in harness with the analyst—even to the extent of interchanging some functions.
3. They must be able to accept direction but also be capable of taking initiative.
4. They must be factually accurate in reporting, and in addition capable of analysis and interpretation.

G. Special problems may accompany the management of intelligence personnel.

1. In some jurisdictions because of the presence of both "badged" officers and civilians in the same office, the commander must work out special arrangements to enable these two groups to work together.
2. Because intelligence personnel rarely enjoy concrete recognition of their accomplishments, he must, in order to maintain morale:
  - a. Personally keep unit members informed of how and for what their product is being used.
  - b. Push hard for promotions.
  - c. Vary assignments within the unit and seek temporary or rotational assignments outside the intelligence unit.
  - d. Directly and aggressively correct any imbalance between compensation levels of "badged" officers and civil service analysts.

#### IV. TRAINING AND INTELLIGENCE

A. Intelligence training programs for the general patrol force, or non-intelligence officer.

1. The training courses should clear away mysteries surrounding the concept of intelligence. Non-intelligence officers should be taught generally what the intelligence process is. They need *not* know the specifics of individual cases.
2. The contributions that non-intelligence officers, particularly those on patrol duty, can make to the final product of an intelligence agency should be explained.

They should be made aware that a good observer and a good reporter can be invaluable source of information.

3. Several hours of the training program should be devoted to the matter of organized crime—its complexity and its sophistication.
4. The patrolman should be instructed on where and how he can gain access of the intelligence unit.
5. A lecture should be given on the policy-making function of the agency head and how this relates to intelligence.

B. Intelligence training programs for the intelligence officer.

1. The primary emphasis in this course should be placed on analytic techniques.
2. The course should start with an exploration of the intelligence process.
  - a. Emphasis should be made to explain the difference between the intelligence function and the operational function.
  - b. The different categories of intelligence and their primary uses should be covered. The categories are indicative or warning, tactical, strategic and evidential.
3. The need for intelligence by the strategists of the agency should be stressed, but at the same time it must be made clear that intelligence is a contribution to strategy, not a determinant of strategy.
4. The status of organized crime in the particular locality should be thoroughly covered:
  - a. The range of activities of organized crime, including its involvement in legitimate business.
  - b. The susceptibility of the law enforcement agency to penetration.
  - c. The common misconception that organized crime is always ethnically (or family) based must be dispelled.

C. The command level.

1. What intelligence can do for the command level should be the basic theme.
2. The training program should emphasize:

- a. The normal use of intelligence by policymakers.
  - b. The methodology employed in the intelligence process and particularly the latest analytical techniques.
  - c. The responsibility of the command level for quality control of finished products for policymakers.
3. Other themes may include.
- a. New developments in collection techniques.
  - b. Managing the intelligence process.
  - c. Court decisions and intelligence limitations.
4. The techniques used in the training course should be carefully selected. Unless the training officer is thoroughly familiar with sophisticated methods, such as "war gaming," he should stick to traditional approaches, such as seminars and written exercises.

## V. SECURITY AND THE INTELLIGENCE PROCESS

- A. Security is a particular concern of the intelligence unit because of the sensitivity of the subject matter in the unit's file and the attractiveness of the unit to organized crime as a target of penetration or corruption.
- B. To protect the integrity of the intelligence unit its commander must take appropriate steps in three areas:
- 1. *Personal security.* To insure the trustworthiness of an individual, the unit should
    - a. Conduct a background investigation on both professional and personal aspects of a candidate's life, including his financial status and his associates.
    - b. Conduct periodic updates of the background investigations of the unit's members.
    - c. Indoctrinate new personnel with the importance of security.
    - d. Where legal, the polygraph can be used.
  - 2. *Physical security.* Information on file must be protected against access by any unauthorized persons, by whatever means.

- a. Entrance to the area, occupied by the intelligence unit must be restricted to its own or approved personnel.
    - (1) Barriers must be established to screen all entrants.
    - (2) At night, if no one is on duty, an electronic or mechanical alarm system should be in operation.
  - b. Files containing sensitive material should be placed in a separate area and, preferably, stored in a safe. Other files can be kept in ordinary filing cases if there is no problem with securing the room.
  - c. The unit with a computer must take special measures to protect the computer and its data from penetration or misuse.
    - (1) Access to its consoles must be limited to authorized personnel.
    - (2) Computer programs may be coded to restrict retrieval to those who know the code.
    - (3) The computer should be programmed to refuse direct outstation inputs or retrieval.
    - (4) The computer room must be protected from unauthorized entry which could lead to the damage of the machinery and/or data stored on tapes.
3. *Operational security.* The unit must insure that the activities and plans of both the intelligence investigator and analyst are securely guarded.
- a. Office phones should be checked periodically for wiretaps and electronic eavesdrop devices.
  - b. The investigator should use unmarked and inconspicuous cars.
  - c. Security should be observed in communications between field and office.
    - (1) Telephone calls—preferably from public phones—should be made directly to the intelligence unit, by-passing the agency switchboard.
    - (2) Where radio must be used, the intelligence unit should have a different frequency from the rest of the agency.

(3) On-going operational activities should not be disclosed to other elements of the agency unless absolutely necessary.

C. Security should *not* be an end in itself.

1. The ultimate purpose of determining the reliability of prospective recipients is to pass intelligence to all qualified consumers

inside or outside the agency who have a need to know.

2. Security should not be used to conceal mistakes, corrupt activities or the employment of illegal techniques by members of the unit or agency.

3. Security must maintain the privacy of the information in the files from unauthorized persons.

## Appendix E

# EXAMPLES: STRATEGIC INTELLIGENCE REPORTING

### BOOTLEGGED CIGARETTES

In April 1971, the tax on cigarettes in the Commonwealth of Massachusetts was increased by \$0.04 to \$0.16 per pack. This increase brought Massachusetts level with Connecticut on the per-pack tax for cigarettes. The increase in Massachusetts was part of the Governor's tax program and was expected to raise an additional \$24 million in tax revenue. Connecticut and Massachusetts are now tied for third highest cigarette tax in the country. The actual per-pack tax rates for cigarettes in New England are:

Connecticut .....	\$0.16	New Hampshire:	
Maine .....	.12	Regular and king	\$0.085
Massachusetts .....	.16	100 mm. ....	.09
Rhode Island .....	.13	Vermont .....	.12

*NEOCIS comments:* The tax increases in Massachusetts and Connecticut with the concomitant increases in the total price per pack of cigarettes leads to the projection that organized crime in New England will be attracted to the business of smuggling and distributing bootlegged cigarettes.<sup>2</sup> The tax on cigarettes in all six New England States greatly exceeds that of the two large tobacco producing States of Virginia (\$0.025 per pack) and North Carolina (\$0.02 per pack). Organized crime has both the funds and expertise to conduct large-scale operations in bootlegging cigarettes in New England as they have done in other States. As a result, the expected tax revenue from the increase may not be as great as projected as more and more

Source: New England Organized Crime Intelligence System

<sup>1</sup> The two examples in this appendix came from the New England Organized Crime Intelligence System "Briefs," June 1971.

<sup>2</sup> Italics by author of manual.

untaxed cigarettes are brought north and sold through organized crime controlled distributors, vending machines, and stores.

A front page article in the May 9, 1971, issue of the New York Times reported that New York State Tax Department officers recently estimated the total tax loss (city and State) due to bootlegged cigarettes at \$6.9 million a year. Joseph Carter, assistant director of the Special Investigations Bureau, said he thought a figure of between \$20 and \$30 million annually would be more realistic, while a cigarette wholesalers group estimated a 5-year loss to all States to total \$441 million. The Times article further reported that in New York, a flourishing market, Governor Rockefeller has called for a thorough examination of contraband cigarette traffic. It is noted that the \$0.12 per-pack tax of New York is equalled or exceeded by five of the six New England States.

### ORGANIZED CRIME'S TRAINING SCHOOLS

Source: Task Force Report: Organized Crime, Washington, D.C., 1967

Life, February 12, 1971

Very little has been recorded about the current methods of training employed by various organized crime families for their particular skills. Consequently, one of the targets established in the basic intelligence collection plan of NEOCIS is the identification of organized crime training, instruction, and/or schooling methods and procedures. The task force report identified several methods of training and instruction that have been employed by organized crime members in

the execution of lower class crimes. The report also pointed out that soon there would be no place in the higher levels of organized crime for high school dropouts and that the skills now needed within organized crime do not come "automatically" and are not merely those necessary to "avoid trouble." In connection with this, it is interesting to note that a *LIFE* magazine article, concerning airport theft, reported the accuracy of the "Mob's spotting system" for high-value shipments and then indicated that at John F. Kennedy International Airport in New York, a cargo supervisor had founded a "criminal school for spotters" in which he instructed recruited cargo handlers in what kind of shipments to watch for. Each graduate spotter was then paid \$500 if the theft succeeded. To get the process started, the spotter called a predesignated telephone number and repeated the following code sentence: "I got a party tonight." These successful high-value thefts have included a pouch containing \$320,000 in diamonds and a packet containing \$217,500 cash.

*NEOCIS comments:* The Life article has pointed out that one group of low-level criminals actually received formal schooling in a criminal

skill and, as stated previously, the Task Force Report identified methods of training and instruction employed in the execution of other low-level crimes. However, do we know how the highly skilled organized crime fence learns to "wash," "clean up," or legitimize \$320,000 in diamonds and over \$217,000 cash?

In 1968, a new auto antitheft system was introduced whereby turning off the ignition also locked both steering and transmission. This system has done much to foil the young joyrider. However, the system has done virtually nothing to thwart the professional auto theft rings which pocket approximately \$1 billion a year from their efforts. It takes a safe manufacturing company a year or longer to develop a modern \$8,000 safe, but members of organized burglary rings can take such a safe apart in only an hour's time. There appears little doubt that organized crime is staying on top of the advances of modern security technology.

Organized crime's capabilities, technical advances, and their methods of teaching highly professional criminal skills to syndicate members and associates are areas which should be of interest and concern to all law enforcement agencies.

## Appendix F

# GUIDELINES: BACKGROUND INVESTIGATION OF APPLICANTS— INTELLIGENCE UNIT<sup>1</sup>

### STAFFING BACKGROUND INVESTIGATION

#### I. Introduction

The intelligence unit must maintain an unequaled standard of excellence in its personnel and their performance. The degree of success which the unit enjoys will be limited by the integrity of its employees. The process whereby personnel are selected can, therefore, be regarded as the key to successful law enforcement operations. The most important step in this selection process is the background investigation of applicants for positions with the unit. This investigation is necessary in order to evaluate the qualifications, background, character, and suitability of the applicant in determining its eligibility for a position of public trust. Any doubts as to the applicant's suitability will be resolved in favor of the intelligence unit.

#### II. Responsibility of Personnel Conducting the Investigation

Agency (or intelligence unit) personnel conducting applicant background investigations must be resourceful and attempt to uncover any undesirable qualities an applicant might possess. In order to successfully process an applicant for employment and maintain a high level of professionalism the agent conducting the investigation must keep the following in mind at all times.

<sup>1</sup> The Guidelines presented here are, for the most part, those developed by the Florida Department of Law Enforcement for its use in applicant investigations.

- A. Be deeply motivated and aware of the responsibilities.
- B. Be adept at gathering all facts possible.
- C. Possess a sense of fairness and respect. Report all facts, both for and against.
- D. Evaluate the facts carefully.
- E. Be a good interviewer.
- F. Be tactful, diplomatic and patient.
- G. Put aside personal comparison.
- H. Maintain a professional and moral responsibility to the agency.
  - I. *Review the application*
    1. Determine if all information has been provided. If application needs a clarification or lacks certain data, prepare a memorandum to personnel requesting the additional information.
    2. Determine if any information provided or developed affects the applicant's eligibility for employment.
  - J. *Report Derogatory information to the supervisor immediately.*
    1. Derogatory information should be fully developed.
    2. The reports should reflect unbiased and complete inquiry.
    3. Information should be immediately evaluated to determine whether further investigation is warranted.

NOTE.—The investigator's character, ideals, standards, personality and ability



to understand his fellow man will have a tremendous effect upon the evaluation of background findings.

### III. The Background Investigation

#### A. General

1. Advise the interviewee the position for which the applicant is being considered.
2. Request that all interviews be treated as confidential.
3. Interview the interviewee in private.
4. The interview must be voluntary.
5. The investigation must be impartial and unbiased.
6. Obtain information, don't give it. Avoid character assassination or spreading of rumors.
7. Watch the interviewee for reactions to specific questions.
8. Whenever possible personal contact should be made with the interviewee. Appointments should be made prior to an interview whenever possible. In lieu of personal contact make telephonic inquiries and/or send letters.

#### B. Objectives

1. Determine if an applicant is qualified for employment with the intelligence unit.
2. The following points must be kept in mind throughout the investigation which may predict success or failure in the position.
  - a. Character and reputation
  - b. Loyalty
  - c. Associates and/or relatives
  - d. Qualifications and ability
  - e. Emotional stability
  - f. Social adaptability
  - g. Health

#### C. Areas to investigate

1. *Criminal records*
  - FBI files
  - Agency—DAI files
  - Agency—NCIC files
  - State/motor vehicle/DL files
  - Sheriff and local PD files
  - County judge's office
  - Subversive files

Criminal and civil court records  
Police warrant files  
Other

#### 2. *Personal history* (divorce, marriage, birth, etc.)

Bureau of vital statistics  
Military or draft board records  
Civil courts

#### 3. *Loyalty*

Check membership in organizations  
Professional Associates  
Fellow workers-travelers  
Teachers  
Employer  
Neighbors  
Other

#### 4. *Employment*

Dates of:  
Type of promotions  
Rate of pay  
Description of duties  
Abilities (aptitude and initiative)  
Attendance record  
Recommendations  
Ability to get along with others  
Reason for leaving

#### 5. *Education*

Dates attended  
Any disciplinary action  
IQ rating or testing scores  
Attendance record  
Infirmary at school  
Average grade  
Activities in school  
Standing in class  
Any radical tendencies

#### 6. *Residence and neighborhood investigation*

Emotional stability  
Drinking habits  
Previous residences  
Personality traits, behavior and reputation  
Marital problems  
Spends leisure time  
Ability to budget and live within means.

#### 7. *References*

Personal contacts whenever possible.

8. *Military service*
  - a. There is VA Form 07-3288 obtainable from the VA that will give information about a veteran.
  - b. Provost marshal—record check (give name, branch, and military unit when requesting information.)

9. *Financial status*
  - Ratings (satisfactory, unsatisfactory)
  - Any judgments
  - Debts (banks or loan company)
  - Amount of payments
  - Public records or pending civil action

10. *Health*
  - Family doctor—hospitals—clinics
  - Check neighborhoods

D. *Sources of information*

1. State investigative bodies (es. State police, beverage) Federal investigative bodies (ex. U.S. Justice Department; Treasury Department)
2. County and circuit clerks office, U.S. district court clerk.
3. Probation and parole departments
4. Welfare and health departments
5. Licensing agencies
6. Telephone directory
7. Newspaper files (morgues)
8. Commercial credit bureau
9. Utility companies
10. Chamber of Commerce (Better Business Bureau)
11. Auto clubs
12. Plant and security forces
13. Railroad investigative staff
14. Hospital and medical records (doctors records)
15. Bureau of vital statistics
16. Records bureau of Federal, State, County and City P.D.'s.
17. Selective Service boards—Military service—Veterans Administration.
18. Motor Vehicle records
19. School, college, and instructor records
20. Employment records—fellow workers
21. Associates—relatives

22. Organization memberships (ex. labor, fraternal)
23. Banks
24. Retail businesses
25. Church—baptismal records
26. Neighborhoods
27. Industrial Commission

E. Additional information regarding form used by the applicant investigation unit.

1. *Personal History* (verify)

Birth	Adoption
Marriage	Separation
Divorce	Legal name change
Death	

Review records, ascertain cause of action and adverse publicity.

Source of Information: Other State agencies, bureau of vital statistics, State and county records.

2. *Naturalization* (Verify if applicable)
  - Through immigration and naturalization records or court records. Need date and place of entry; date and place of naturalization and number.
3. Financial investigation (information to be furnished to the credit bureau).
  - a. Applicant's name
  - b. Date and place of birth
  - c. Social security number
  - d. Marital status (name of spouse and DOB)
  - e. Present and past addresses and dates residing there.
  - f. Schools, addresses and dates attended.
  - g. Employment addresses and dates.
  - h. Credit record—debts over \$100.
  - i. Parents name if applicant single
  - j. Credit check to be made in all areas resided in by the applicant or his parents.
4. *Education*
  - a. If letters sent submit release forms with correspondence.
  - b. Personal contact—interview a registrar representative, school officials, instructors and fellow students if possible.

- c. Places to check: Registrar's office; security personnel; dean's office; housing office, judicial affairs office.
5. *Personal references*
- a. Personal contact when possible.
- b. *Letters*
- NOTE.—If derogatory information exists concerning a personal reference, ascertain the association between the applicant and reference. Developed references should be acquired whenever possible.
6. *Relatives*
- a. Obtain information regarding close relatives and associates during the investigation of an applicant.
- b. If derogatory allegations are uncovered, further investigation may be warranted to verify or refute the charges.
7. *Employment*
- a. Verify all employment including any new ones discovered during the investigation. In most cases current employment of an applicant should not be verified until employment by agency is imminent.
- b. Interview supervisors and fellow employees.
- c. If applicant in business for himself, interview competitors.
- d. All unemployment should be accounted for.
8. *Neighborhood*
- a. Personal contact (landlords, neighbors behind, across, either side and above or below applicant's former residence).
- b. Assistance
- (1) Police precinct
- (2) Other police agencies—out-of-State (prepare letters)
9. *Selective service status*
- a. Contact local selective service to determine if properly registered, classified, lottery number, etc.
- b. If reserve, determine whether ready or standby.
- NOTE.—If standby, ascertain stand-  
by reserve classification in addition to draft classification. 1-R = Available for order to active duty. 11-R = Not available because of civilian occupation. 111-R = Not available because of dependency.
10. *Military service*
- a. Prepare a letter to be forwarded to the repository of records requesting service record. (Submit release form at that time.) Check for information concerning any physical disabilities or problems.
- b. There is a VA Form 07-3288 available from the Veterans Administration which will give information regarding a person's VA record.
11. *Medical*
- Check with personal physician or departmental records.
- NOTE.—Will need applicant's release form.
12. *Organizations*
- a. During investigations make inquiries to determine if the applicant has been affiliated with any subversive or dissident organizations.
- b. If allegations are received indicating disloyal, subversive or criminal activity, attempt to contact known informants in the area of the activity and clarify.
13. *Foreign travel* (if applicable)
- a. State Department
- b. Immigration and Naturalization Service and/or U.S. Custom Service.
14. *Initiate arrest checks* (applicant and all members of the family) include traffic, criminal, wanted and complaints.
- a. Out-of-State and in-State
- (1) Teletype
- (2) Letters
- (3) Personal contact (Local law enforcement agencies)
- b. FCIC—wanted check
- c. NCIC—wanted check
- d. FBI—applicant only (initiated by personnel)

- e. Verify all reported information under court record in application.
- f. FBI check—if former police officer, check field office in the area where the applicant was an officer for civil rights violation and FBI indices.
- g. When necessary, name search local police agency files regarding personal and developed references.

NOTE.—Ascertain details of arrest or complaints. Not necessary to search names of relatives under 15 years of age.

- 15. Acquaintances in agency should be interviewed as developed references.
- 16. *Drivers license checks* (verify)
  - a. Out-of-State
  - b. In-State

#### IV. Report of Investigation

##### A. Heading

- 1. Title
- 2. Dates covered
- 3. Recommended disposition

##### B. Synopsis

- 1. Introductory information
- 2. Personal history

- 3. Arrest record
- 4. Financial investigation
- 5. Education
- 6. Employment
- 7. Personal and developed references
- 8. Neighborhoods

#### GENERAL INFORMATION REGARDING THE SYNOPSIS

1. When using applicant's name, use full name. If using name more than once in the synopsis, the surname can be used prefixed by Mr., Miss, or Mrs.

2. When describing a place always identify by city or State.

3. Any derogatory information must be thoroughly explained.

4. The synopsis must cover all the elements listed in part IV(B) of this brochure. The only exception would be in cases where a specified area does not apply, or the investigation was terminated.

5. In the case of a termination the backup material will not be typed. However, that information which was secured will appear in a type-written synopsis and termed a partial background investigation.

## Appendix G

# BIBLIOGRAPHY

### A. GENERAL BIBLIOGRAPHY ON ORGANIZED CRIME

- ALBINI, JOSEPH L. *The American Mafia; Genesis of a Legend*. New York, Appleton, Century, Crofts, 1971.
- American Academy of Political and Social Science, Philadelphia. *Combating Organized Crime. Its Annals*, v. 347 (May 1963), pp. 1-112. Gus Tyler, editor.
- BERS, MELVIN K. *The Penetration of Legitimate Business by Organized Crime—An Analysis*. Prepared for the New York State Identification and Intelligence System and the National Institute for Law Enforcement and Criminal Justice. Washington, D.C., LEAA, U.S. Department of Justice, April 1970.
- BLAKEY, G. ROBERT. *Organized Crime in the United States*. *Current History*, v. 52 (June 1967), pp. 327-333 and 364-365.
- "Bull Market in Thievery." *Forbes*, v. 102 (December 15, 1968), pp. 34, 37-38.
- The role of the Mafia in the stealing of securities.
- Chamber of Commerce on the United States. *Deskbook on Organized Crime*. An Urban Affairs Publication of the Chamber of Commerce of the United States, Washington, D.C., 1969.
- . *Marshaling Citizen Power Against Crime*. Washington, D.C., Chamber of Commerce of the United States, 1970.
- Chicago Crime Commission, "Spotlight on Legitimate Businesses and the Hood, Part II." In remarks by Charles Harting Percy. *Congressional Records* (Daily edition), v. 114 (June 24, 1968), S7595-S7596.
- CRESSEY, DONALD R. *Theft of a Nation; the Structure and Operations of Organized Crime in America*. New York, Harper and Row, 1969.
- . "The Functions and Structure of Criminal Syndicates." Appendix A of the President's Commission on Law Enforcement and the Administration of Justice, *Task Force Report: Organized Crime*. Washington, D.C., Government Printing Office, 1967.
- DEMARIS, OVID. *Captive City*. New York, Lyle Stuart, Inc. 1969.
- DUSTER, TROY. *The Legislation of Morality*. New York, The Free Press, 1970.
- EDELHERTZ, HERBERT. *The Nature, Impact, and Prosecution of White-Collar Crime*. National Institute of Law Enforcement and Criminal Justice. (ICR 70-1), Washington, D.C., Government Printing Office, May 1970.
- GARDINER, JOHN A. *The Politics of Corruption: Organized Crime in an American City*. New York, Russell Sage Foundation, 1970.
- with the assistance of David J. Olson. "Wincanton: The Politics of Corruption." Appendix B of the President's Commission on Law Enforcement and the Administration of Justice, *Task Force Report: Organized Crime*. Washington, D.C., Government Printing Office, 1967.
- . "Public Attitudes toward Gambling and Corruption." *Annals of the American Academy of Political and Social Science*, v. 374 (November 1967).
- HILL, ALBERT F. *The North Avenue Irregulars; A Suburb Battles the Mafia*. New York, Cowles Publications, 1968.
- HINDELAC, MICHAEL J. "Bookies and Bookmaking: A Descriptive Analysis." *Crime and Delinquency*, v. 17, No. 3 (July 1971), pp. 245-255.

- HUTCHINSON, JOHN. "The Anatomy of Corruption in Trade Unions." *Industrial Relations*, v. 8 (February 1969), pp. 135-150.
- Illinois Crime Investigating Commission. *Juice Racketeers; Report on Criminal Usury in the Chicago Area*. Illinois, Illinois Crime Investigating Commission, June 1970.
- KING, RUFUS. *Gambling and Organized Crime*. Washington, D.C., Public Affairs Press, 1969.
- LANDESCO, JOHN. *Organized Crime in Chicago*. 2d ed. Chicago, University of Chicago Press, 1968.
- Law Enforcement Assistance Administration. Organized Crime Program Division. *The Role of State Organized Crime Prevention Councils*. Washington, D.C., Organized Crime Program Division, LEAA, 1970.
- LOFTON, OLIVER. "Organized Crime in the Ghetto." Speech in the *Congressional Record* (May 4, 1970), H3845.
- MAAS, PETER. *The Valachi Papers*. New York, G. P. Putnam's Sons, 1968.
- MESSICK, HANK. *Lansky*. New York, G. P. Putnam's Sons, 1971.
- . *Syndicate in the Sun*. New York, The Macmillan Company, 1968.
- National Symposium on Law Enforcement Science and Technology, 1st, Chicago. 1967. *Law Enforcement Science and Technology; Proceedings of the First National Symposium on Law Enforcement Science and Technology*. Washington, D.C., Thompson Book Company, 1967.
- See pp. 3-46.
- New York (State) Commission of Investigation. March 1970. *Racketeer Infiltration into Legitimate Business*. This report is an extract from the Twelfth Annual Report of the New York State Commission of Investigation (March 1970).
- New York (State) Temporary State Commission of Investigation. *An Investigation of the Loanshark Racket; A Report*. New York, 1965.
- Oyster Bay (New York) Conference on Combating Organized Crime, 1965. *Combating Organized Crime*. A report of the 1965 Oyster Bay Conferences on Organized Crime. Albany, 1966.
- Pennsylvania Crime Commission. (Office of the Attorney General. Department of Justice.) *Report on Organized Crime*. Harrisburg, Pa., 1970.
- President's Commission on Law Enforcement and Administration of Justice. *The Challenge of Crime in a Free Society*. Washington, D.C., Government Printing Office, 1967.
- See Chapter 7, "Organized Crime."
- . *Task Force Report: Organized Crime*. Washington, D.C., Government Printing Office, 1967.
- REID, ED., and DEMARIS, OVID. *The Green Felt Jungle*. New York, Trident Press, 1963.
- Research Institute of America. "Protecting Your Business Against Organized Crime: Research Institute Staff Recommendations, April 15, 1968." In remarks of Jack Edwards. *Congressional Record* (Daily edition) v. 114 (May 15, 1968), H3856-H3863.
- RUTH, HENRY S., Jr. "Why Organized Crime Thrives." *Annals of the American Academy of Political and Social Science*, Philadelphia, v. 374 (November 1967), pp. 113-122.
- SALERNO, RALPH. *The Crime Confederation; Cosa Nostra and Allied Operations in Organized Crime*. Garden City, N.Y., Doubleday and Company, Inc., 1969.
- . "Organized Crime's Growing Threat to American Business." *Business Management*, v. 35 (November 1968), pp. 57-59.
- SHELLING, THOMAS C. "Economic Analysis of Organized Crime." Appendix D of President's Commission on Law Enforcement and the Administration of Justice, *Task Force Report: Organized Crime*. Washington, D.C., Government Printing Office, 1967.
- SEIDL, JOHN MICHAEL. *Upon the Hip—A Study of the Criminal Loan Shark Industry*. Ph. D. dissertation, Harvard University. Washington, D.C., Law Enforcement Assistance Administration, 1969.
- SMITH, DWIGHT C., Jr. "Cooperative Action in Organized Crime Control." *Journal of Criminal Law, Criminology and Police Science*, v. 59, No. 4 (December 1968), pp. 491-498.
- SMITH, WILLIAM. "The Unseen Impact of Organized Crime on Manufacturing." *Modern Manufacturing*, v. 1 (July 1968), pp. 160-161.
- TURNER, WALLACE. *Gamblers' Money, A New*

*Force in American Life*. Boston, Houghton Mifflin, 1965.

Dated, but interesting account of prominent syndicate leaders' interests in organized gambling.

TYLER, GUS. "An Interdisciplinary Attack on Organized Crime." *The Annals of the American Academy of Political and Social Science*, v. 347 (May 1964), pp. 104-112.

———. *Organized Crime in America; A Book of Readings*. Ann Arbor, Mich., University of Michigan Press, 1962.

An interesting collection of essays that are mostly historical. Some of the more incisive remarks come from Tyler's introductions to the various parts of the volume.

United Aircraft. Corporate Systems Center. *Definition of Proposed NYSIIS Organized Crime Intelligence Capabilities*. A recommended Development Plan. (A report prepared for the New York State Identification and Intelligence System.) Farmington, Conn., United Aircraft Corporate Systems Center, December 21, 1966.

See Chapter 2 and Appendix.

*U.S. Laws, Statutes, etc.*

Omnibus Crime Control and Safe Streets Act, 1968. Public Law 90-351. 90th Congress, H.R. 5037, June 19, 1968, 82 Stat. 197.

U.S. Congress. Senate. Committee on Government Operations. *Organized Crime and Illicit Traffic in Narcotics*. Washington, D.C., Government Printing Office, 1965.

U.S. Congress. House. Committee on Government Operations. Legal and Monetary Affairs Subcommittee. *Federal Effort Against Organized Crime: Report of Agency Operations*. Hearings, 90th Cong., 1st and 2d sess., parts 1-3: April 5, 1967-February 8, 1968. Washington, D.C., Government Printing Office, 1967-1968.

———. *Federal Effort Against Organized Crime: Role of the Private Sector*. Hearings, 91st Cong. 2d sess., August 13-September 15, 1970. Washington, D.C., Government Printing Office, 1970.

U.S. Congress. Senate. Committee on the Judiciary. *Obstructions of Criminal Investigations; Report to Accompany S. 676*. (90th Cong., 1st sess., Senate. Report No. 307) Washington, D.C., Government Printing Office, 1967.

———. *Permitting the Compelling of Testimony and the Granting of Immunity With Respect to Certain Crimes; Report to Accompany S. 677*. (90th Cong., 1st sess., Senate. Report No. 308) Washington, D.C., Government Printing Office, 1967.

The bill would authorize immunity grants from criminal statutes directly applicable to organized crime.

The bill would make it a Federal crime to intimidate, harass, or attack witnesses who have provided information to Federal investigators prior to the commencement of criminal proceedings. It would assist in prosecuting and convicting organized crime members.

U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Criminal Laws and Procedures. *Controlling Crime Through More Effective Law Enforcement*. Hearings, 90th Cong., 1st sess., Washington, D.C., Government Printing Office, 1967.

Hearings held March 7-July 12, 1967.

———. *Measures relating to Organized Crime*. Hearings, 91st Cong., 1st sess., March 18, 19, 25, 26, and June 3, 4, 1969. Washington, D.C., Government Printing Office, 1969.

U.S. President, 1969- (Nixon) *Organized Crime*. Message . . . (91st Cong., 1st sess. House. Document No. 91-105) Washington, D.C., Government Printing Office, 1969.

"The Urban Poor and Organized Crime." In remarks of Joseph M. McDade. *Congressional Record* (Daily edition), v. 113 (August 29, 1967), H11431-H11435.

## B. BIBLIOGRAPHY BY CHAPTER

### Chapter I: The Role of Intelligence in Combating Organized Crime

DULLES, ALLEN. *The Craft of Intelligence*, Harper and Row, New York, 1963.

KENT, SHERMAN. *Strategic Intelligence for American World Policy*. Princeton, N.Y., Princeton University Press, 1966.

RANSOM, HARRY H. *The Intelligence Establishment*. Cambridge, Mass., Harvard University Press, 1970.

United Aircraft. Corporate Systems Center. *Definition of Proposed NYSIIS Organized Crime Intelligence Capabilities*. A Recommended Development Plan. (A report prepared for the New York State Identification and Intelligence System.) Farmington, Conn., United Aircraft Corporate Systems Center, December 21, 1966.

See section 2.

## Chapter II: The Intelligence Process

Department of the Air Force.

Air University. Extension Course Institute. *The Intelligence Cycle*. (2001-1) Extension Course Institute, Gunter Air Force Base, Alabama.

Begins usefully enough with a brief description of collection, production, and dissemination, but soon gets into the Air Force application. Chapter 2, on production, has some useful passages.

HEWITT, WILLIAM H. *Police Records Administration*. Rochester, New York, Aqueduct Books, 1968.

New York State Identification and Intelligence System. *A New Concept in Criminal Justice Information Sharing: The New York State Identification and Intelligence System*. Albany, New York, NYSIIS, April 1967.

SHAW, WILLIAM. "An Introduction to Law Enforcement Electronics and Communications," *Law and Order*, v. 13, No. 4 (April 1965), pp. 44-48; 13, No. 6 (June, 1965), p. 30.

U.S. Department of the Army. "Techniques of Surveillance and Undercover Investigations." Technical Bulletin TB PMG 8. Washington, D.C., Department of the Army, Headquarters, November 2, 1965. Useful theory of technique.

———. "Polygraph Examinations." Technical Bulletin TB PMG 22. Washington, D.C., Department of the Army, Headquarters, November 1, 1966.

Some useful comment on theory of polygraph technique.

U.S. Army Intelligence School. "Intelligence Research Officer/Technician." Program of Instruction. Fort Holabird, Maryland, U.S. Army Intelligence School, June 1970.

No substance but some useful bibliographical additions.

U.S. Department of the Treasury. Federal Law Enforcement School.<sup>1</sup>

"Evidence." Text 14 (4-71).

"Description and Identification." Text 33 (3-69).

"Undercover Operation." Instructor Guide 48 (1-69); Student Guide 48 (1-69); Test 48 (1-69).

"Surveillance." Instructor Guide 35 (4-71); Student Guide 35 (4-71).

"Informants." Instructor Guide 35 (4-71); Student Guide 35 (4-71).

WILSON, O. W. *Police Administration*. New York, McGraw-Hill Book Company, 1963. Especially Chapters 14, 15, and 18.

New York State Identification and Intelligence System. *Security System for Organized Crime Intelligence Capability*. Reprints available from Law Enforcement Assistance Administration, U.S. Department of Justice. (Information releasable to any criminal justice agency.)

BRISTOW, ALLEN P. *A Preliminary Study of Problems and Techniques in Decision Making for the Police Administrator*. Thesis for masters of science in public administration, Los Angeles, School of Public Administration, University of Southern California, June 1957.

BRISTOW, ALLEN P., and GABARD, E. C. *Decision Making in Police Administration*. Springfield, Ill., Thomas, 1961.

GAMMAGE, ALLEN Z. *Basic Police Report Writing*. Springfield, Ill., Thomas 1961.

HARNEY, MALACHI L., and CROSS, JOHN C. *The Informer in Law Enforcement*. Springfield, Ill., Thomas, 1968.

KAHN, GILBERT; YERIAN, THEODORE; and STEWART, JEFFREY R., Jr. *Filing Systems and Records Management*. 2d ed. New York, McGraw-Hill Book Company, 1971.

O'HARA, CHARLES E. *Fundamentals of Criminal Investigation*. 2d ed. Springfield, Ill., Thomas, 1970.

WHISENAND, PAUL M. *Police Supervision; Theory and Practice*. Englewood Cliffs, N.J., Prentice-Hall, Inc. 1971.

<sup>1</sup> Requests for copies of Federal Law Enforcement School texts should be sent to the Technical Assistance Division, Office of Criminal Justice Assistance, Law Enforcement Assistance Administration, U.S. Department of Justice, Washington, D.C. 20530.



- WHISENAND, PAUL M., and TAMARU, TUG T. *Automated Police Information Systems*. New York, John Wiley and Sons, Inc., 1970.
- SUCHMAN, EDWARD A. *Evaluative Research; Principles and Practices in Public Service and Social Action Programs*. New York, Russell Sage Foundation, 1967.
- United Aircraft. Corporate System Center. *Definition of Proposed NYSIIS Organized Crime Intelligence Capabilities*. A Recommended Development Plan. (A report prepared for the New York State Identification and Intelligence System.) Farmington, Conn., United Aircraft Corporate Systems Center, December 21, 1966.
- See section 2.

### Chapter III: Structure of an Intelligence Unit

- ANDERSON, ANNESE. *Organized Crime: The Need for Research*. Law Enforcement Assistance Administration, U.S. Department of Justice, December 1970.
- BRISTOW, ALLEN P., comp. *Police Supervision Readings*. Springfield, Ill., Thomas, 1971.
- BROWN, WILLIAM P. *A Police Administrative Approach to the Corruption Problem*. Prepared for the Organized Crime Program Division, Law Enforcement Assistance Administration, U.S. Department of Justice. (Available Fall, 1971).
- CRESSEY, DONALD R. "Methodological Problems in the Study of Organized Crime as a Social Problem." *Annals of the American Academy of Political and Social Science*, v. 374 (November 1967), pp. 101-112.
- EASTMAN, GEORGE D., and EASTMAN, ESTHER M. *Municipal Police Administration*. Washington, D.C., International City Management Association, 1969. Chapter by Earhart and Pace on vice, organized crime, and intelligence.
- HEWITT, WILLIAM H. *Police Records Administration*. Rochester, New York, Aqueduct Book, 1968.
- Institute on Police Management for Supervisory and Administrative Personnel, Dallas, 1962. *Police Management for Supervisory and Administrative Personnel*. Springfield, Ill., Thomas, 1963.
- New York State Identification and Intelligence System. *A New Concept in Criminal Justice Information Sharing: The New York*

*State Identification and Intelligence System*. Albany, New York, NYSIIS, April 1967.

- WHISENAND, PAUL M. *Police Supervision; Theory and Practice*. Englewood Cliffs, N.J., Prentice-Hall, Inc., 1971.
- WILSON, O. W. *Police Administration*. New York, McGraw-Hill Book Company, 1963. Especially chapters 1 through 7.
- WILSON, O. W. *Police Planning*. Springfield, Ill., Thomas, 1957.
- United Aircraft. Corporate Systems Center. *Definition of Proposed NYSIIS Organized Crime Intelligence Capabilities*. A Recommended Plan. Farmington, Conn., United Aircraft Corporate System Center, December 21, 1966.
- See parts 4 and 5.

### Chapter IV: Staffing the Intelligence Unit

- ANASTASI, ANNE. *Psychological Testing*. 3d ed. London, The Macmillan Co., 1970.
- Useful guide to range of tests available.
- BLUM, RICHARD H. *Police Selection*. Springfield, Ill., Charles C. Thomas, 1964.
- Chapters on background investigation and psychological testing.
- PIGORS, PAUL, and MYERS, CHARLES A. *Personnel Administration, A Point of View and a Method*. 5th ed. New York, McGraw-Hill Book Company, 1965.
- Good basic text though directed at industrial and white collar management.
- WILSON, O. W. *Police Administration*. New York, McGraw-Hill Book Company, 1963.
- See Chapter 8.
- THORNDIKE, ROBERT L., ed. *Educational Measurement*. 2d ed. Washington, D.C., American Council on Education, 1971.
- BELLOWS, ROGER M. *Psychology of Personnel in Business and Industry*. 3d ed. Englewood Cliffs, N.J., Prentice-Hall, 1961.
- BELLOWS, ROGER M., with the assistance of M. FRANCES ESTEP. *Employment Psychology; The Interview*. New York, Rhinehart, 1954.
- BRISTOW, ALLEN P. *Effective Police Manpower Utilization*. Springfield, Ill., Thomas, 1969.
- . comp. *Police Supervision Readings*. Springfield, Ill., Thomas, 1971.
- GERMANN, A. C. *Police Personnel Management*. Springfield, Ill., Thomas, 1958.

WHISENAND, PAUL M. *Police Supervision; Theory and Practice.* Englewood Cliffs, N.J., Prentice-Hall, Inc., 1971.

## Chapter V: Training

American Academy of Political and Social Science. Philadelphia. *Gambling*, Philadelphia, 1950. V. 269 (May 1950).

BRERETON, GEORGE H. "The Importance of Training and Education in the Professionalization of Law Enforcement," *Journal of Criminal Law, Criminology and Police Science*, v. 52 No. 1 (May-June 1961), pp. 111-121.

GAMMAGE, ALLEN Z. *Basic Police Report Writing.* Springfield, Ill., Thomas, 1961.

GERMANN, A. C. "Education and Professional Law Enforcement," *Journal of Criminology and Police Science*, v. 58, No. 4, December (1967), pp. 603-609.

Law Enforcement Assistance Administration, Organized Crime Program Division. *Police Guide on Organized Crime.* Organized Crime Program Division, LEAA, U.S. Department of Justice.

See Chapter I and the section on training.

LOFTEN, OLIVER. "Organized Crime in the Ghetto." Speech in the *Congressional Record*, (May 4, 1970). H3845.

National Sheriffs' Association. *Manual on Training for Sheriffs.* (A Law Enforcement Assistance Administration project report by the National Sheriffs' Association) Washington, D.C., Government Printing Office, 1969.

*Police Training and Performance Manual.* Washington, D.C., National Institute of Law Enforcement and Criminal Justice, LEAA, U.S. Department of Justice, (September 1970) (PR 70-4).

SEIDL, JOHN MICHAEL. *Upon the Hip—A Study of the Criminal Loan Shark Industry*, Washington, D.C., Law Enforcement Assistance Administration, U.S. Department of Justice, 1969.

U.S. Department of the Treasury. Federal Law Enforcement School. "Ethics and Conduct for Investigators." Student Guide 1 (5-71). "Effective Writing for Investigators." Text 44 (5-69).<sup>2</sup>

U.S. Department of the Treasury. Internal Revenue Service. Intelligence Division. *Digest of Wagering Operations.* Document No. 5466 (1-63) Washington, D.C., Government Printing Office, 1963.

Westinghouse Broadcasting Corporation. *The Corrupt City.* A documentary file, New York, 1969. Suchman,

WILSON, O. W. *Police Administration.* New York, McGraw-Hill Book Company, 1963. See Chapter 7.

## Chapter VI: Security

HEALY, RICHARD L. *Design for Security.* New York, John Wiley and Sons, Inc., 1968.

Deals with physical aspects of security only. Suggested use of modern techniques and devices.

New York State Identification and Intelligence System. *Security System for Organized Crime Intelligence Capability.* Reprints available from Law Enforcement Assistance Administration, U.S. Department of Justice. (Information releasable to any criminal justice agency.)

Project SEARCH (System for Electronic Analysis and Retrieval of Criminal Histories), Committee on Security and Privacy. *Security and Privacy Considerations in Criminal History Information Systems.* Technical Report No. 2, July 1970. Project SEARCH Staff, California Crime Technological Research Foundation, Sacramento, California.

U.S. Department of the Army. *Polygraph Examinations.* Technical Bulletin TB PMG 22. Washington, D.C., Department of the Army, Headquarters, November 1, 1966.

Some useful comment on theory of polygraph technique.

## Appendix A: Intelligence and the Law

American Bar Association. Project on Minimum Standards on Criminal Justice. *Standards Relating to Electronic Surveillance.* Tentative draft. June 1968.

American Bar Association. Special Committee on Electronic Data Retrieval. *Computers and the Law; An Introductory Handbook.* New York, Commerce Clearing House, 1966.

See the section on substantive law aspects

<sup>2</sup> See footnote 1, page 147, for information on obtaining these texts.

- of computers, especially number 6, "Evidence."
- BLAKEY, G. ROBERT. "Aspect of the Evidence Gathering Process in Organized Crime Cases," Appendix C of *Presidents Commission Task Report Organized Crime*. Washington, D.C., Government Printing Office, 1967.
- . "Controlling Crime Through More Effective Law Enforcement." [Statement on problems associated with electronic surveillance.] In U.S. Congress. Senate. *Committee on the Judiciary. Subcommittee on Criminal Laws and Procedure*. Hearings, 90th Cong., 1st sess., Washington, D.C., Government Printing Office, 1967. pp. 932-954.
- For his complete testimony, see pp. 931-1001.
- CREAMER, J. SHANE. *The Law of Arrest, Search and Seizure*. Philadelphia, W. B. Saunders Company, 1968.
- DASH, SAMUEL. *The Eavesdroppers*. New Brunswick, N.J., Rutgers University Press, 1959.
- FASCELL, DANTE B. "Electronic Surveillance of Organized Crime." Remarks in The House. *Congressional Record* (Daily edition) v. 144, January 16, 1968: H75-H77.
- Recommends the use of restricted, court-ordered electronic surveillance by investigative agencies of the Federal Government in organized crime cases.
- HRUSKA, ROMAN LEE. "Electronic Surveillance by Authorized Law Enforcement Officers." Remarks in the Senate. *Congressional Record*. (Daily edition) v. 113, August 8, 1967: S11133-S11139.
- MCCLELLAN, JOHN L. "Organized Crime Evidence." Remarks in the Senate. *Congressional Records*. (Daily edition) v. 115, June 9, 1969: S6092-S6096.
- Comments of the Alderman disclosure requirement that files be opened to criminals who have been subjected to unlawful electronic surveillance and a Life magazine article consisting of excerpts of conversations overheard through FBI electronic surveillance.
- MILLER, ARTHUR R. *The Assault on Privacy; Computers, Data Banks, and Dossiers*. Ann Arbor, University of Michigan Press, 1971.
- . "Personal Privacy in the Computer Age," *Michigan Law Review*, v. 67, p. 1089.
- "Nixon and Courts Stir Wiretap and Bugging Disputes." *Congressional Quarterly Weekly Report*, v. 27, April 25, 1969: 593-603.
- A factsheet on the electronic surveillance controversy including its use in organized crime investigations.
- Project SEARCH (System for Electronic Analysis and Retrieval of Criminal History), Committee on Security and Privacy. *Security and Privacy Considerations in Criminal History Information Systems*. Technical Report No. 2, July 1970. Project SEARCH Staff, California Crime Technological Research Foundation, Sacramento, California.
- RUEBHAUSEN, OSCAR M., and BRIM, ORVILLE G., Jr. "Privacy and Behavioral Research," *Columbia Law Review*, v. 65, No. 7 (November 1965), pp. 1184-1211.
- SILVER, EDWARD S. "Organized Gambling and Law Enforcement," *Journal of Criminal Law, Criminology, and Police Science*, v. 50, No. 4 (1959-1960), p. 397.
- SCOULAR, ROBERT F. "Wiretapping and Eavesdropping; from Olmstead to Katz." *St. Louis University Law Journal*, v. 12 (1968), pp. 513-549.
- U.S. Congress. Senate. Committee on the Judiciary. *Obstruction of Criminal Investigations; Report to Accompany S. 676*. (90th Cong., 1st sess., Senate. Report No. 307) Washington, D.C., Government Printing Office, 1967.
- UVILLER, H. RICHARD. *Lawful Electronic Surveillance; A Manual for State Prosecutors and Law Enforcement Officers*. Law Enforcement Assistance Administration, U.S. Department of Justice. (Available in the fall, 1971.)
- WESTIN, ALAN F. *Privacy and Freedom*. New York, Atheneum, 1970.
- WHEELER, STANTON. *On Record: Files and Dossiers in American Life*. New York, Russell Sage Foundation, 1969.