

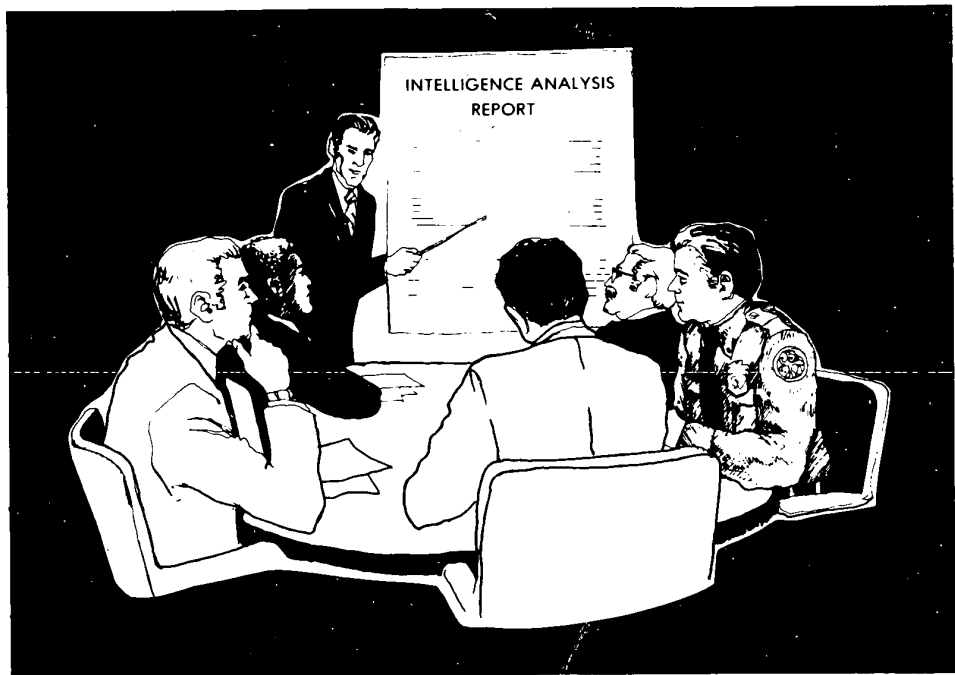
ORGANIZED CRIME CONTROL

REVISED EDITION

SEPTEMBER 1976

BASIC ELEMENTS OF INTELLIGENCE

A Manual for Police Department Intelligence Units



Box 491
39392

039392

BASIC ELEMENTS OF INTELLIGENCE

REVISED EDITION

SEPTEMBER 1976

Prepared for the:

**ORGANIZED CRIME DESK
ENFORCEMENT PROGRAM DIVISION
OFFICE OF REGIONAL OPERATIONS**

By:

DON R. HARRIS, Ph. D.

With Assistance From:

**MIKE MAXFIELD
GLENNIE HOLLADY**



**LEAA
LIBRARY**

This manual was prepared for the Law Enforcement Assistance Administration, U.S. Department of Justice by C.A.C.I., Inc. under contract number J-LEAA-127-75. Points of view or opinions stated herein are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, D.C. 20402 - Price \$2.40
Stock No. 027-000-00443-1

TABLE OF CONTENTS

	Page
FOREWORD	vi
PREFACE	vii
CHAPTER I: INTRODUCTION	1
A. The Historical Focus of Police Intelligence	1
1. Economic and Social Costs of Organized Crime	2
2. Changing Nature of Organized Crime	2
3. White-Collar Crime: A Growing Threat	3
B. Implications for Law Enforcement Agencies	3
C. The Intelligence Role	3
1. Tactical Intelligence	4
2. Strategic Intelligence	4
D. The Structure of an Intelligence Unit	7
E. Intelligence and the Chief	7
F. The Role of the Commander of the Intelligence Unit	8
CHAPTER II: INFORMATION FLOW	9
A. Introduction	9
B. Flow of Information from Non-Intelligence Police Department Units	9
1. Information Flow from Non-Intelligence Units in the Department	10
2. Information Flow from Other Agencies	11
C. Information from Sources Other Than Law Enforcement Agencies	12
D. Intelligence Unit Investigators	13
E. Collection Planning	15
CHAPTER III: THE FILING SYSTEM	16
A. Purpose	16
B. Information Requirements	19
C. Structuring the Files	20
1. Indexing	20
2. Basic Report Filing	21
3. Questionable Reports on Alleged Criminals or Their Associates	21
4. Sensitivity and Reliability of Information.	22
D. File Room Procedures and Operations	24
1. File Clerk Functions	24
2. Forms	24
3. Mechanical Filing Aids	24
4. File Room Security.	25
E. Guidelines	25
CHAPTER IV: Analysis and Reporting	27
A. Role of Analysis	27
B. Duties of the Intelligence Analyst	27
1. Reading and Indexing	28
2. Developing and Maintaining Information	28
3. Identifying Information Requirements	29
4. Performing Research and Analysis	29

831128

	Page
5. Preparing Intelligence Reports	29
C. Techniques	30
1. What is Analysis?	30
2. An Example of Analysis	31
3. Pursuing Civil Violations	33
4. Using Intelligence Files	33
5. Use of the Hypothesis	34
D. Preparing Intelligence Reports	36
1. Oral Tactical Response	36
2. Written Tactical Response	36
3. Strategic Reports	36
4. Periodic Reports	36
 CHAPTER V: STAFFING AND TRAINING THE INTELLIGENCE UNIT	 38
A. Introduction	38
B. Staffing the Intelligence Unit	38
1. Unit Commander	38
2. General Criteria for Staff Selection	38
3. Determining the Analytic Discipline Needed	41
4. The Special Nature of Staffing the Intelligence Unit	44
C. Training	46
1. Training for the Non-Intelligence Officer	46
2. Training Intelligence Officers	47
3. Command Level Training	51
4. Understanding Methodology and Process	52
 CHAPTER VI: MANAGEMENT OF A POLICE INTELLIGENCE UNIT	 53
A. The Problems	53
1. Collection	53
2. Collation/Files	54
3. Analysis	54
B. Suggested Solutions	55
1. Relationship with the Chief	55
2. Developing an Adequate Flow of Information	57
3. Focus of Effort	58
C. Supervision	60
D. Selection and Training of Staff	60
E. Evaluation	61
 APPENDIX A: GUIDELINES FOR POLICE INTELLIGENCE UNITS	 62
A. Guides for the Investigator	63
B. Guidelines: Types of Information That Can Be Kept in the Intelligence File	67
C. Guidelines Controlling Dissemination Outside the Department	70
 APPENDIX B: SAMPLE DEBRIEF FORM AND LIST OF SELECTED SPECIFIC QUESTIONS	 74
 APPENDIX C: OPERATIONAL PROCEDURES FOR AN INTELLIGENCE INFORMATION CONTROL AND FILING SYSTEM	 79
A. The Role of Information Control	79
1. The Accession or Control Number	79

	Page
2. Logging	79
3. Distribution	79
B. Indexing	80
C. The Operation of the File Room Staff	81
APPENDIX D: THE COMPUTER AND THE INTELLIGENCE UNIT	93
A. Introduction	93
B. Conditions Favorable to Conversion to the Computer	93
1. Availability of a Secure Computer	93
2. Volume of Data to be Handled	94
C. The Computer and the Intelligence Process	94
1. Collection—Information Flow	94
2. Collation	95
3. Analysis	95
4. Security	95
APPENDIX E: SECURITY	100
A. Introduction	100
B. Personal Security	101
1. The Background Investigation	101
2. Update of Background Investigation	102
3. Polygraph	105
4. Security Training	105
C. Physical Security	105
1. The Office	105
2. The Files	110
3. Security and the Computer	110
4. Security and Privacy	110
5. Organization of the Office for Security	110
D. Operational Security	110
E. The Responsibility of the Unit Commander	111
APPENDIX F: ANALYST MANUAL	119
A. Building the Information Base	119
B. Responding to Tactical Requests	120
C. Intelligence Reports-Strategic Intelligence	120
1. Surveying Information Sources	120
2. Formulating Hypotheses	121
3. Designing a Collection Plan	121
4. Collecting and Collating	122
5. Analysis	122
D. Techniques of Analysis	123
1. Association Charting	123
2. Use of Statistical Techniques in Intelligence Analysis	125
E. Reporting Intelligence	129
APPENDIX G: EVALUATING THE INTELLIGENCE FUNCTION	133
A. Evaluation Approach	133
1. Monthly Intelligence Unit Self-Analysis	133
2. Monthly Evaluation of the Intelligence Process	134
3. Monthly User Evaluation of Intelligence Unit Output	134

	Page
B. Proposed Numeric Evaluation System	134
1. Collection	135
2. Processing/Collation	135
3. Analysis	136
4. Production/Dissemination	136
5. Management Procedures	136
C. Proposed Seven-Value Approach to Evaluation of an Intelligence Unit . .	138
1. Collection	138
2. Processing/Collation	139
3. Analysis	139
4. Production/Dissemination	140
5. Management Procedures	140
6. Guidelines for Intelligence Operations	141
D. Evaluation of an Intelligence Unit by Establishing a Value for the Individual Member of the Unit, Relative to Task to Which the Person Is Assigned	141
1. Intelligence Investigator	147
2. Intelligence Analyst	149
E. Evaluation of the Intelligence Unit by the User	152
BIBLIOGRAPHY	155
A. General Bibliography on Organized Crime	155
B. Bibliography by Chapters	159
C. Bibliography by Appendices	162

LIST OF TABLES AND FIGURES

CHAPTER III

Page

TABLE 1: SUGGESTED SENSITIVITY AND REPORT EVALUATION CODES	23
---	----

CHAPTER I

FIGURE 1: THE INGELLIGENCE PROCESS	5
--	---

CHAPTER III

FIGURE 1: CONTROL AND FLOW OF INFORMATION AND DOCUMENTS	17
--	----

CHAPTER IV

FIGURE 1: ANALYSIS PROCEDURE	33
FIGURE 2: USING THE HYPOTHESIS	35

CHAPTER V

FIGURE 1: CRITERIA FOR SELECTION OF INTELLIGENCE UNIT STAFF.	39
---	----

FOREWORD

The "Basic Elements of Intelligence," the first manual for police intelligence units, was the product of two men experienced in the processes and operations of intelligence at the national level. They 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 the need to develop and to improve intelligence directed toward organized crime.

The current redraft of the Intelligence Manual (a suggested short title) is largely the product of the experience gained by one of the authors, Don Harris, in the period 1971-1975. The manual reflects an often expressed need to recast the basic principle in terms of current police experience and operations. There has been widespread agreement with the principles set forth in "Basic Elements." But much has happened in the past few years in the intelligence posture to assist police units in fighting organized crime. In particular, LEAA has substantially increased the resources devoted to this sector of the total criminal law enforcement program.

The current manual, as in the case of the first one, is in a real sense a collective effort. Police intelligence units (and those associated with Federal agencies and the state and local prosecutor offices) have given generously of their time to share approaches, successes, and problems. This is the essential body of data from which the suggested approaches to an effective operation of the intelligence process were drawn. While the final product must be the responsibility of the author, without this broad access to actual operations the effort would have been impossible.

The current manual contains many of the ideas and concepts of Dr. Godfrey, in many places in his own turn of phrase as especially is the case in Chapter V on staffing and training. Two members of the CACI staff also made important contributions. Mike Maxfield did the initial drafting for Chapter IV, Analysis and Reporting; and Appendix F, The Analyst Manual. Glennie Hollady did the initial drafts for Chapter III, The File System - Collation. The focus and impact owes much to the review in draft by Dr. Hayes, Division Manager, CACI, and to the editing by Carol Franco. Without the technical support and general shepherding by Joyce Nalley, the text would have remained untyped and unassembled.

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 because 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 that techniques from disciplines unfamiliar to law enforcement can be adapted effectively to aid in the fight against organized criminal elements.

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

CHAPTER I

INTRODUCTION

An effective intelligence unit is one of the most important weapons the police department has in its fight against crime and especially against those criminals who, by organizing, seek to maximize their illegal gains. An intelligence unit supports current investigations by bringing together information from all sources to assist the investigator on a current case. In organized crime operations it provides an assessment of the activities of major organized criminals and their associates. The unit provides the chief of the department with an analysis of what is known of the particular group under review. It indicates the potential for launching enforcement action with the information available or recommends that additional information be gathered to determine whether enforcement actions can be undertaken.

An intelligence unit that provides the support required in a police department's fight against crime must be able to perform all functions in the intelligence process. This process includes collection of information, collation and filing, analysis, reporting, and dissemination. In addition, the unit must have effective leadership to integrate the various elements of the process. The unit commander must determine priorities and establish a close relationship with the senior commanders within the department and the chief to learn first-hand their reactions to the intelligence unit's efforts.

An effective unit requires a trained, motivated staff. The department must be responsive to the needs of the unit commander and must be prepared to provide personnel to meet the job requirements for the intelligence investigator, intelligence analysts, and file clerk.

Finally, to establish the integrity of the operation and maintain the intelligence files, the department must have guidelines for the flow of information into the intelligence files and for purging material that has become irrelevant, particularly in light of the developing legal situation as defined by Federal and state laws.

This manual is designed to present guidelines for organizing and operating an effective police intelligence unit. Emphasis is placed on the problems involved in combating organized crime, which includes much that is now being called "white-collar" crime. It attempts to define the concept of intelligence and its role in the criminal justice system while at the same time providing a practical handbook for the law enforcement intelligence unit. In particular, the intent is to assist

intelligence units, large or small, in their efforts against major crime in their jurisdiction, whatever its form.

Chapter I outlines briefly the history and growth of organized crime in the United States as well as the infiltration of organized criminal elements into legitimate business and government, the social and economic impacts of this crime, and its implications for the criminal justice system. It defines the meaning of "intelligence" as it applies to law enforcement agencies as a tool for fighting organized and white-collar crime. Finally, it discusses the growing public concern over the right-to-privacy issue and its legal implications for law enforcement intelligence units.

Each subsequent chapter deals with a specific element of the intelligence function. Chapter II outlines the various sources and methods for gathering the kinds of information necessary to produce sound intelligence; the organization of the filing system for storing, protecting, and disseminating intelligence information is discussed in Chapter III; Chapter IV provides the intelligence analyst with techniques for developing hypotheses from raw intelligence data for producing and disseminating intelligence for strategic and tactical operations; Chapter V discusses staffing and training the intelligence unit; and finally, Chapter VI explores the overall organization and management of the intelligence unit. Appendices supplement the manual where more detailed discussions on particular aspects of the intelligence function are required.

Since intelligence units will vary greatly in size and focus according to particular needs and the resources available, this manual presents general guiding principles that can be applied to small and large intelligence units alike. Specific examples are used to illustrate and are not intended to be followed slavishly.

A. The Historical Focus of Police Intelligence

Criminal intelligence in the past has focused on an aspect of criminal activity categorized as "organized." It primarily encompassed gambling, loan-sharking, narcotics, prostitution, and pornography. There was ample evidence that nationally organized groups attempted to control these activities, or at least provided the services essential to their operation. In certain urban areas, especially New York City, northern New Jersey,

Chicago, and New Orleans, there was evidence that the groups engaged in the listed criminal activities were also involved in corrupting labor unions and public officials.

Historically, groups of criminals organized their activities to prey on the masses of immigrants that crowded into major American cities in the late 19th and early 20th centuries. The scale of operations of organized criminals expanded greatly during the prohibition years. When prohibition ended in 1933, the gangs of bootleggers that had amassed huge sums of money sought ways to continue a flow of illegal gain. They did this by organizing rackets and infiltrating legitimate business. While the various games represented many different ethnic groups—there were Polish, Irish, German, Jewish, Italian, and Sicilian gangs—a series of gangland wars left the Sicilian-Italian group in control.¹ Under this leadership the gangs continued to flourish and grow until 1951 when the Kefauver Committee identified a nationwide crime syndicate operating in many of the large cities with control of the most lucrative rackets.²

In 1967, the President's Commission on Law Enforcement and Administration of Justice found the Mafia or La Cosa Nostra operating 24 core groups whose criminal operations and penetration of legitimate business varied from area to area.

While there is some debate as to how centralized the leadership of organized crime is, there is general agreement that a crime confederation does exist and that groups are in frequent communication with each other “. . . to gain money and power without regard for law by utilizing economic and physical force, public and private corruption, in an extension of the free-enterprise system.”³

1. Economic and Social Costs of Organized Crime.

The most serious threat to society from organized crime comes when criminal syndicates use vast sums of money gained from illicit enterprises to undermine legitimate business enterprises and political institutions. Organized crime has infiltrated labor unions, the entertainment business, manufacturing, real estate, and even the stock market. To measure its impact in terms of dollars would be a formidable, if not prohibitive, task.

In 1972 the stock brokerage industry alone estimated that stolen or missing securities of 1.2 billion dollars were being utilized in illegal operations around the

world.⁴ The loss of income tax revenue from organized crime operations is incalculable. It has been estimated that illegal betting on horse racing, lotteries, and sporting events alone totals at least \$20 billion a year with the syndicate taking about \$6 to \$7 billion as its share (this is about three times the amount of the annual budget for U.S. foreign aid).⁵ Loan sharks have been known to charge interest rates as high as 500 percent. Millions of dollars of cargo are pilfered from airports and piers by trucking companies and union locals working for a criminal group. Labor union pension funds have been used for loans to finance illegal or questionable enterprises, and construction companies have used shoddy materials and workmanship through kickback arrangements.

What this means, translated to the level of the everyday citizen, is higher prices through the monopolistic practices of organized crime, shoddy merchandise, poorly constructed and unsafe buildings, and higher taxes. More important is the threat to the free enterprise system. Organized crime operates on the local level as well, controlling businesses such as laundries, taxicab companies, paving-contract firms, travel agencies, insurance underwriting firms, vending machine companies, and restaurants.

The social costs of political corruption by organized crime are even more difficult to assess. Organized crime needs the involvement of the political system to profit from economic opportunities. The President's Commission concluded that “all available data indicate that organized crime flourishes only where it has corrupted local officials.”⁶ Over and over again, investigations into criminal activities have turned up close connections with respectable persons in business and public officials at all levels of government. Corruption is achieved through bribes and contributions to political campaigns; a police officer is bribed or overlooks gambling and a state or Federal legislator's vote on a bill is bought by the criminal organization that contributed heavily to the person's campaign through a front organization. Hence, organized crime is, in part, a subversion of the democratic process which ultimately will produce a political system where the strong and powerful exist at the expense of the weak.

2. **Changing Nature of Organized Crime.** To recognize only crime that falls into the category of major

¹Cressy, p. 9

²Kefauver Commission, 3d Interim Report, S. Rep. No. 307, 82d Congress, 1st Session 150 (1951).

³As quoted from the New York Joint Legislative Committee on Crime in Hank Messick and Burt Goldblatt, *The Mobs and the Mafia* (New York: Ballantine Books, 1972).

⁴Senator Charles H. Percy, U.S. Senate, *Hearings before the Subcommittee on Securities of the Committee on Banking, Housing and Urban Affairs, 92d Congress, 2d Session* (Washington, D.C.: Government Printing Office, 1972: pp. 65-69).

⁵Cressy, p. 75.

⁶President's Commission on Law Enforcement and Administration of Justice, *Task Force Report: Organize Crime* (Washington, D.C.: Government Printing Office, 1967).

rackets controlled by the syndicate is to ignore other kinds of criminal enterprise that can rightfully be called organized crime. Auto theft rings, credit card operations, land swindle deals, and white-collar crimes may be operative through an *ad hoc* organization having little or no connection with syndicate crime organizations. Organized crime is said to be one of America's fastest growing industries, attracting all elements of the society including the respectable businessperson and the esteemed politician. Organized crime has become not only more "democratic" in its composition but more sophisticated in its techniques. Its leaders are lawyers, accountants, bankers, and computer experts.

3. **White-Collar Crime: A Growing Threat.** White-collar crimes have been defined as: "...illegal acts characterized by guile, deceit, and concealment—and do not depend upon the application of physical force or violence or threats thereof. They may be committed by individuals acting independently or by those who are part of a well-planned conspiracy. The objective may be to obtain money, property, or services; or to secure business or personal advantage."⁷

White-collar crimes include pilferage, fencing stolen property, embezzlement, credit card and check fraud, bankruptcy fraud, insurance fraud, kickbacks, payoffs, and computer-related crime. Like syndicated crime, it is impossible to determine accurately the direct financial cost of white-collar crime, but a modest estimate puts it at no less than \$40 billion annually. Fraud is often a contributing factor in the closing of banks; employee dishonesty accounts for almost one-third of business failures annually; and dishonesty by business executive and employees boosts the cost of retail goods as much as 15 percent.⁸

Other consequences of white-collar crime are the risks to health and safety by tainted or unsafe products that violate health laws, building codes, and consumer safety regulations. Of even more serious dimension is the erosion of the moral code that creates the attitude "everybody does it."

White-collar crime, like organized crime, is under-reported. When prosecution does take place it is usually done without the cooperation of the business community. Often a company will accept restitution by the employee or prefer to avoid bad publicity by covering up the incident rather than reporting it to police authorities. Lack of confidence in the criminal justice system and an unwillingness to get involved in long court procedures also inhibit cooperation by the business community.

⁷Chamber of Commerce of the United States, *White Collar Crime*. Library of Congress, Card Catalogue No. 74-75321, 1974.

⁸*Ibid.*, p. 5.

B. Implications for Law Enforcement Agencies

While the responsibility for fighting organized and white-collar crime is given to law enforcement agencies at Federal, state, and local levels, these agencies are faced with limited resources and personnel, public apathy, lack of cooperation from witnesses in order to prosecute, and competing pressure from an ever-increasing rate of "visible" crimes. Moreover, while organized crime is "organized" and without territorial limits, the law enforcement system throughout the United States is a collection of largely autonomous decentralized agencies that cooperate at some levels but often compete with each other. Indeed, competition rather than cooperation among the various units of a police department often inhibits effective law enforcement operations.

Increasingly, law enforcement agencies have moved toward utilizing technology and training to develop new strategies against organized crime and white-collar crime. An information system whereby criminal data can be collected, systematized, analyzed, and shared among the units within a police department and among law enforcement agencies at local, state, and Federal levels is a primary step. Intelligence units collect and filter information that can be used for tactical purposes of law enforcement operations in organized and white-collar crime. But even more important, intelligence can be used to detect or anticipate criminal trends. This puts the law enforcement agency in a position of initiating plans of action on a long-term basis rather than merely reacting to criminal behavior.

C. The Intelligence Role

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

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 factor, "best guess." The process which

generates these judgments, descriptions, or facts and near facts, is called the intelligence process. The process involves a series of interconnected functions or activities: collecting pieces of information from various sources; evaluating that information as to its accuracy and usefulness; collating or systematically organizing the information for storage and retrieval; analyzing the information for its meaning and reporting the findings; reevaluating the entire process to assess its weak spots and determine how well the intelligence unit is serving its role within the law enforcement agency (see Figure 1.)

The end product of the collection, evaluation, collation, and analysis process is an informed judgment or simply a factual description of a state of affairs. Each step in the process is essential to the operation of the next function. At the same time there is continuous feedback such that functions performed further down the process indicate more should be done in one or more of the prior functions. For example, it may be found in the analysis stage that additional information is needed which may in turn affect the analysis and final report. The end product might be a descriptive report that may be of use only within the intelligence unit to contribute to an ongoing investigation or study; it might be a link analysis provided for an enforcement unit or special task force of the police department; or it could be a projection of the growth of criminal activity for a geographic area over time for use by the chief of the department.

To categorize the differences in intelligence end products it might be helpful to focus on the use of the material by consumers of intelligence. On this basis, there are two broad though often overlapping categories: tactical intelligence which serves current investigations and strategic intelligence used in developing major cases and for long-range planning.

1. **Tactical Intelligence.** In its simplest form, tactical intelligence support is the answering of requests by enforcement investigators for information on specific subjects and/or locations. The most direct and observable pay-off for a department having an intelligence unit is its ability to use the accumulation of information in its files to assist the enforcement investigators in their daily activities. This form of support is considered to be "intelligence" even though nothing has been added to the information. The fact that the information has been accumulated, filed, and retrieved is an exercise of the intelligence function. It could also be that when a piece of information was filed it was also collated or associated with other data on the subject or location in the file.

When information was retrieved to answer the investigator's query, the analyst might have been able to give an opinion on the meaning of the accumulated information. This would have added "analysis" to the other elements of the process exercised in the intelligence unit's response to the investigator's query. The analyst would be collecting the retrieved information and combining it with his/her own knowledge of the circumstances. The analyst might suggest to the investigator that the subject be found in another location or be involved in additional crimes. He/she may suggest others known to be involved in the specific type of criminal activity with whom the subject might be associated.

To restate, tactical intelligence is the support given by the intelligence unit to investigative units or individual investigators in the course of an investigation. The support consists of responding to queries on the subject under investigation. The information is most often given orally by telephone.

2. **Strategic Intelligence.** Analyzing information in the files in order to assist investigators in probing major criminal conspiracy, projecting potential criminal operation, or producing an estimate of future major criminal activities in the jurisdiction is called strategic intelligence. It is probably the single most important activity in the department since it assists investigators in making "quality" or major cases. Moreover, it enables investigators to get ahead of organized criminals. It allows the law enforcement agency to initiate counteractions rather than waiting and reacting after the fact. By being prepared and alert to potential organized criminal activity, the department can direct its investigators to look for information on expected developments. Finally strategic intelligence is an input to the chief and to his/her planning for more effective action against crime in the jurisdiction.

Examples of strategic intelligence would be:

- An analysis of a particular type of criminal activity—car thefts throughout the jurisdiction, with focus on possible connections with local parts distributors or dealers in other locations. The study would review current activities and project future potentials.
- A study of all types of crime in an area within the jurisdiction to determine the extent to which there are relations among the criminals (or the same criminal committing several types of crimes) and whether there is one or more continuing organizations among the criminals. The study would suggest what might be done to gain further information or launch enforcement action.
- A profile of one major criminal and associates, or of an alleged organization of criminals. The study

FIGURE 1
THE INTELLIGENCE PROCESS

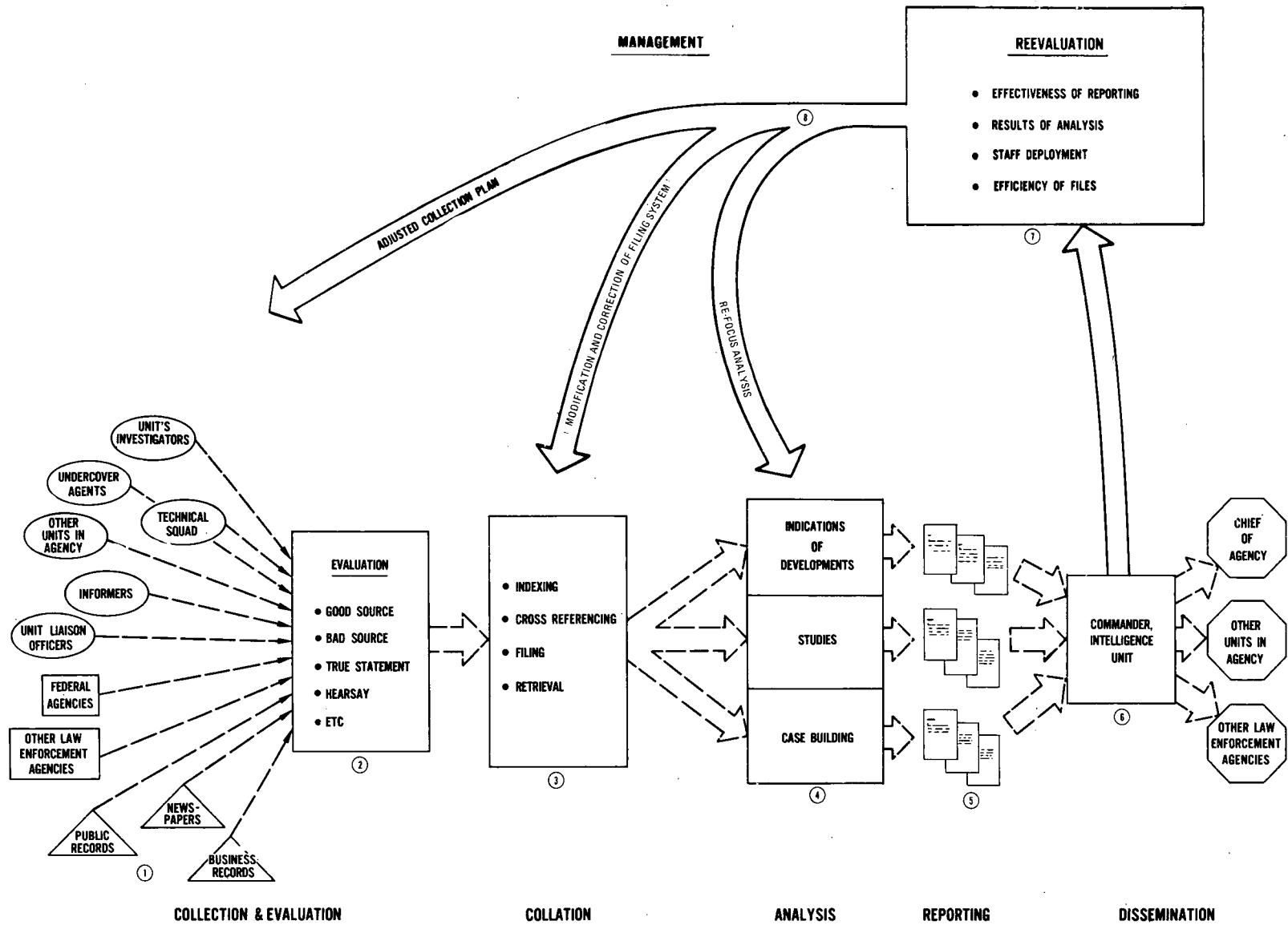


FIGURE 1 - THE INTELLIGENCE PROCESS

<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 a 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, and so forth, 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 reports prepared in the unit before they are sent out.
7.	The connecting link between the intelligence process and the management of the process is the 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 the 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 assets.

would suggest information gaps, potential areas of enforcement action, and future activities of the group.

- An analysis of information on a new form of major criminal activity (at least new in the jurisdiction), proposing what further actions could be undertaken to establish a flow of information adequate to pull ahead of the activities of the criminal group and to prepare for enforcement action.

- An annual assessment of specified categories of major crime, including organized crime, to cover an analysis of the effectiveness of past actions, an estimate of developments in the crime categories over the coming year, and suggestions as to how intelligence and investigative efforts should be focused to successfully overcome these criminal trends.

The larger strategic role of the intelligence unit enables the law enforcement agency to go beyond tactical operations aimed at apprehending individual criminals and to take an overall view of the costs and effects of criminal behavior. By drawing on the expertise of economists, criminologists, accountants, sociologists, computer experts, and other specialists for strategic analysis input, new insights can be gained as to how laws might be restructured or business policies changed to reduce organized and white-collar crime.

D. The Structure 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 these could have a crippling effect on the effective functioning of the intelligence unit. Other activities or organizational sub-elements can be added, but they merely give the operation greater flexibility and sophistication.

The minimum essentials are:

- *Files* containing information arranged for rapid and effective analysis. They should be thoroughly cross-referenced especially in terms of types of criminal activity, as well as biographically.

- A formal, permanent arrangement for the *flow of raw information* to the unit from whatever sources can be tapped: unit investigators, investigators in other elements of the department and other agencies, public and official record repositories, and private data collections where possible and legally defensible.

- One or more persons specifically designated as *analysts*, capable of developing patterns, networks, connections, and new areas of organized crime penetration from the file records and the incoming raw information. 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.

E. Intelligence and the Chief

The principal mission of the intelligence unit must be to support the chief. To fulfill this responsibility, the unit must understand the chief's requirements. Because of the obligation to lead the agency in its effort to reduce or neutralize organized crime, the chief should always have a full picture of the strength, influence, and effectiveness of major criminal groups in the jurisdiction (and neighboring jurisdictions). He/she should have a strong feeling for the weaknesses in the social and economic fabric of the city he/she serves. For example, it is important to know what types of businesses, unions, and social organizations are controlled or penetrated by organized crime and to what degree. Equally, the chief should have some appreciation for which institutions are most susceptible to future penetration—and this includes, of course, the political institutions of the jurisdiction. Finally, the chief must be informed of potential areas for major enforcement actions. A disciplined, imaginative intelligence unit, equipped with proper manpower resources, can provide the chief with support on all of these fronts.

But the chief cannot expect intelligence support to flow up automatically. In establishing the mission and goals of the intelligence unit, the chief must be willing to communicate his/her needs and requirements to the unit commander. The chief must find some time to respond to intelligence unit support, giving the unit commander some ideas of how effective the support is. Finally, only the chief can ensure that the intelligence unit has an adequate flow of information. As will be discussed elsewhere in the manual this is the critical problem. The chief, as commander, must direct that all elements of the command understand and comply. Furthermore, it is necessary to support the subordinates who do not understand the role and function of the intelligence unit.

Flexible use of intelligence materials as a prime tool of management is 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 efficiently to emergencies. These have been the hallmarks of leadership. As the size and functions of law enforcement agencies have expanded, leaders have not always kept pace with the changes taking place. 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 of the budget process.

What has been lacking, too often 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 preparations can be made to preempt them. When planning is done, it is often at the last moment when preparations are by necessity hasty and possibly ill-conceived.

This unhappy picture, admittedly somewhat exaggerated, is a product of shabby 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 to fulfill a specific responsibility. It has been unwilling to use some of the bright minds in its ranks to measure, dissect, or pore over a problem to 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 chief who wishes to establish a sound and effective intelligence unit that can serve all operational levels of the organization (including his/her own) should begin by getting down to basics. The chief must define what an intelligence unit should do and what its functions should be. It is important to have a firm grasp of where the unit should fit structurally in the agency and to understand its minimum essential components. Having been satisfied on these counts, the chief will be in a position to move toward objectives.

F. 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 commander. In most cases the commander is the one who must take the initiative to improve the staff, ensure that there is unfettered access to the agency head, and educate the whole agency as to what it can gain from the activities of the unit.

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

In the struggle for allocating resources, it is the unit commander who must prove the case. The commander's case will be more difficult to prove than other unit heads because he/she will not be able to point to the number of arrests or other concrete indicators as measures of success. Indeed, the commander may have been working closely with other jurisdictions, giving them developed cases, since the statutes of the local jurisdiction are inadequate for successful prosecution. In any event, it is necessary to present a sufficiently convincing picture of the extent and nature of the threat of organized crime operations in the jurisdiction and the effectiveness of the unit's operation in order to gain support.

CHAPTER II

INFORMATION FLOW

A. Introduction

The flow of information is the lifeblood of the intelligence process. Without an adequate flow of useful information, the files will be sparse and not very useful and there will be little material for the analyst to analyze. It cannot be said too strongly that if arrangements cannot be made in a department for a large, continuing, automatic flow of information into the intelligence unit, it would be better to disband the unit. It is a waste of resources to try and continue an intelligence unit that depends only on its own investigative resources for information. There can never be enough investigators assigned to the intelligence unit to provide an adequate flow of information. The intelligence unit must have access to the general flow of reporting on criminal activity to gain a picture of crime in the jurisdiction. This forms the context within which specific information can be requested as the unit focuses on specific areas of actual or potential criminal activities.

Information available to the intelligence unit can come from many sources—from its own investigators, investigators in other elements of the department, the patrol division, other local and state departments of government and the various agencies of the Federal Government. It comes in various forms—the normal investigator report which records information gained on a surveillance or an interview, informant debriefing reports, arrest records and notices of disposition, and unorganized but vital sources of information given orally, either on a person-to-person basis or by phone. It is essential that the intelligence unit establish a procedure whereby a written record is kept of all information obtained orally. Information is also obtained from the public press, law enforcement and other types of periodicals, and public records.

Normally, there are two uses for information collected:

- Tactical or rapid response to assist the investigator in the field
- Strategic or a written report in which extensive treatment is given to a specific type or area of crime in the jurisdiction.

It is important to note, however, that the same information can be used to satisfy both types of requests. The names, addresses, and associations that are

given out over the telephone to investigators are also important to the analyst who is trying to develop a report on the interrelationships among two or three major criminals and their activities.

The unit commander is responsible for developing techniques and relationships to insure that the unit obtains information sufficient in quantity and quality to fulfill its responsibilities. As discussed later in Chapter VI, the unit commander has a very difficult task since he/she must negotiate, request, and beg for cooperation in an effort to gain agreement from other investigative elements in the department to provide the intelligence unit with their reports. To be timely, this information should refer to current cases. But this creates fear that the intelligence unit personnel, not directly involved in the case, may allow the information to leak and thus “blow” the case. In some units there is still concern that the intelligence unit is competing. In a few instances it is a real problem because the intelligence unit investigators are still involved in enforcement actions. These and other problems must be dealt with by the intelligence unit commander in order to achieve the flow of information required by the unit.

It is a basic premise of this manual that the intelligence unit should be prepared to support the department in its activities against all major criminals in the jurisdiction. The efforts should not be restricted to those crimes identified as “organized crime.” This is the basis for the recommendation in the paragraphs below, that the intelligence unit must have access to reporting on the general criminal activities in the jurisdiction. Only in this way can the department be sure that someone is examining criminal activities for associations among major criminals, for the emergence of new criminals, and for interconnections between major areas of criminal activity. The following section examines some of the aspects of gathering and inducing the flow of information from the various elements of the department.

B. Flow of Information from Non-Intelligence Police Department Units

A basic assumption of this manual is that the intelligence unit cannot, with its own resources, develop a flow of information sufficient for its analysts to do an

effective job in the areas of criminal activity for which it is responsible. Ordinarily the intelligence unit is responsible for the traditional vice squad criminal activities, namely, gambling, prostitution, pornography, and shylocking. In addition, it assists the narcotics unit and is frequently responsible for other areas in which there is organized criminal activity such as hijacking, fencing, land fraud, stolen and counterfeit securities, and car theft. Finally, it is responsible for following members of organized crime groups in areas where they operate. There is no possibility that the intelligence unit can produce information on all of these areas with only its own investigators. The basic problem for most intelligence, therefore, is to determine where to obtain needed information and how to get it from units that have it.

1. Information Flow from Non-Intelligence Units in the Department. Basic to the role of an intelligence unit in a department is that the analyst have some way to develop an understanding of crime and crime patterns throughout the jurisdiction. It is essential to establish some context in which to place the criminal activities. The information on the general crime scene can best be derived from the general reporting by the police department as a whole. The intelligence unit should review reports that are given to the chief from the investigation and patrol units. Most criminals (or alleged criminals) who are being studied by the intelligence unit are members of the criminal population of the jurisdiction and are not restricted to the criminal acts in which they indulge. If there is money to be made in narcotics, they push narcotics; but they are also ready to engage in robbery given a good opportunity.

The intelligence unit needs investigative reports and debriefing notes from informers and undercover personnel in the other investigative elements of the department. Ostensibly, this would seem to be too great a review task for the intelligence unit. Yet the unit would not use all of the information but would select that which is valuable. It is imperative that the choice rest with the intelligence unit. In certain larger departments, the problem can be eased by eliminating categories of reports the intelligence unit has indicated are not essential to its task.

The most difficult task in the information flow process is to convince investigators and their supervisors that the intelligence unit can only maximize its assistance to investigators by knowing what is going on, the kinds of cases that are being made, and, therefore, the kinds of intelligence help the investigators require. The intelligence unit, if it is operating properly, will be able to do more than merely run name or address checks for investigators. What is sought is a flow of information that ensures that the intelligence files have the most

complete data on major criminals and their activities that exist in the department. Such a flow would provide the analyst with the data for making connections and associations that can be fed back to investigators as they work on a current case. It should be made clear to investigators and their supervisors that without information on current cases, the intelligence unit can give relatively little assistance. As discussed below, this is a matter of major concern for the chief of the department. Finally, the intelligence unit must have a program to tell the contributors from elsewhere in the department how important their input is and what is being done with it. It is only normal that people will be more responsive if they know they are making a contribution and that its value is being explicitly recognized.

The burden of reviewing investigative reports can be eased if the intelligence unit and the other investigative elements can agree on a reporting format that permits quick review. What is being suggested is a report format with a beginning statement that gives the name of the principal offender and some means of identification, for example, an FBI number, social security number, birthdate. There should be space for names of any associates who were discovered at the time of the arrest or the surveillance and types of criminal activities under investigation. The appearance of these facts at the top in the same sequence would allow the analyst to review the report quickly to determine its usefulness to the intelligence unit. If the cases concern homicide or breaking and entering (primarily street-level criminal action), the analyst would probably pass the material through to be shredded. On the other hand, a quick review of the reporting will give a feel for the various kinds of criminal activity going on in the jurisdiction as well as associations between areas of criminal activity that are known and those where there has been no previous connection. For example, it may be possible to relate certain kinds of burglary and fencing operations. It should be noted that this use of format will serve also to keep the reporting officers aware of the intelligence unit's interests.

Other important sources of information to the intelligence unit are informers and undercover personnel. It is of great importance to the intelligence unit (and thus to the department) that it have access to the informers working with the individual investigators. This is not to say that the intelligence unit needs to know the informers or meet with them. Rather, the unit should be permitted to submit questions to the informers. In most cases, informers live in and are part of the criminal element in the jurisdiction. Since crime is not compartmentalized, they hear much that goes on beyond their specific criminal areas. This sort of reporting furnishes

excellent material to the intelligence unit. Where the allegations or information provided by informants is questionable, it would be placed in a temporary file until further confirmation. (See Chapter III for a discussion of the temporary file.) The department should formalize its approach to informants. One method would be to develop a questionnaire which can be used periodically by investigators to query their informants. (A copy of such a questionnaire is attached in Appendix B.)

While some departments still operate on the basis that informants are the "property" of individual investigators, this approach is ineffective. To maximize the value of informants, a central file should be established in which all informants are listed and their areas of specialty, in terms of knowledge of criminal activity, are noted. Investigators need not be limited to their own informants as a case develops but can request assistance from other informants. A central file also eliminates duplication. An informant might be paid by several investigators without the investigators' knowledge.

The security of the informant can be assured by giving the person a code number. Whenever reports that include this information are submitted they should be referred to by this number. If the system is effective, only the handler and his/her supervisor will be able to connect a name with the number.

Finally, the formal listing of informants as department assets forces an evaluation of their worth. This is necessary so that all who receive information from an informant understand how the investigator, who is running the informant, and the supervisor feel about the information. It is essential that at least two persons know and evaluate the informant. Normally this should be the investigator and the supervisor.

2. Information Flow from Other Agencies. Additional valuable sources of information are provided by other law enforcement agencies in the jurisdiction or those who have representatives there. This would include local and state as well as Federal units. Because of the flexibility of criminals, information is often needed from out-of-state departments. There is a great deal of exchange of information among the regions of the United States today, but recent court decisions and new Federal and state laws affecting the exchange and dissemination of information will influence this. (See Appendix A for a discussion of this problem.)

As a practical matter, the most effective way to enhance the ability of an intelligence unit to gather information from other agencies is to be willing to exchange information with that agency. This requires that a department adopt a policy that specifically states what types of information can be distributed to which department. This is a matter of such importance that the

guidance should be approved by the chief and the specific rules determining what material can be disseminated should be approved by the intelligence unit commander. The decision as to what can be given to which department involves some feedback, formal or informal, as to how a particular department has handled intelligence material in the past. It is important that the intelligence unit know what happens to its information once it is circulated. The unit is still responsible for the material because it was its decision to release it. An intelligence unit can threaten to discontinue an exchange with a unit that has mishandled information in order to ensure better handling of its information in the future.

The department guidelines should restrict intelligence dissemination to other law enforcement agencies which have a need-to-know. Where exceptions are requested by other governmental agencies, the chief should decide, unless this function has been formally delegated to the intelligence unit commander. In such a situation advice from the department counsel or the prosecutor's office might be helpful.

a. Liaison Officers. A most effective way to increase the flow of information from other units is to use a liaison officer. A liaison officer's primary function is to act as a two-way conduit in the exchange of intelligence information. In order to gain the desired types and quantity of information from other agencies, the liaison officer must have information to exchange which has been approved by the unit commander. If the liaison officer cannot exchange information, this person will have a great deal more trouble obtaining the kinds of information sought by the intelligence unit. In order to enhance the effectiveness of the liaison officers, it is essential that they are aware of the major items of information that are needed by their own units and the major cases that are being run by their departments. In a real sense, the liaison officer is running an intelligence operation against the units that are visited. He/she is trying to gain as much information as possible on subjects of interest to the unit. The friendliness of the exercise comes only through an ability to offer needed information in return.

The activities of the liaison officer discussed here are a formal function. It is not considered to be an informal meeting between friends in two departments. It is important to develop close relationships with investigators and intelligence units in other departments, but the goal is to exchange hard-copy information. Where the only exchange that is being given is word of mouth, it is difficult for the receiving intelligence unit to evaluate the validity of the information or to substantiate the source when it is filed. Thus, the objective in the liaison effort should be to obtain as great a flow as

possible of hard-copy or written statements of information.

The actual designation of liaison officers can vary considerably depending on the size of the unit. In most units the personnel pinch is such that it will be impossible to assign an officer full time to liaison duty. This means that the liaison function must be performed by investigators as an additional duty. This in turn puts an additional responsibility on supervisors to be sure that investigators so designated give the proper amount of time to both functions. The case load on most investigators is already very heavy. The only practical answer lies in both the supervisor and the investigator understanding the function of liaisoning and accepting its value. Whenever possible, the units to which an investigator is assigned as a liaison officer should be those that are contacted as a normal part of investigative work—making inquiries, checking files, cooperating on a case, and so forth. By these techniques, the value of liaisoning will be apparent to the investigator and additional work will be minimized. The result will be additional flow of information into the intelligence unit.

In a large intelligence unit, it is possible to have a group of badged personnel as designated liaison to other law enforcement agencies in the area. Ordinarily they would divide up the various units and make rounds to their officers periodically depending on how much information is exchanged and what other problems confront the intelligence unit at the particular time. Also, in large organizations, some of the liaison officers should coordinate and collect information from other elements of their own departments. This is particularly true in large cities such as New York, Chicago, and Los Angeles where there are several levels of investigative units and other specialized operations, all of which are potentially useful to the intelligence unit. These officers should also establish liaison with the local units in the department, either the precinct or district level, in order to enhance the flow of information from patrol units concerning known criminals in their particular area.

Whatever the size of the unit, the fact that most in the police profession are reluctant to talk to unsworn personnel from other units, especially about cases or other investigative activities, mitigates against the use of civilian analysts where they are employed. Thus, the problem cannot usually be eased by assigning the task to a non-badged person, regardless of expertise or trustworthiness.

b. The Team Approach. Another approach to obtaining information for the intelligence unit is to form investigative teams on which the intelligence unit will participate with its investigators and/or its analysts. This is an excellent approach in major cases, especially if the

major criminals are within the normal purview of the intelligence unit. The assignment of intelligence investigators and analysts who are aware of the information available to the intelligence unit will greatly assist the enforcement investigators. The intelligence investigators and analysts, while assisting in the development of an evidential case, will also be able to furnish this information to the intelligence unit for indexing and filing. In such operations information will be developed on criminals and alleged criminals other than the subject criminal or criminals. Once the intelligence unit has committed its personnel to help with a particular case, every effort should be made to encourage continued sharing of information of this type by the investigative unit. It is hoped that as a result, a better feeling will emerge among enforcement investigators. Sharing can become a practical demonstration that the intelligence unit is effective, noncompetitive, and will not misuse the information.

C. Information from Sources Other Than Law Enforcement Agencies

There are also many open sources from which valuable information can be obtained, information that is usually of a background or generally informative nature. The most general source is the newspaper. Here articles appear concerning activities of the various members of the underworld, as well as stories of actions by members of organized crime and by members of law enforcement agencies in other parts of the country. The newspaper should be considered a potentially fruitful source because reporters are very much intelligence operatives. Newspaper stories from other areas can also be useful devices to gain an information flow across jurisdictional boundaries. The possibility of controlled exchange of information with trusted newspaper reporters should be considered. However, it should be done only with the express permission of the unit commander, who in turn should have coordinated with the legal advisor to the department or the office of the district attorney to establish the ground rules for such an exchange to ensure that laws on privacy are not broken.

The usual method of obtaining information from newspapers (and other periodicals) is to clip and file articles, 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. However, when relative cost favors the clipping service (still a high-cost item), care must be taken to be sure the correct materials are clipped and that important items of interest are not overlooked.

As an alternative to clipping, the staff of an intelligence unit can be called upon to abstract articles from 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 newspaper file covering 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 clipping or abstracting, attention should be given to any items about known or suspected major criminals and their associates—their marriages, activities, deaths, and the higher educational focus and marriages of their children. Attention should also be given to stores suggesting new opportunities for organized crime or changes in the operation or management of businesses, indicative of the possibility 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, and so forth. The intelligence newspaper reader should be looking not only for names of known criminals, but also for their lawyers, their banks, and companies in which they or their associates have an interest. It is important to be aware of major deals where a considerable amount of money is involved. Criminals have substantial funds available to buy into legitimate deals, but they usually 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.) Such records 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 provide indications rather than evidential intelligence; 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, and so forth. 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 that 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 contact state and/or local agencies, such as those responsible for overseeing the operation of banks, hospitals, insurance, mortgage and deeds, corporations, and so forth. A list of names, including criminals, their associates, lawyers, and front organization persons, 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.

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 signed or anonymous letters. 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 the person in a position to see, hear, and possibly record facts of value concerning a crime. These people 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 differs from the "informer." The latter is anyone whose mode of living, habits, and personal relations place him/her in contact with criminals. This person's identity must be kept secret for protection and to maintain him/her 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.

D. Intelligence Unit Investigators

It is important that, if possible, all intelligence units have available some investigators under the control of the unit commander. The general flow of information discussed above is essential to file-building in terms of general knowledge of the criminal situation in the jurisdiction. None of these sources, however, is adequate to develop specific information. As an analyst develops an hypothesis, information gaps will appear that must be filled to test the hypothesis. Filling such gaps requires that an investigator obtain empirical evidence. It may mean surveilling one person or a group of persons, staking out a particular address or location, being present in a particular area for a matter of time, or checking records and interviewing persons with direct or indirect knowledge of the particular situation.

The intelligence unit must always be alert for the appearance of frauds and swindles in types of businesses where not reported before. The analyst will require information on how this particular industry or business operates. While the analyst can obtain a certain amount of information by reading and researching, an experienced investigator will still be needed to interview persons and develop an understanding of how the particular business operates.

Ordinarily there is a distinction between field work and office work in an intelligence unit in that the investigator tends to spend a majority of time in the field while the analyst spends most time reading and developing reports in the office. However, in order to give the analyst some understanding of the street investigation, it is well to permit this person to go on fact-finding operations with the intelligence investigator and, in some cases, to allow the analyst to do his/her own interviewing in noncriminal matters.

The role of the investigator in an intelligence unit is more difficult than that of the investigator in an enforcement unit. The intelligence investigator ordinarily does not follow through to an arrest. This can be a very important negative factor for the morale of the unit. In addition, the type of investigation undertaken by the intelligence investigator is, in a real sense, preevidential. The investigator explores certain suggestions of criminality without hard facts and probes gaps in information or tentative suggestions of criminality made by informants. It may be that the validity of the informant is in doubt or the informant was uncertain about the activities.

To be cost effective, the intelligence investigator should avoid operating against street-level type crime and focus instead on major criminals. The latter may be involved in the normal traditional criminal activities or may be a "respected" member of the business community about whom there is some information of fraudulent activities. The intelligence investigator must be prepared to operate in a different environment from the normal street-level investigator. It should be understood that it is a waste of police department funds for the intelligence unit to be used only to collect names and data on street criminals who are already being pursued by the investigators in the enforcement units. This concept is the basis for the argument throughout this manual that the focus of a police department (or a prosecutor's special squad) intelligence unit should be on major criminals in high-priority areas of crime. It should not be restricted to something narrowly defined as organized crime, often restricted to criminal activities that are the target of the vice squad.

The intelligence unit investigator should develop informants just as if he/she were an enforcement investigator. But areas in which some informants operate will be different. The investigator will need help in probing into legitimate business areas such as banking, used cars, wholesale furniture, trucking, and so forth in which there is reason to believe organized crime has an interest. It is from being alert and successfully investigating reports of potential illegal activity that an intelligence unit can determine the outlines of a case. If an enforcement unit can wrap it up quickly, citizens in the jurisdiction can be saved from being swindled out of thousands, if not millions, of dollars.

Intelligence informants should be handled in the same manner as the enforcement informants. The intelligence unit commander should be aware of the identity and the value and reliability of an informant and have proven his/her use before paying from the department informant fund. Investigators will have contacts they will be reluctant to disclose, but no funds should be made available unless they are brought within the system. There is too much opportunity for subsequent charges and counter-charges over the misuse of the informant fund to operate the informant payoff system in other than a most rigorous, controlled fashion.

The intelligence unit investigator, as well as the intelligence unit commander and liaison officers (if there are any), should be alert for cases under investigation by enforcement investigators in which information peripheral to the case but of importance to intelligence can be developed. In such instances it may be useful for the intelligence unit to assign one or more of its investigators to the operation. While help is being provided to the enforcement investigators, the intelligence personnel are also gathering information to fill gaps in their intelligence files. It should be a rule that the intelligence investigator never becomes involved in an arrest situation unless he/she is supporting a fellow officer or preventing a crime. The reason for avoiding the arrest situation is threefold: to reduce or minimize the extent to which the intelligence investigators become widely known; to avoid committing them to the time-consuming operation of appearing in court; and perhaps most importantly, to avoid any grounds for other investigative units believing that the intelligence unit is in competition. Wherever such a belief exists, the flow of information into the intelligence unit from other elements in the department fails to materialize.

Finally, there must be departmental guidelines covering the activities of the intelligence unit investigator. It is imperative that the investigator be told specifically how the new laws protecting privacy impinge on activities.

Improper action on the part of the investigator can lead to a suit busting the intelligence files. It can jeopardize a future case. This manual cannot be specific as to the content of guidelines since they must reflect state laws. However, Appendix A outlines certain major areas that should be covered.

E. Collection Planning

An effective flow of information into the intelligence unit will not just happen. The intelligence unit commander must take the initiative. If not, there will be little or no focus in the information coming into the intelligence unit. Intelligence investigators, if left to their own devices, tend to be unsystematic. They work on potential leads suggested by their informants or given to them by other members of the department. These activities may or may not be important in terms of the goals of the unit. The investigators in other elements of the department will not know of information needed by the intelligence unit. To solve both problems, the unit commander must establish a priority statement of information requirements.

The intent of the collection plan is to integrate three potential areas of information: (1) the investigators assigned to the intelligence unit (but often insufficient to meet the total need), (2) other elements of the department, and (3) other law enforcement departments. The collection plan becomes the vehicle by which the unit commander obtains help from the other investigative units of the department.

In developing the collection plan, the unit commander should undertake a two-step operation. The first part is accomplished within the intelligence unit. The unit commander should request chief subordinates (or in a small unit, all members) to give their views on the most important areas in which the intelligence unit should focus its efforts and the most important intelligence gaps to be filled. The reason this help may be needed from the entire staff is that while the analysts may have been working on important projects, the investigators are knowledgeable about developments in criminal activities. This provides an effective interaction between the analysts and the investigators that assures a successful intelligence unit operation.

The collection plan, developed on the basis of inputs from the intelligence staff, is more than just a statement of information gaps. To develop an explicit statement of these requirements, the intelligence commander must review major criminal activities within his/her responsibility (which should encompass *all* major criminal activity). The commander has to develop an intelligence unit position as to the importance of the several

potential areas of investigation, a priority listing. This then becomes a statement of most, if not all, of the important developing criminal problems in the jurisdiction. It must be remembered that the focus of the intelligence unit is on developing cases to be investigated rather than those already in the hands of the enforcement investigators.

The second step of the collection plan operation is its submission for review, discussion, and approval to the chief (and/or other senior commanders in the department). The plan will give the intelligence unit's appreciation of the most important criminal problems in a priority order. The list should not be too long, probably never more than 10 entries. This is a practical matter depending on the sharpness of the focus and the size of the intelligence effort. It will also indicate major information gaps and suggest how they are to be filled. The recommendations will include an estimate of what can be obtained by the intelligence unit's own resources, what other departments may be able to provide, and finally what must be obtained by the commitment of resources of other elements of the department.

To restate, the collection plan approach is an essential tool of the intelligence unit commander in an effort to make the chief and the other senior commanders aware of the contribution the intelligence unit can make to the department. In particular, collection planning assists in the following ways:

- It periodically appraises the chief of potential areas of criminal activities in the jurisdiction. It is recommended that the periodicity of the collection planning be monthly.

- It enables the intelligence unit commander to obtain agreement by the chief to the potential areas of criminal activity that are outlined in the report. These may be changed in the meetings with the chief, but that is no problem. What is important is that the outcome be a statement of the primary problems of criminal activity in the jurisdiction for the coming months which is approved by the chief.

- Gaining the approval of the chief to the areas of focus establishes the basis on which the intelligence unit commander can rest a case for requiring help from the other elements of the department.

- All of this activity makes this exercise a focal point for the senior commanders and the chief to review developing criminal problems and to plan their efforts to overcome, mitigate, or forestall them. A basic premise of this manual is that the criminal element has many intelligence persons seeking to exploit the public and that the police can successfully combat this element only by effective information gathering and analysis.

CHAPTER III

THE FILING SYSTEM

The criminal intelligence files of a police department have, until recently, generally been considered a storehouse for names. The names included known and alleged criminals and their associates. Furthermore, many of the names were those of lawyers, doctors, and others who may have had some contact with known or alleged criminals. Aside from the question of constitutionality, the bulk of the files were ineffective because information could only be retrieved by name.

This chapter presents some principles to guide the organization (or reorganization) of files to fulfill the needs of the intelligence analysts more effectively and meet the developing legal rules as they apply to the handling of information by law enforcement agencies. In both instances, the results will provide a more efficient collation (information review, indexing, and filing) system that should enhance the effectiveness of the intelligence unit's operation. In particular, the information in the files will be readily available for reviewing a specific criminal activity across the jurisdiction or in a specific geographic area. Both are essential if the analyst is to identify developing situations and trends in criminal activity in the jurisdiction. The suggested guidelines provide a basis on which an intelligence unit can develop its own regulations for filing and disseminating information and purging irrelevant or non-verifiable data.

A. Purpose

The filing system is the storage of data without which the intelligence function is meaningless. Without a high quality store of readily retrievable information, meaningful analysis cannot take place. Yet too often a casual attitude toward filing procedures results in poor organization and breaches of file security as well as inadequate facilities and understaffing. On the other hand, if filing procedures are too tightly controlled, the file room becomes little more than a resting place for carefully kept but seldom used records.

Certain elements are necessary to a successful intelligence unit filing system:

- Guidelines and specifically assigned responsibility for determining the kinds of information that shall be kept in the files, the method of reviewing the material for continued usefulness and relevance, and the method of disposing material purged from

the files considered to be no longer useful or relevant.

- A systematic flow of pertinent and reliable information.
- A uniform procedure for evaluating, cross-indexing, and storing information.
- A system capable of rapid and efficient retrieval of all information.
- Explicit guidelines for disseminating information from the files.
- Security procedures.

Coordination of these elements is vital if the filing system is to function as the primary resource for personnel charged with producing tactical and strategic intelligence. (See Figure 1 for a schematic presentation.)

The intelligence unit commander is responsible for applying departmental informational system guidelines to the intelligence files. The commander must urge that guidelines should cover the collection, filing, and dissemination of information. Growing public concern over the right-to-privacy issue is creating stringent Federal and state legislation governing not only access to information on individuals but also the types of information that can be collected and stored in files. This is of particular concern to the intelligence unit which, by the nature of its function, collects highly sensitive information including allegations that are difficult to substantiate, particularly in the short term. The intelligence unit, even more than other police units, must be scrupulous in collecting, storing, and disseminating information to avoid violation of the right to privacy. (For a discussion of the major legislation governing criminal justice information, see Appendix A.)

A system for routine purging of the files according to fixed guidelines will further insure a viable data collection. Information that is no longer useful for analytic purposes, but which must be kept for statute of limitations or for other legal reasons, should be stored in the most economical manner possible (for example, on microfilm). Reviewing and purging files should be done on a systematic time schedule, according to established guidelines, and under the supervision of the intelligence unit commander or designated senior personnel.

In addition to the legal aspects, selectivity in what goes into the files will insure that the filing system does not become a string-saving operation. It should be a

FIGURE 1

CONTROL AND FLOW OF INFORMATION AND DOCUMENTS

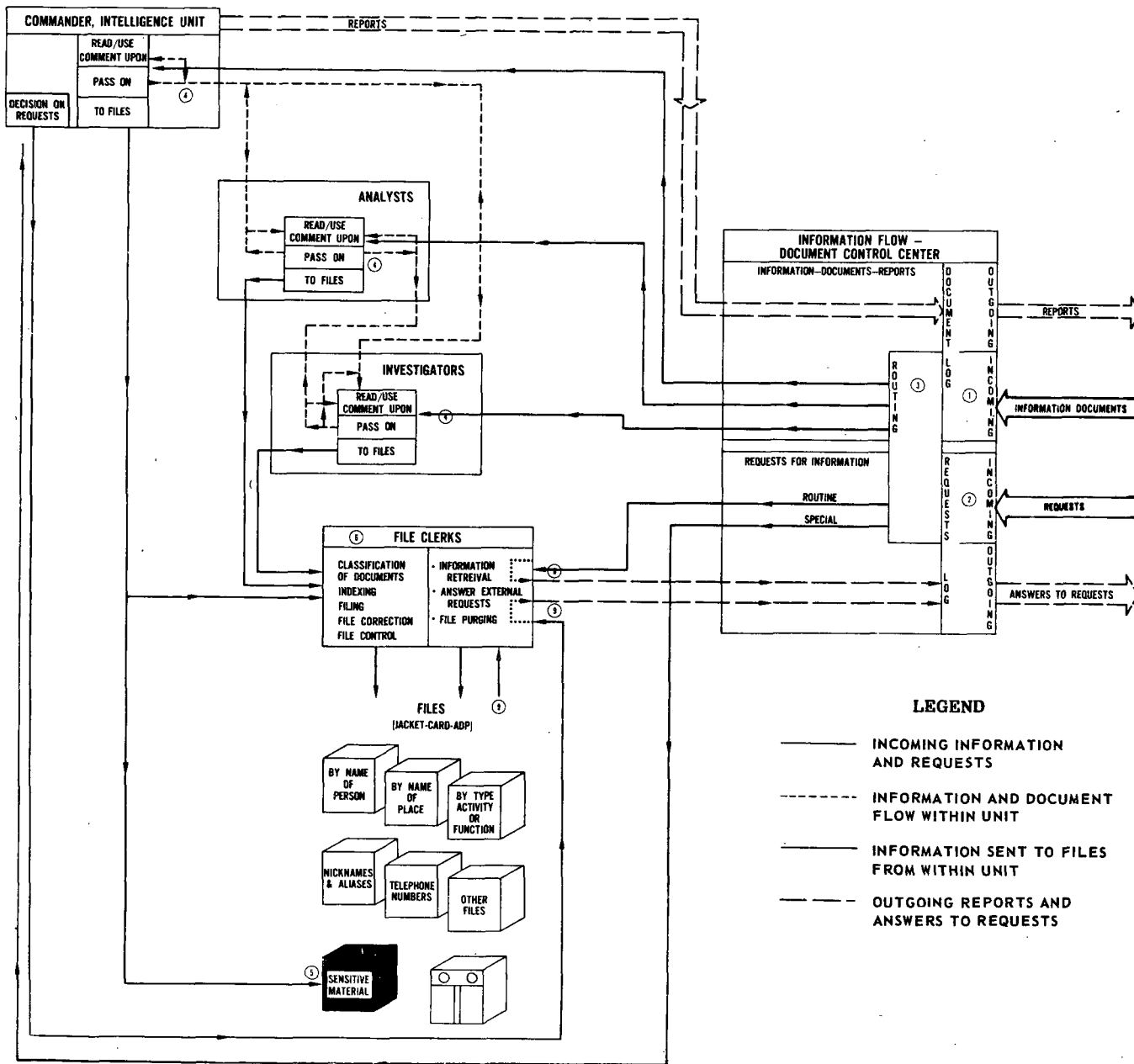


FIGURE 1 - CONTROL AND FLOW OF INFORMATION AND DOCUMENTS

<u>Step</u>	<u>Activity</u>
1.	All documents and pieces of information should enter through a single point in the intelligence unit and be distributed from there. The extent of logging to be done depends on volume of information flow relative to the clerical staff. For items deemed important to record, 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 taking action.
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 <i>read</i> , <i>initial</i> , and <i>pass on</i> . In addition to reading, they may make some <i>comments on</i> items in the material. The material may also be current and they may <i>make use</i> of it by adding to the information they are accumulating on a current research project or a current case.
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 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 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 another designated person) for decision as to how it should be answered and specifically what information is to be given.

cardinal rule that information that is not used or cannot be verified (or at least supported by another source) within a defined period should not be kept in the files. If a certain class of information is found to be valueless or of marginal use to the analyst or investigator, its collection should be questioned. If the information could be made more useful by better retrieval methods, the cross-indexing process may need review.

One approach to the problem of information of doubtful validity is to keep it out of the main intelligence file by creating a temporary file in which to hold such materials. Its status should be determined within a specified time limit, perhaps 6 months. If it cannot be confirmed within the specified period, it should be purged from the temporary file and destroyed. The material in the temporary file should not be allowed outside the intelligence unit since its validity remains in doubt.

It is essential that a systematic approach toward coding and cross-indexing information be used so that when queried, the files will consistently turn out all the information in the file on a person or subject. Of equal importance, the information retrieved should indicate the reliability of the source and the validity of the information. In addition, the files must be structured so that confidential material and sources are restricted to those with a "need to know" and a "right to know." This requires a system for coding information for its sensitivity and securing separate files and guidelines for disseminating file information. It is equally essential that coding, cross-indexing, and general operation of the filing system be performed by persons disciplined in the care, maintenance, and security of the files.

Intelligence unit files should be kept separate from the central records unit of the police department. Due to the peculiar nature of information that is collected for intelligence purposes, it is imperative that security be observed to guard against compromising the intelligence unit. Physical security of the file room, limited access to the files by authorized personnel, and strict observance of legal guidelines for collecting, storing, purging, and disseminating file information will help insure the integrity of the intelligence unit. (See Appendix E for a discussion of security.) Security for computerized files presents unique problems that must be dealt with when the feasibility of computerization is being considered. (See Appendix D for a discussion of computer security.)

Finally, the filing system should be tailored to the specific needs of the intelligence unit. These needs may vary depending on the size of the unit, the type of criminal activity it must handle, the governmental unit within which the intelligence unit operates, and other factors such as geographic location. Above all, the

system must be such that the clerical staff can keep abreast of the flow of information. A highly complex system that bogs down is worse than a simple name index that is used efficiently. A system in which information is backlogged prevents rather than facilitates the effective operation of an intelligence unit.

B. Information Requirements

The basic requirements of an intelligence unit file system arise from requests for information by enforcement units of the department and other user agencies and for strategic analyses by the chief. Strategic analyses examine a specific facet or area of criminal activity in depth and are often inputs to departmental planning. But the bulk of the day-to-day requirements are for information to be used for tactical operations. For example, the intelligence unit investigator may request information to develop and prove a hypothesis about a narcotics ring operating in a given area; the intelligence unit liaison officer (where used), assigned to another unit, might request information about a specific criminal to assist in building a case; or an investigator may need the names and addresses of associates of a suspect who is under surveillance. Most of these tactical requests will require only a search of the name file. But if the intelligence unit is to serve as more than a name file, it must be able to check the requested name quickly against other categories of information—addresses, locations, automobiles, telephone numbers, and most importantly, criminal activity files for a given date. In addition, conclusions in analyst reports that have been indexed and approved for dissemination can be passed on where they are relevant.

Additional tactical requirements for information will come from other units of the police department and other criminal justice agencies including the courts, the district attorney's office, other police departments, state enforcement and prosecutorial agencies, and Federal investigative agencies. Formal agreements can be worked out between the intelligence unit and individual agencies for sharing information according to state and Federal legal guidelines. Only those agencies with a right to know and a need to know should have access to intelligence information. Those agencies having a right to know are Federal, state, and local criminal justice agencies and such other bodies that have the power to subpoena. The need to know requires that the requesting agency state a specific and legitimate need for the information and that the intelligence unit commander (or designee) accept the validity of the need.

The informational requirements of the analysts in the intelligence unit are more demanding. A series of names

and addresses is not enough (see Chapter IV). To be effective, the material should be indexed such that all pertinent information is categorized according to criminal activities, geographic locations, addresses, associates, and modes of operation.

C. Structuring the Files

There are several approaches to organizing the intelligence unit filing system. Selecting the best one depends on the needs of the unit. In some very small units, the file system consists solely of jacket files, in which all reports on a specific individual are filed (in that individual's personal folder.) This traditional approach poses severe limitations to rapid retrieval of information since specific raw data are not indexed and retrieval must rely heavily on the memory of file room personnel who are familiar with the contents of each jacket file. It does not provide a way to determine quickly the extent of information that may be accumulating on criminal activity by geographic area or at a specific location, or by category or subcategory. Thus it cannot provide the analyst with classes of information necessary to establish links or to assess patterns or trends in criminal activity.

This method can be improved by establishing a master name file in which all reports pertaining to an individual are indexed onto a file card that contains the person's name, the report number, date, and the type of activity. The report itself can then be filed according to the file system—in the individual's jacket file, an intelligence case file, or serially by report number. The name-index card allows rapid retrieval of a specific report wherever it is filed by querying the master name file and identifying the report by number or name. The card also provides a quick summary of the criminal activity related to the individual.

1. **Indexing.** None of the preceding approaches to filing provide sufficient collation assistance to the analyst. For this purpose, the file must provide multiple paths for querying the stored information. This can be done by indexing all items of relevant information to the subject or functional category. Normally this is accomplished by using index cards on which the desired amount of information is recorded concisely, with reference made to the basic document. This approach is ideal where a computer is available since the information can be keypunched for direct input to the storage elements. While indexing in this manner takes more clerical time, the cost is more than offset by an improvement in analyst efficiency.

A normal set of card indices would include:¹

¹See Appendix C for sample index cards and for more complete presentation of a model filing system.

- Name (with information as described above)
- Aliases
- Address
- Telephone numbers (with name of subscriber and known users)
- Auto licenses (with owner and known users)

Suggestions as to information to be included on the index cards are as follows:

• **The Name Index.** Should include, in addition to the individual's name, the aliases used and the birthdate. The intelligence report is then indexed onto the name card by recording the date, report number, and the criminal activity or the code for the criminal activity. A new card can be made out each time a report is received or successive reports on the same individual can be recorded on the card. The accumulation of reports on an individual may indicate that an important new criminal figure is emerging. This should be called to the attention of the analyst who may then want an extensive biographic file on the individual.

• **The Alias Index.** Should relate aliases and nicknames to names of known criminals who are called by such nicknames and aliases. Often an informer knows only a nickname. Indexing in this manner may initially help in identifying a known criminal in a new area. The alias cards can also be filed alphabetically in the Name Index File, eliminating the need to check more than one file.

• **The Address Index.** Should, at a minimum, include address, precinct (or area of jurisdiction), and type of premise (residence, bar, restaurant, pool hall). Each report is indexed on the address card as it is on the name card so that reports of activity at a specific address can be quickly retrieved. The accumulation of entries on a specific address may indicate a new focus for criminal meeting that demands further investigation.

• **The Telephone Number Index.** The telephone index file should be restricted to those numbers having useful information. For example, reports of who uses a particular phone, and whether it is a home, bar, or public phone can be helpful. They suggest relationships as to what type of activity is going on or being planned. Other than this type of material, information on telephone numbers is readily available from the telephone company.

• **The Auto License Index.** Is required where either the state has not computerized its license records or the intelligence unit is unable to query a state-computerized system directly through its own console. But even with a computerized system, an index system may be useful to keep track of persons, other than the registered owner, who use a car. A card index is also important where out-of-state cars become involved in criminal activity in the jurisdiction.

- Further improvements to the filing system can be achieved by including a *criminal activities index or abstract file*. Indexing by criminal activity is one of the most useful tools for an analyst, since all information received on a particular criminal activity is in one place and can be readily retrieved. This index can be used, for example, to probe the interrelationships among criminals committing similar criminal acts in various parts of the jurisdiction. It can also be used to suggest individuals who may be involved in criminal activity where the criminal is unknown but the type of act and mode of operation are known.

The criminal activity index classifies crimes into categories and subcategories of criminal activity. A numeric coding scheme such as the Dewey decimal system can be used to ease the recording process. The criminal activity index can also serve as a more complete record in the form of an abstract of the pertinent material from each intelligence report, and includes the date and reference number for the basic report. Another very simple approach to a criminal activity index is filing a copy of each intelligence report according to the criminal activity classification described in the report. If more than one activity is described in the same report, a copy can be filed for each type of criminal activity reported.

- Two other useful indices are a *biographic form* and a *location index*. A biographic form is based on the belief that it is necessary to gather all information possible in one place concerning major known or alleged criminals in the jurisdiction. This is of great assistance to the analyst in responding to requests for information on such "important" persons. The usefulness of the approach is greatly enhanced if the form is kept up-to-date and has an index attached to it recording the base documents from which the biographic data are derived.

The concept of a location index is based on the belief that the analyst needs devices to help determine associations between areas of responsibility and other criminal activities. The location index form offers a place to abstract a brief note concerning all reported crimes (or at least those categories of criminal activities of interest to the intelligence unit) occurring either at a specific location or in a selected geographic area. This index can be useful in detecting criminals and for discovering associations among criminals who engage in different types of crimes, for example, narcotics and fencing, or fraud and shylocking. It is the law enforcement agency that categorizes crime and observes jurisdictional boundaries, neither of which is of concern to the criminal.

In all three of these major indices—criminal activities, biography, and location—each report should contain a

brief abstract of the important points. If done correctly, the need for retrieving the basic report would be reduced and in many cases eliminated. The abstract should include names of known or alleged criminals, together with a concise statement of their reported activities, and where and when they occurred. Often this is enough for the analyst to link persons, persons and locations, or criminal activities and persons. By xeroxing the forms as new abstracted information is added, the analysts can have updated information on their assigned areas of crime at all times. These data can be referred to as the analysts review the daily flow of new information and as an aid to understanding its meaning. In these circumstances, the analyst does not have to get the reports or ask the clerks to bring out all of the basic reports. Hence, much clerical and reading time can be saved. The cost is in terms of analyst time to indicate what information is to be abstracted and of clerical time to put the abstracted information on the forms.

2. Basic Report Filing. One final decision with respect to the filing system is how and where to file the basic reports. Often the basic report, once indexed, is filed in a jacket file of the most important person mentioned or in a criminal activity file which is central to the report. Some agencies have a system in which intelligence case numbers are given to certain major criminals, types of criminal activity and areas, and the basic documents are filed accordingly after being indexed. In either of these cases, if the report refers to more than one person or type of criminal activity, each must be recorded on its own index card and cross-referenced to the jacket where it is filed.

The recommended approach is to file all reports in series once they are indexed. Analysts and clerks can rely on the cross index files and abstracts for their searches. The faster and easier these basic files can be stored and retrieved, the more time clerks have to maintain the indices and abstracts. If a simple serial number system is used to file basic reports, the file clerk need not search for specific name or activity files in which to place them but only to file them serially by the document control number. The clerk will also find it easier to locate reports because they will all be filed in the same place.

3. Questionable Reports on Alleged Criminals or Their Associates. The file system must take into account the problems raised by the new statutes directed toward protecting privacy. It is no longer possible to enter all information on individuals into the files automatically as it is received. Each item must be subjected to the test of relevancy and to its legality under the department's guidelines (which are, in turn, based on the appropriate state and national laws). There is little problem where

the information relates to a known criminal and is developed during an active case in which searches have been carried out with warrants. What is touchy is the decision on allegations where the source is not known or has not been totally accurate in the past, or where there is no criminal record on the subject.

One approach that may help resolve or at least minimize this problem is the use of a *temporary file*. The operation of the temporary file would be based on the following ideas:

- The file is primarily for reports on individuals rather than on activities.

- The analyst (or whoever has the responsibility for deciding on material to be put in the files) should put reports into the temporary file if the main file has no other information on the principal subject in the report and if the investigator has indicated on the report serious reservations about the accuracy of the source on this particular subject.

- If the report has references to several subjects, only one of whom fits the above definition, all subjects should be indexed into the main file except the name in doubt. That name should be noted in the temporary file until its final disposition is determined. If the doubt is removed then the name will be indexed into the main file.

- It is essential that information in the temporary file *not* be disseminated outside the intelligence unit (except to other elements of the department with the express approval of the unit commander and the understanding that it is not to be used in any manner which might cause it to be circulated).

To enhance court acceptance of this approach, a time limit must be placed on how long the material can remain in this file while its validity is being checked. The time may be short when the intelligence unit uses its own investigators on a priority basis. More time may be required when requests have to be made to other elements of the department or other agencies for assistance in finding corroborating information. Finally, if the allegations relate to relatively unimportant activities, no investigative action will be called for and dependence will be put on the daily flow of reports. But a maximum time must be specified; a reasonable time would seem to be 6 months. If no acceptable supporting information is received in the stipulated time, the information must be removed from the file and destroyed. In this manner the privacy of persons against whom allegations cannot be supported can be protected. Where the information is corroborated, it should be indexed and entered into the main file.

The temporary file may simply be one in which the basic reports are filed chronologically, by name, or by

criminal activity. Alternatively, a miniature index file can be established for examining this information in several ways. The basic reports would be filed chronologically. Another approach followed by some organizations (New Jersey State Police and Washington State Police) is to maintain the temporary nature of selected reports on individuals where the fact of criminality is in doubt by indexing that report on special colored cards and/or putting colored tabs on the reports. The result is the same. File room personnel are alerted *not* to disseminate the information so marked. Special purging procedures can be stipulated for this material. How the individual department chooses to act will depend on the number of reports in the file and how often it is used by the analysts.

4. Sensitivity and Reliability of Information. The need to mark information to indicate its sensitivity and reliability is often overlooked in intelligence information handling. While most intelligence units tend to be overcautious in "holding closely" material from a sensitive source, the report is not necessarily marked in any way to inform future readers. Moreover, the sensitivity of information relates both to its source and its content. For example, information that could only have come from a source close to the inner circle of a criminal group would be sensitive because, should any group member learn that the police had the information, the informant could be identified. At the same time, information on the groups might indicate that they were engaged in certain activities which, were the initial information to leak, could "blow" the eventual enforcement action against this group of criminals. Thus, a single report can be sensitive in terms of source and substance.

In order to protect sources that are considered sensitive, as well as to protect operations based on the substance of information received, the intelligence unit must have a means for indicating the degree of sensitivity of the information. The material can be marked with a numerical or letter code that can be associated with the report as a whole or parts thereof. Determining sensitivity is usually the responsibility of the person or agency forwarding the information to the intelligence unit. However, in certain circumstances the intelligence unit classifies information because of its awareness of other information.

Defining degrees of sensitivity is sometimes difficult. In large measure, this is because all information that enters the intelligence system is considered confidential. Thus, ordinarily information in the intelligence system is classified either as "confidential" or as "sensitive," meaning it must be controlled by the unit commander and not circulated through normal channels. This

confidential classification is necessary to protect the integrity of the system as well as the privacy of the persons to whom the information relates. Hence information in the intelligence system must be circulated only to those with a right to such material (for example, a law enforcement officer) and a need to know (working on a case where the data are relevant). To classify information above confidential, that is, sensitive, should mean that the originator believes access to the information should be restricted. Thus, it cannot be processed in the normal manner and entered into the general intelligence file (at least on a current basis) but must be kept in a secure file to which access is limited to those receiving express permission by the unit commander.

Reliability of information, on the other hand, poses an equally demanding problem. The bulk of material the intelligence unit receives is allegations, most of which may at least initially be unverified or of an unknown quality. There may be doubt about the accuracy of the source, or information already in the files may dispute the new information. The subject of the information (either a person or activity) may be new and further investigation may be required. Therefore, it is imperative that the originating source indicate the reliability of the information on the report. In some cases, the analyst may give the information a second classification as to its reliability that is based on knowledge of other related material in the files.

An understanding of the reliability of information is also essential to protect the privacy of individuals. The intelligence unit must be wary of circulating information, the validity of which is in doubt. But if the material must be circulated, the intelligence unit must state its reservations clearly on the report. An example of the need for care in handling such material is an allegation received about criminal acts of politicians or civil servants. Such reports must be treated with special care because such allegations may have been made for political reasons. Furthermore, in such circumstances the tasks of classifying information as to sensitivity and reliability are joined.

Table 1 presents one approach to coding material for its sensitivity and reliability. For the reasons cited above, the two classifications are deemed necessary for sensitivity. The material is either believed to be sensitive and treated accordingly, or it is simply treated as confidential. The reliability of coding is based on the belief that two factors should always be taken into account in determining the reliability of the material, namely, the source and the substance of the report.

Rubber stamps can be made so that material can be marked "Sensitive" or "Confidential." The codes for sensitivity (SS or SC) are for ease in marking index cards. Highly sensitive material should be stored in a safe with access limited to the unit commander or other designated persons.

TABLE 1

SUGGESTED SENSITIVITY AND REPORT EVALUATION CODES

Sensitivity Coding

Sensitive (SS)	Must be closely held to avoid jeopardizing the source or the initiation of an important investigation	Material so stamped must be stored in a locked file under direct control of the unit commander or his/her designee
Confidential (SC)	May be circulated in and outside department to law enforcement officers with need to know	Standard operating procedure for handling to be established by unit commanding officer and approved by chief of department

Reliability Coding

Source:	Law Enforcement Officer	A
	Source known and reliable in past	B
	Source known but not always reliable	C
	Reliability of source unknown	D
Content of Report:	Factual	1
	Probably true	2
	Factuality unknown	3

D. File Room Procedures and Operations

1. **File Clerk Functions.** Information to be incorporated into the intelligence unit's file system will usually be in the form of a standard investigator report. It will be reviewed by the analyst (or the person given this function) who will underline or circle information on the report that is to be indexed and coded in the files. Based on these instructions, the file room staff should perform the following tasks:

- With respect to all names underlined in a report, the file clerk should check the name file for an existing card on the individual and record the report number, date, and activity on the card. If no card exists, the file clerk should fill out a name card file and record the information on it. (Departmental procedure may require that a new name card be filled out each time.) If there is a number of referrals to a specific name in the file, it should be called to the attention of the analyst.

- Alias names should be checked in the same manner, instituting a new card where none exists and, where known, cross-referencing the individual's legal name on the alias file card.

- Addresses underlined in the report should be checked against the address file, following the same procedure as in the name check. If a number of reports have been indexed against a specific address, the file clerk should alert the analyst. It may indicate that new criminal activity is developing and further investigation is required.

- The type of criminal activity and/or the analysts' abstract (if there is one) should be recorded in keeping with the procedures of the filing system. At a minimum there should be a criminal activity index card on which the report number is recorded. The name index card should also indicate type of criminal activity.

This process should be followed for all other file classifications included in the file structure.

2. **Forms.** Size of forms to be used in the filing system should be determined by need. For simple name index files the 3x5 cards allow for more extensive recording of information and for indexing successive reports onto the same card. The letter-size 8½x11 inch form can be used for biographic, location, and criminal activity files where extensive information is needed. All file forms should be of the minimum size to contain the necessary information without wasting file equipment and floor space.

Colored forms are useful for segregating files, for routing forms to other departments, or for facilitating file purging. A color can be used to coincide with the time schedule for reviewing and purging the files. Thus, if green name cards are used for a specific period, they

provide a quick visual indication of which records should be reviewed for purging.

3. **Mechanical Filing Aids.** As the activity of the intelligence unit grows, it may move (resources permitting) toward greater mechanization of the filing system. Space and the rapidity with which technological advancements are made prohibit a lengthy discussion of the many mechanical aids available. However, unit commanders should be aware of three widely used methods of increasing the efficiency of the file system—the photocopying machine, microfilm storage, and computerization.

The use of photocopying equipment for reproducing copies of records and reports greatly reduces the need for clerical time and effort. It is possible to reproduce a number of copies of the intelligence report for each file classification and eliminate other file forms and cross-indexing procedures. One copy would be filed in the name file according to the name or names in the report, another in the address file, and still another in the criminal activity file. This eliminates the necessity for filling out file forms. However, the thin paper of the photocopy is less easy to handle in filing than the heavier file cards.

Microfilm is an efficient way to store records where space becomes a problem, particularly where records must be kept but do not need to be in the active files. Yet microfilming presents problems in reviewing and purging the files and should not be used indiscriminately. It is best used for records that are needed only for legal purposes or seldom utilized. Furthermore, microfilm readers also utilize space in the file room so calculation of space saving should include this element.

It is conceivable that, in time, computers will be more efficient and economical for even the smallest intelligence unit filing system. Because of the increasingly complex operations of organized crime, law enforcement agencies within and among the states realize the need to share information and to utilize to fullest advantage the storage and retrieval benefits the computer can provide. Along with the advantages, however, computerization poses a myriad of security problems that increase with the number of agencies sharing the system. These problems must be dealt with if the value of the automatic data processing approach is considered essential. (Computer security is discussed in greater detail in Appendix E.)

The intelligence unit, anticipating that it may convert to computers, should select a format of reporting that is conducive to the system it plans to adopt. For example, on some forms it is a simple matter of adding a numerical code to each information box. This allows the information on the form to be fed into the computer and retrieved as needed.

4. **File Room Security.**² 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 without fear of compromising sensitive information. They should also be confident that the integrity of the information in the files is secure.

a. **The Office.** To achieve the desired security, access to the file room should be restricted to intelligence unit personnel. A log should be kept of all non-unit people who enter the intelligence unit's area. In a larger unit a receptionist may handle phone calls and the logging-in of visitors, but in a small unit this function may be combined with file room responsibilities. A system should be devised to identify all persons other than intelligence personnel coming into the intelligence unit area. Furthermore, the file room must have additional controls, a controlled area within a secure area. The physical layout of the intelligence unit is important to assure security needs.

During working hours, one person should be responsible for admitting visitors to the intelligence unit. A person should also be in charge of the files and their security. When no one is on duty, the intelligence unit area must be secured by electronic or mechanical means that will trigger an alarm should anyone attempt to make an unauthorized entry. This is particularly applicable to the file room. The alarm should ring in a command center which presumably is staffed 24 hours a day. Access to files during hours when no one is on duty should be controlled by the unit commander.

b. **The Files.** The records can be kept in ordinary metal filing cabinets if the room itself is secured. If there is a problem securing the file room, the files should be equipped with locking devices with the person in charge of the file room, the senior analyst, and the commander of the intelligence unit holding the keys or combinations to the locks.

E. Guidelines

This chapter has reviewed the importance of the file system to the operation of the police intelligence unit and to the other investigative elements of the department. The system must be prepared to support rapid response requirements from investigators on current cases. It must have collation procedures that will assist the analytic effort in probing a criminal or a criminal activity in depth and/or across the jurisdiction.

²See Appendix E for an extended discussion of security measures.

The new Federal and state laws establishing new legal bases for collecting, filing, and disseminating intelligence information add another dimension to the importance of the filing system. It must provide support to the intelligence unit and to the department as a whole and maintain procedures for determining the types of informational assistance that will be extended to other law enforcement agencies. But now it must also have its operational procedures within the legal framework set by Federal and state laws to ensure the continued, unobstructed operation of the intelligence unit.

While the emphasis in these statutes has been on controlling the dissemination of information on individuals, more attention is being directed toward collecting and storing files on individuals. Because of the peculiar nature of information collected by intelligence agencies which, by necessity, includes obscure and often unsubstantiated information, more stringent laws are being devised to control the collection, storage, and dissemination of intelligence data. The Criminal Justice Information System Act of 1974 (S. 2964, H.R. 12574) limits dissemination of intelligence information to criminal justice agencies and only to those with a specific need to know as well as the right to know. In addition, it imposes the obligation on every criminal justice agency to "keep records current and accurate."

The necessity for periodic review and purging of the intelligence unit files is twofold:

- To insure that the data bank be kept in a manageable and useful form by providing a means for re-evaluating the information in the files, and

- To provide further safeguards for insuring individual right to privacy guaranteed in the U.S. Constitution and reinforced in Federal, state, and local statutes.

Much of the reviewing of intelligence information is done on an ongoing basis as the analyst evaluates data that flow back and forth between the file room and his/her desk. Nevertheless, to insure that reviewing and purging are done systematically, a time schedule should be developed. It is recommended that the review be continuous so that there is no greater workload that might destroy the system because there are not enough personnel. General criteria applied to intelligence data for reviewing and purging should include:

- Frequency of use When was the last time the files were queried for this information?
- Value How useful is the information to the analyst? to investigators? Does the original purpose for collecting it still exist? Is it potentially useful?

- Reliability Has the information been substantiated?

- Completeness and accuracy Is the information complete? Does it need updating?

A rating system should be devised for identifying data that should be purged. This can be done by rating the data against a checklist of the critical elements. This checklist might include:

- a. Cannot be substantiated
- b. No file entry for 5 years from the last file entry
- c. No criminal background
- d. No association with organized crime figures, gangs, militant or subversive groups
- e. Storage of data violates a state/Federal statute
- f. Approval for purging by supervisor
- g. Approval for purging by commander of intelligence unit

No file will be purged unless elements f and g are present along with one or more elements a, b, c, d, or e. When all requirements are met for purging, the information should be destroyed by shredding or incineration.

It should be noted that the above-suggested approach to purging guidelines has reference to the main intelligence file. The handling of a temporary file should be kept separate and its operation covered by special instructions.

It is beyond the scope of this manual to review all the statutes governing intelligence data. Laws and guidelines are being worked out at the several levels of government. Guidelines for the intelligence unit file system should be developed under legal guidance and submitted for review to the district attorney or the state attorney general. The importance of developing filing system procedures for intelligence files that conform to the new, still dynamic, legal basis cannot be overstated. If this is not done, the files can be exposed and disrupted, destroying the intelligence unit's operational capability.

CHAPTER IV

ANALYSIS AND REPORTING

A. Role of Analysis

Analysis is a normal function of the police investigator. The investigator accumulates information (evidence) and reviews it according to the logical steps in reconstructing a crime. Analysis is a logical thought pattern that the investigator never considers a separate function. When assigned to a case, the investigator begins by establishing the information needed and planning how to obtain it—asking questions and surveilling suspects. At the same time, the investigator constantly develops ideas about who committed the crime and how it was committed and discards those that do not fit the facts as they are accumulated. These ideas can be described as hypotheses. Such hypotheses are the basic tools of the intelligence analyst as well. Yet analysis in the intelligence unit, unlike that done by the investigator, is a separate function to be performed on a full-time basis by one or more intelligence unit personnel.

Analysis is the key to the success of an intelligence unit. Without the explicit performance of this function, the intelligence unit is nothing but a file unit. It may have much information that is helpful to enforcement investigators, but such information must be given direction and meaning. This is not always an easy task. For example, new criminals or criminal activities may not fit known, normal patterns.

That analysis has been discussed as a separate function should not be considered a contradiction to earlier assertions of the continuous overlap among all phases of the intelligence process. The distinctions between analysis and other phases presented here are not absolute. For example, there apparently is a one-way relationship between the products of investigative activities and the intelligence report, namely, an intelligence report is the direct result of the collection of a particular body of information. However, the same report can also indicate (or state) a requirement for information which leads to collection activity. Similarly, the relationship between analysis and other phases of the intelligence process is not always apparent. Collation (the process of systematically sorting and classifying information) and analysis (the activity by which raw information is transformed into intelligence) are often performed simultaneously. Thus, although analysis is a unique phase in the intelligence process as we have

defined it, the distinction between analysis and other activities will not always be clear-cut.

Despite the lack of precision in setting out analysis as a distinct phase in the intelligence process, no problem exists with respect to the activities of an intelligence analyst. This is especially true when analyst activities are compared with those of an investigator. Generally, the investigator provides the analyst with raw information while the analyst processes and relates this raw information to existing data and develops suggested avenues of approach to the investigator. Analysts, utilizing information supplied by investigators, make judgmental decisions concerning the short- and long-term implications of criminal activity in terms of tactical operations and strategic assessment. The investigator uses intelligence information to make decisions regarding particular enforcement operations. Their activities are highly interdependent, but the overall responsibilities of the investigator and analyst are necessarily distinct, allowing the analyst to maintain a broad view of criminal activity while the investigator focuses on specific enforcement problems. The analyst looks beyond specific cases to ascertain the similarities and differences among many different cases. Field work should therefore not occupy a significant proportion of the analysts' efforts since the time spent in investigative work is not likely to contribute to the analyst's general knowledge of his/her area of responsibility.

B. Duties of the Intelligence Analyst

The analyst is responsible for performing several specific tasks relating to the processing of new and existing information. The major duties are presented here. It should be noted, however, that the nature of these duties and the personnel responsible for them will vary from unit to unit. In small units the unit commander or the deputy may perform the actual analysis. In some units the person responsible for the files may also do analysis, while in larger units one or more persons may perform analysis on a full-time basis. The analytic activities presented here must be performed by an intelligence unit, but do not comprise a statement of the duties of a specific person or job position. These are:

- Reading and indexing incoming reports

- Developing and maintaining, as personal tools, files and sources of information that relate to the analyst's particular responsibilities

- Identifying information requirements
- Performing research and analysis as required
- Preparing intelligence reports

1. **Reading and Indexing.** It is the analyst's responsibility to review promptly reports and other routed materials. The analyst must concentrate on how the material contributes to his/her area of responsibility rather than simply reading the material for general awareness. In this sense the information requirements of the analyst differ from those of the investigator. The analyst should continually refer to a list of information requirements and tentative hypotheses about crime in the area. In this way previously identified gaps can be filled.

A corollary to this activity is a systematic review of daily newspapers and other periodicals to discover leads to potential new areas of crime in the jurisdiction, criminal activities in other jurisdictions that may occur in the future in this jurisdiction, and new approaches being used in other jurisdictions to fight old and new forms of criminal activity. Several analysts may share responsibilities for reading a number of periodicals. Each must be aware of the general interests of the others in clipping an article for review and routing it to the analyst responsible for a particular subject area. Reports and periodical articles considered potentially useful and retained in the files must be indexed by the relevant subjects. The analyst decides whether or not to retain an item and how it is to be indexed. If in doubt, the analyst should consult others before discarding a potentially useful item or burdening the filing system with useless information. Similarly, information that relates more to the interests of another analyst should be passed on for a decision regarding indexing.

While reading, the analyst will indicate how a report is to be indexed by underlining the appropriate items such as names, addresses, license numbers, and dates. Lengthy reports should be abstracted and the filing category in which the abstract is to be placed should be noted. The abstract informs the user of the contents of a report or article; it functions as a table of contents and hence should be a brief, concise statement of the contents of the particular file. A list of the headings under which the item is indexed should also be included on the abstract form.

The files of an intelligence unit are among the analyst's most useful tools. As such, a continuous flow of inputs to the intelligence unit's central files is critical. The quality of the file contents and the utility of the filing system as a whole depend on the care with which

reading and indexing activities are undertaken. These duties should be performed systematically to insure that all relevant and practical sources of information are reviewed and properly integrated into the filing system.

2. **Developing and Maintaining Information.** Each analyst should develop and maintain personal "tools"—lists of names, sources of information, association charts, tentative hypotheses, operating assumptions—that help him/her keep up-to-date on trends and new developments in his/her area of responsibility. Such tools comprise the analyst's personal files and contain unverified information and tentative hypotheses the analyst has formulated about major criminal activity within the area. These are readily available for the analyst to review while reading incoming reports. It should be noted that use of the word "personal" is not meant to indicate that the analyst can consider work files as personal property and take them along when changing assignments. Like all information in the intelligence unit, the information must be considered confidential and dealt with in the manner prescribed by departmental regulations.

What is being suggested here is that each analyst focus, assemble, and analyze current information in terms of the accumulation of data from past reports received according to his/her own approach to analysis and to personal work habits. Approaches differ widely, but all analysts need a personal information-abstracting system to be systematic and effective in determining the meaning of newly acquired data.

The types of information utilized in maintaining personal tools will certainly vary among analysts, but some generalizations may be made. Several examples of such working files and categorizations that augment the information contained in the central files on an *ad hoc* basis are as follows:

- Names of criminals known or believed to be operating in the analyst's geographic or functional area
- Lists of personal sources of information
- Names, locations, and overt and suspected covert activities of business establishments
- Up-to-date link diagrams of associations, both verified and hypothesized, among criminals
- Untested or partially tested hypotheses and supportive or disconfirming evidence that may be brought to bear and further evaluated against new information
- Documentation of current project activities including successes, failures, uncertainties, and planned future inquiry
- Day-to-day tabulations of data being collected

The characteristic common to the above tools is that they provide the analyst with an orderly, traceable

structure to his/her investigations. By imposing logical structure and systematic order on a diverse collection of raw data and seemingly unrelated facts, successful analysis can be undertaken. The analyst uses personal files to impose order on the unverified information and massive array of data that are brought to bear on analysis.

The organization of information drawn from reports should not interfere with the normal flow of information into, or the analyst's use of, the central files. These are not substitute files but rather repositories of supplemental information which will help the analyst understand his/her area of criminal activity. Furthermore, personal files are not so large that the analyst spends much time performing the duties of a file clerk. Finally, the analyst must be careful to avoid breaches of security, including data from sensitive reports in his/her own material.

3. Identifying Information Requirements. The analyst is responsible for maintaining, on a continuous basis, a list of information requirements or questions which, if answered, would add to an understanding of developments in his/her area of criminal activity. The nature of stated information requirements may vary, but they should be as specific as possible and justifiable. Most commonly, information requirements arise from uncertainties which have been identified either by hypothesis or in a collection plan. Deriving requirements in this manner enables the analyst to express uncertainties as specific questions to which collection efforts may be directed.

The analyst has a special responsibility to recommend priorities among the information requirements. In a current major case, any information that would contribute to a successful enforcement action would almost automatically be considered important. But information requirements also grow out of an analyst's hypothesis. If the analyst is right, it could result in an important arrest; if mistaken, it would be a wasted effort. The analyst must prove a need for information in the second type of requirement. As a practical matter, the workload may be so great that, though winning the argument, information gathering must be postponed until the investigators have time. The generalization is obvious—requirements posed by current cases tend to be given high priority. The analyst and the unit commander must press for attention to non-current and strategic requirements.

In a sense, the identification of information requirements is among the most important functions performed by the intelligence unit. Asking specific questions provides direction and focus for investigators and other field personnel, thereby most effectively utilizing search resources.

4. Performing Research and Analysis. Research is simply defined as an in-depth investigation of a given problem for discovering new facts. It is perhaps misleading to equate research and analysis, but they are treated together to emphasize the similarities between them. Both are based upon the thorough examination of a specific problem directed toward a more complete understanding of criminal activity. Specific steps for conducting intelligence analysis and research are treated in greater detail in Appendix F. The present section will only briefly outline the analyst's role in intelligence research.

In most cases, research will be undertaken to provide information on a subject with which the analyst is somewhat unfamiliar. In this respect, research differs from analysis; research is more concerned with basic information gathering and organizing, while analysis assumes that this activity has been largely completed. The analyst undertakes analysis to learn of a new area of crime, a new racket in his/her area of responsibility, or suspected activities of a group of criminals previously inactive in the analyst's area. As is the case with most activities in the intelligence process, the key to successful research lies in a systematic, thorough procedure from the initial formulation of a problem through information gathering and conclusions. Often, when research is required because the analyst has limited experience in a particular area, the in-house information which may be brought to bear on the problem will also be inadequate. Analysts must therefore be familiar with information resources outside the department. Specialized supplementary information may of course be obtained from libraries and other public sources, but the analyst should also be prepared to develop his/her own sources as required.

5. Preparing Intelligence Reports. The subject of writing the intelligence report will be treated in greater detail later in this chapter. This discussion is designed simply to outline the analyst's responsibility for the production and dissemination of the results of his/her efforts.

The intelligence report is designed to inform the reader of the *findings* of an analytic process. Although the written intelligence report is the most formal and perhaps most desirable medium for disseminating the results of analysis, in many cases the intelligence information provided by analysts will be given informally over the telephone or in person. It is essential that such oral communication, whether in response to requests or initiated from within the intelligence unit, be put in writing and filed for future reference.

The analyst assumes primary responsibility for producing written intelligence reports. These may be

specifically requested by an operational unit or administrator or they may be periodic reports initiated by the intelligence unit. In either case, the report should be explicitly stated and the summary and conclusion presented at the beginning of the report. Although the report should present an overview of the underlying steps and assumptions contained therein, an intelligence report should not laboriously detail the research process. Such material need only be highlighted and documented to the extent that the reader can estimate the validity of the findings. As a final note, all analyst-written reports should be indexed into the main file so the analysis is not lost and has to be redone at a later date.

C. Techniques

In carrying out the general functions of analysis in the intelligence process discussed above, the analyst can expect to be called upon to bring some specialized techniques to bear on the problems in his/her area of responsibility. These are not so much specific analytic techniques as they are methodological routines. In this section these are discussed as a set of procedures that should be developed by the analyst until they become routine work habits. Such techniques are not unique to intelligence analysis; they are utilized to some degree by virtually all law enforcement personnel. What makes them so important in intelligence is their systematic application and development. Appendix F presents more specific methods that are often useful to the analyst, summary presentations of this information in the present section, and a series of examples of the techniques discussed. The present section simply introduces the reader to the concept of analysis and outlines systematic approaches to the investigation of criminal activity for the intelligence analyst.

1. **What Is Analysis?** Analysis is that activity whereby meaning, actual or suggested, is derived through organizing and systematically examining diverse information. Although, as actually employed in police intelligence, analysis may not appear to be a distinct activity which may be unambiguously identified, there are certain characteristics common to all analysis. In keeping with our earlier assertion that the tools of the analyst are a set of procedures, analysis itself is defined in terms of a fundamental procedure which consists of three basic steps:

- Summarizing the relevant information.
- Comparing the summary with expectations derived from an initial hypothesis.
- Explaining the results of this comparison.¹

¹After Anderson and Zeldidch (1968: 284).

This definition of analysis relates to our conceptualization of the intelligence process as a whole, and to the relationships between analysis and other stages in the process. It can be seen that summarization follows directly from collection and collation, and that explanation implies the production of intelligence reports. Similarly, the general goal of analysis as stated above is completely compatible with the specific goals of an intelligence analyst. Given the validity of these definitions a remaining question relates to their usefulness in explaining how one does analysis.

In summarizing intelligence information the analyst is reducing both the *number* of individual pieces of information available and the *content* of each. The facts and speculations from all sources are reduced to those required. This activity is essential to prevent the analyst from being swamped by data that are only marginally relevant to a particular assignment. Summarization differs from collation in that the former is specific and focuses on a specific requirement. When summarizing relevant information the analyst should highlight the important facts and exclude or minimize those that are less important or reliable. The expertise of other analysts and field investigators should be sought in evaluating and summarizing intelligence reports. Although a great deal of tedious effort is required in this step, the process of summarization is most characteristically a preparatory function by which data are reduced to a form that lends itself to systematic examination and comparison of information.

The comparison of data is the critical step in analysis since, through this activity, meaning is derived. The data the analyst has organized and summarized are compared to a set of expectations derived from an initial hypothesis. In addition to imposing a general structure on the analysis, the hypothesis is the source of criteria that determines the significance of observed data. In other words, the analyst, by referring to a hypothesis, formulates a set of expectations and compares actual observations with those expectations. In this stage certain statistical techniques may be usefully employed since statistical analysis is largely concerned with comparing expectations and observed data. (The uses of statistics will be discussed at greater length in Appendix F.) Similarities or regularities in the geographical distribution of racket activities or in the activities of a particular suspect will be noticed by a systematic comparison of arrest records and field observation reports. In the comparison step, the analyst should also be aware of the differences among the data under examination. Very often a deviant case among, for example, a group of similar businesses provides a good indication concerning the nature and extent of organized criminal penetration.

In the comparison step the analyst asks what is significant. The question "What does this indicate?" is addressed in the final step of analysis, explanation. In actual practice, the analyst will have some tentative explanation in mind while actually comparing the data. (See the section on the role of the hypothesis below.) But it may be useful to treat explanation as a separate step. Explanation of the results of the comparison stage may be the final step before producing intelligence reports. The analyst may also find that he/she is unable to explain the results of the analysis, in which case more information is sought, or existing data is subjected to a more thorough examination. In any event, the analyst should determine:

- Whether the data exhibit significant relationships.
- The meaning of the relationships or lack of them in terms of the purpose of the analysis.
- The larger meaning of these findings in terms of the intelligence unit's overall knowledge of a particular organized crime activity.
- Requirements for additional information and/or further analysis.

2. **An Example of Analysis.** In this example the analyst is examining the extent of organized crime penetration in the local construction industry. The analyst is interested not only in determining the particular contracting firms controlled by criminal elements but also in following the pattern of action that precedes a typical take-over. Toward this end, the analyst will develop a hypothesis that reflects current knowledge about the operation of the construction business and the activities of organized crime. This hypothesis is as follows:

Take-overs of contracting firms by members of organized crime result from indebtedness to loan sharks that is paid off by forfeiting a controlling interest in the business.

At the outset of the analysis this hypothesis may be further supported by noting that the construction industry often operates on an unstable margin of available capital. Particularly during the spring and summer months, housing developers may find that they have exhausted available credit from legitimate sources and that a slump in housing sales necessitates additional borrowing. Reasoning such as this at the beginning of the analysis enhances the plausibility of the hypothesis and provides further direction in undertaking the analysis of this problem. This example is presented in summary form in Figure 1.

• **Summarize.** The analyst will have consulted the intelligence files for existing information on job activity in the construction industry and will also have checked

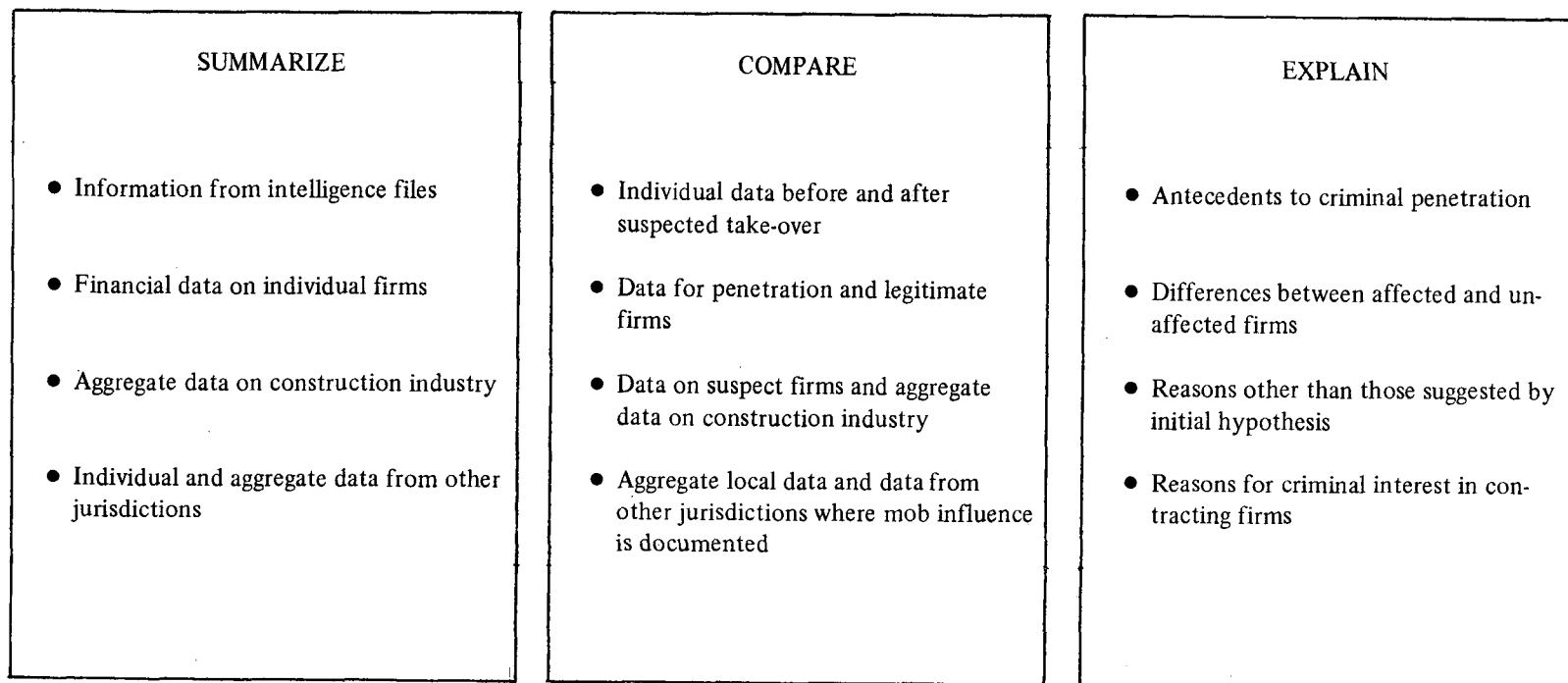
the biographic files of suspects. In addition, the working hypothesis indicates that financial data on local construction firms will be required. This may be obtained informally from cooperative companies and/or from informants. The analyst should also have contacted other jurisdictions for information concerning organized crime influence in the construction industry. Aggregate data on the industry locally, regionally, and nationwide should also have been obtained. The summarization step requires that all of this information be examined and reduced to that which is needed in evaluating the stated hypothesis. Furthermore, these data should be consistently formatted to facilitate comparison. This does not mean that information for each individual, business, or location must be complete and identically categorized in all respects. The individual pieces of information must simply be reduced to a form by which they may be systematically examined and compared.

• **Compare.** The financial data for individual firms apparently in similar circumstances should, if the hypothesis is correct, reveal significant differences between firms that have been able to gain some financial support and those that have not. The analyst then must sort out those companies with legitimate support from those in the hands of shylockers. He/she may be aided at this point by differences in the patterns of financial activity before and after a mob take-over. Aggregate data on construction firms in other areas where criminal penetration is not a problem are compared with the local industries. Case histories that document take-overs in other jurisdictions may be compared to local firms. Financial anomalies between suspect and legitimate companies will indicate the methods employed in penetration.

• **Explain.** The results of such comparisons are utilized to evaluate the original hypothesis. Evidence that indicates firms suspected of being recently taken over by organized crime had experienced financial difficulties would tend to support the hypothesis. Contrary evidence would indicate that the hypothesis is in error. In either case, explanations of criminal activity in the construction business should be in terms of the operating hypothesis. If the original hypothesis is supported, the results of the comparison step can elaborate upon that explanation. Where the initial hypothesis is rejected, the explanation step can direct the analyst toward formulating a new hypothesis.

It should be obvious that in actual practice analysis is not such an orderly activity proceeding from step to step. Indeed, as has been noted before, it is sometimes difficult to distinguish analysis itself from other stages of the intelligence process. However, all successful analysis should employ the steps discussed above. As in virtually

FIGURE 1
ANALYSIS PROCEDURE



all phases of intelligence activity, the key to sound, productive analysis lies in systematic traceable procedures that allow the analyst to document conclusions. This is important not only in providing evidence for "successful" analysis, but also for pointing out unproductive areas of inquiry so that they may be avoided or approached differently in the future.

3. Pursuing Civil Violations. The historical difficulties in assembling sufficient evidence to prosecute organized crime figures are among the reasons for developing a police intelligence capability. The controlling figures behind organized criminal operations are often far removed from direct contact with illegal activities and are therefore not easily subject to prosecution for criminal offenses. Also, the requirement for a legitimizing occupation and other factors have increased the movement of organized crime into seemingly legitimate business activities. For a number of reasons trends of this sort have impeded criminal prosecution of organized crime. The analyst should therefore be prepared to develop new and perhaps unusual methods for exploring organized crime activities.

Among the most successful approaches has been the pursuit of civil violations which are often consequences of organized crime penetration into legitimate business areas. The illegal means by which criminal elements gain control of business are often not traceable, but gaps in required documentation of operations and corporate accounting procedures may provide evidence for filing civil charges. Similarly, specialized regulatory agencies at the state or local level may be employed in non-criminal enforcement efforts. The successful use of such prosecution and enforcement techniques obviously requires that the intelligence analyst have some rudimentary knowledge of highly specialized legal, financial, and accounting skills. No effort will be made here to provide detailed guidance on the pursuit of civil violations. Our purpose is merely to point out some of the types of civil crimes with which organized criminals may be charged. To attain this goal, the analyst must focus on gathering specific types of information and utilizing specialized resources either by developing personal skills or consultants.

Perhaps the most familiar non-criminal violation for which organized crime figures have been successfully prosecuted is Federal income tax evasion. But many states have statutes that can be used against those failing to pay state income taxes. In developing such a case, relatively detailed information will be required concerning the financial dealings of the suspects. The focus of an investigation of this sort requires some knowledge of accounting procedures in gathering and analyzing the required data. An analyst with such training can be

teamed with investigators to develop a case. If the case cannot be prosecuted under state laws, it can be turned over to the Internal Revenue Service whose considerable resources may be utilized in further investigations.

Another potentially fruitful area of investigation relates to the activities of various state and local regulatory agencies. For example, the analyst may be able to acquire information which may be used by food and agriculture inspectors against mob-controlled meat supply firms. Similar approaches include investigations for violation of laws regulating activities in establishments holding liquor licenses, labor or union violations, unfair trade practices, local antitrust violations, and violations of equal employment opportunity regulations. Businesses under criminal control may also be investigated for violations of corporate statutes and accounting requirements. An indirect but effective approach to attacking organized crime focuses on pursuing politicians in the pay of criminals. Since much criminal activity depends on protection through political influence, the prosecution of these protectors increases the effectiveness of other enforcement efforts. The goal of tactics such as these is to forcibly curtail or close down the business activities and "covers" of organized crime. Deprived of a legitimate front and political protection, illegal activities and rackets are more vulnerable to criminal prosecution.

This discussion is not meant to ascribe to the analyst a responsibility for investigation and field work but rather to dispel popular conceptions of organized crime as exclusively Mafia-type activity. Since organized crime takes many forms, intelligence analysts must be prepared to direct their efforts toward whatever means are available for curtailing criminal activity. These duties involve determining the vulnerabilities of the organized criminal element, suggesting information to be collected, and performing analyses to determine how those vulnerabilities may be exploited.

4. Using Intelligence Files. Intelligence files are the analyst's most important single resource. It is through the systematic collation and comparison of raw data that finished intelligence is produced. In fact, "intelligence" often refers more to the ways in which information is organized and used than to the contents of that information. For these reasons proper use of the files by analysts assumes particular importance. The analyst's role in providing inputs to the files was discussed earlier in this chapter, and the preceding chapter dealt with the maintenance of the filing system as a whole. Maximum ability to cross reference among functional and subject files was described as the most important criterion for useful intelligence files. In actually doing intelligence analysis these cross references are used to establish

relationships among criminals, businesses, locations, and rackets. The analyst continually refers to those functional files in evaluating patterns of recurring actions or in trying to trace the origins and purpose of unique activities reported in new information.

The files of an intelligence unit are considered the analyst's primary source of information since they are the source first consulted. When beginning a new project or when responding to requests for a specific assessment, the analyst should examine the files for information on the subject before collecting new data. A search through the respective indexes and data files may provide enough information on a suspect person or business or on a particular racket to fulfill a tactical requirement. At a minimum, a thorough examination of data currently at hand will help direct further collection efforts. Another principal use of the central files is in following up new information presented in field reports or derived from other sources. Upon receipt of new information the analyst will often consult the functional files to help place the new information in context. Through such follow-up activities the analyst may recognize patterns of activity for a particular suspect whose movements and activities have been traced, or connect a previously unfamiliar criminal or racket with known activities documented in the files. In other words, a routine file search enables the analyst to *recognize* trends of activity, and to relate new information to trends which have been previously identified.

Much of intelligence analysis, as discussed earlier, is concerned with establishing the relationships among seemingly diverse pieces of information in general, and among seemingly diverse individuals and activities in particular. Efficient intelligence files are structured, not only to accommodate such relationships, but also to simulate them by cross referencing people, places, and actions. In this sense such files are more than tools that are helpful in doing analysis. They represent two of the three steps in analysis described earlier: They contain summarized information which is compared by cross references and functional indexes.

5. Use of the Hypothesis. Throughout this chapter we have often referred to the hypothesis and its importance in intelligence analysis. As employed in scientific research, an hypothesis may be defined as a conjectural statement about the relationships that exist among two or more variables.² The manner in which hypotheses are used in police intelligence is certainly consistent with this definition, but more generally it may be stated that hypotheses are working assumptions that are tentatively accepted as true and utilized to focus

further investigation and analytic efforts. The primary purpose of the hypothesis as used in intelligence analysis is to structure the analyst's inquiry by explicitly stating the problem under investigation and by limiting the possible solutions to those that are most plausible. In other words, the analyst uses all available evidence to derive the most plausible explanation for the criminal activity under investigation. This explanation becomes the hypothesis which the analyst then tests in order to verify, reject, or modify the explanation.

The hypothesis may be a formal written statement that includes all available supportive and disconfirming evidence, or an informal and unstructured idea or explanation that occurs to the analyst as he/she is evaluating some new piece of information. In actual practice, operating hypotheses will fall somewhere between these two extremes. Furthermore, since the main purpose of the hypothesis is to focus the efforts of the intelligence analyst, the form and specific use of hypotheses will vary across units and, to a lesser degree, across analysts within units.

Most generally, the hypothesis is a tool the analyst uses to develop a tentative explanation for some criminal activity. It is based on an examination of existing information relating to that activity. As such, it is obvious that the degree of specificity and certainty with which hypotheses are formulated will vary with the amount of information available. In cases where existing information is limited, hypotheses will be more general or directed more at specifying further information requirements than at offering a detailed explanation of criminal activities.

The analyst may also find it useful to formulate alternative hypotheses where there is limited information available. This approach, often used in the early stages of determining the meaning of a new collection of information, keeps the analyst from focusing too soon on a single hypothesis (which may be wrong). As new information is gained it can be tested for fit against the several hypotheses. Normally, in time, a perceived pattern in the information will permit the analyst to focus on how the criminal activity operates and who may be involved. It must be remembered that the business of intelligence is to probe allegations and suggestions of criminal activity rather than to build an evidential case. If the intelligence analyst's hypothesis is accepted, it becomes the starting point for case building.

Herein lies the principal utility of the hypothesis: It enables the analyst to work back and forth from abstract hypothetical explanations to actual data resulting from field investigations. The example of analysis presented earlier demonstrated this use of the hypothesis and a schematic presentation of this process is given in Figure 2.

² Roscoe (1969: 112).

The initial hypothesis is used as a guide in organizing and summarizing information, and in directing the preliminary comparisons of data. Explanation of the empirical results of this analysis is undertaken with reference to the expected results implied by the hypothesis. In the example, the initial hypothesis suggested that organized crime take-overs of contracting firms result from defaults on usurious loans. The empirical data that would support this hypothesis would be evidence of financial anomalies among suspect firms. If financial difficulties are not evident, the initial hypothesis also helps the analyst keep track of dead ends in the search for patterns in organized crime activity, and thus insures that unproductive areas of inquiry are avoided.

Earlier in this chapter analysis was defined as that activity by which meaning is derived from the systematic examination and organization of diverse information. Given the massive amount of information, the structure imposed by the hypothesis on the activities of analysis and collection is invaluable.

D. Preparing Intelligence Reports

The final products of intelligence analysis are presented in the formal intelligence reports. It was noted earlier in this chapter that the purpose of the intelligence report is to inform the reader of the findings of an analytic process while providing sufficient documentation of the process which led to those findings. Although the actual content and format vary with the type of report, this general purpose is common to virtually all intelligence reports. What follows is a general discussion of the different types of intelligence reports and the characteristics and contents of each.

1. **Oral Tactical Response.** The simplest and perhaps most common type of intelligence report is the oral report. This is most often in response to a specific request by investigators or other units in the department. In producing such a report the analyst is usually providing information on a particular person, his/her recently reported activities, and associates. The content and format of the oral response will vary greatly, conforming to the requirements of the user or to the nature of the requested information. Oral response should be recorded so that the analyst and his/her supervisors are aware of the current requirements for this type of intelligence report and a record is maintained of all information disseminated from the intelligence unit. The report should be indexed and filed for future use.

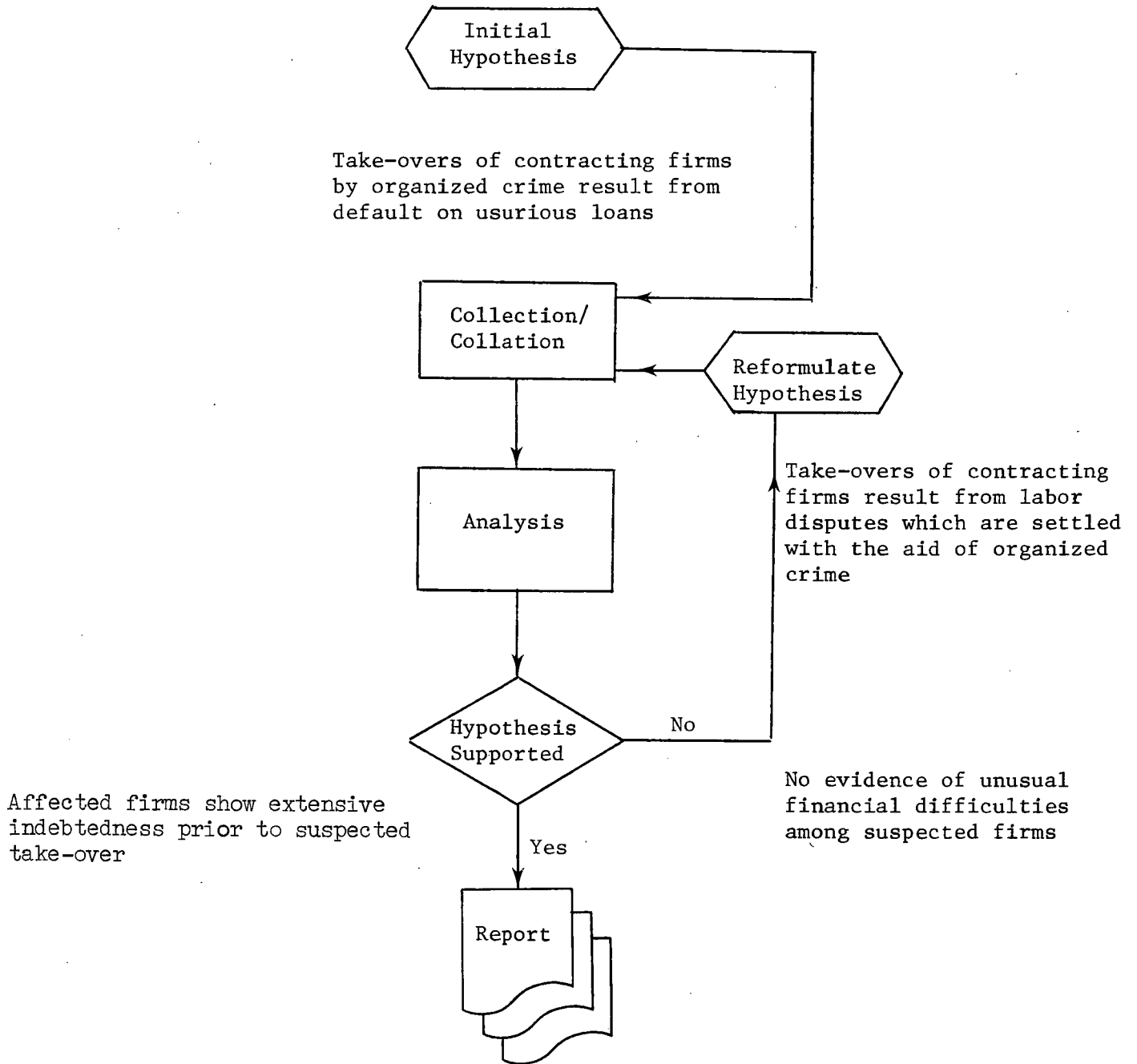
2. **Written Tactical Response.** Reports of this type will most often be in response to a request for an assessment or estimate about a particular criminal

racket, suspect, or business. Even though the person requesting the report will probably know why it has been written, the purpose of the report should be explicitly stated. Next should come the conclusion and, if appropriate, recommended actions to be taken. If the report is lengthy, which is not often the case in tactical intelligence, a summary of the contents should be included that incorporates both the conclusion and recommendations. Generally, however, tactical reports will be brief and focus on a specific enforcement problem. They will therefore not require lengthy discussions of supplementary information.

3. **Strategic Reports.** Strategic intelligence may be generally characterized as an estimate of the extent and nature of a criminal activity, usually geographically or functionally based. It will include an assessment of the current situation and an estimate of future trends and developments. It is more discursive than those mentioned above, but the same general requirements for succinct presentation still exist. The purpose of the report should be initially stated followed by conclusions, recommendations, and a summary. The latter should contain a concise statement of the operating hypotheses and assumptions utilized in the analysis. The strategic report deals more with future activity and involves a greater degree of uncertainty with respect to its findings. A more thorough discussion of the analytic procedure is therefore important to enable the intelligence consumer to evaluate the evidence and assumptions upon which the conclusions are based. The analyst should also explicitly identify what he/she perceives are the major shortcomings and uncertainties of the report. Similarly, requirements for the additional information required to elucidate further the subject of the report should be clearly stated.

4. **Periodic Reports.** The intelligence unit may be called upon to issue a weekly or monthly report on criminal activity in general, or relating to a specific racket or group of criminals. Reports such as these usually focus on a chronic problem area within the jurisdiction. The specific contents of periodic reports will of course vary from unit to unit, but the same general characteristics common to all such reports can be identified. Where the primary concern is with updating knowledge in a particular area, the periodic report should explicitly relate new information to that which was available before. If new trends or a change in previous trends is noted, the relationship of the new activity to that previously identified should be stated. Revised estimates and hypotheses should always be presented in juxtaposition to those they supercede. Since periodic reports often serve as a running record of intelligence unit activity, they should display some

**FIGURE 2
USING THE HYPOTHESIS**



degree of consistency with respect to subject matter, general methodology, and style of presentation.

The differences among these and other types of intelligence reports are less important than the elements that should be common to all, namely, clarity, parsimony, and a central focus that reflects the purpose of the report. Excessive emphasis on the details of the underlying research and

analysis is not desirable, but neither are assertions whose origins and significance are not traceable. The intelligence report represents all of the prior steps in the intelligence process that went into its preparation. The performance of the intelligence unit as a whole, and the effectiveness of the unit in combating organized crime, may therefore be evaluated with reference to the intelligence report.

CHAPTER V

STAFFING AND TRAINING THE INTELLIGENCE UNIT

A. Introduction

Any supervisor setting out to fill a critical and sensitive position in the organization asks two basic questions: "Is the person I am considering for the position capable of doing the job?" and, "Can other officers work effectively with this person?" 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/she clean?" And then, from the point of view of intelligence: "Can this person think analytically; can this person assemble and structure pieces of information to answer the question, why?"

In looking at the staffing of an intelligence unit, the most important selection 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. Another critical category is that of the analyst. This chapter will emphasize the analyst since this is a relatively unique category in law enforcement.

The investigator category poses yet another selection problem. The investigator will usually be a transfer from an enforcement unit and will have experience in investigation. But the investigator will be faced with unique, challenging requirements. In addition to being able to conduct an investigation, he/she 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.

B. Staffing the Intelligence Unit

1. **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 weights the questions differently. The right person for the post of organized crime intelligence unit commander cannot, of course, be found by any process. All kinds of limits, which are familiar to any bureaucracy, are built into the selection process. The selector may have imperfect choices. In mentally juggling the attractions of a smaller list of availables than he/she would have wished, the selector may have to lower standards on some qualifications like

cooperativeness while maintaining them on brainpower. Or he/she may be thoroughly confident of Y's integrity but suspects that Y's taciturnity hides smugness.

However, if there are any misgivings about the integrity of X and Y, the selector should not entertain their candidacies. The intelligence unit commander must be—if nothing else—vigilant about the possibility that organized crime will be seeking to corrupt the law enforcement officers of the agency. There is no room for compromise on this point. Any weakness in the element of the agency most concerned with the penetrative stratagems of organized crime, and any softness in the element of the agency charged with collecting and maintaining the most delicate intelligence materials, would be perilous to the agency as a whole.

2. **General Criteria for Staff Selection.** Much of the same general criteria that apply to selection of an intelligence unit commander will apply in recruiting the balance of the unit's staff (see Figure 1). This is not to say that the commander should seek to fill the office exclusively with subordinates who think as he/she does. He/she will, on the contrary, need 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 subordinates, a unit commander will benefit more from personnel who will not hesitate to suggest an unorthodox approach and challenge traditional assumptions than from a collection of agreeable, think-alike types.

A search for bright, tough-minded personnel can present difficulties. The unit commander should avoid certain personality types who, though they may at first be impressive, will not have the flexibility for sound intelligence work. The officer with his/her mind made up on most issues—no matter how polished that mind may be—will have difficulty dealing with the unexpected. If, for example, the investigation has led to the conclusion that a certain target is surely the wanted culprit in a complex case, the officer may overlook evidence that suggests the contrary, having more confidence in his/her 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 department as a whole. It may

FIGURE 1

CRITERIA FOR SELECTION OF INTELLIGENCE UNIT STAFF

<u>ESSENTIAL</u>	<u>HIGHLY DESIRABLE</u>	<u>DESIRABLE</u>
1. Integrity <ul style="list-style-type: none">- Honesty- Personal candor- Realistic about self	1. Flexibility <ul style="list-style-type: none">- Non-dogmatic- Broad range of interest- Open-minded	1. Perseverance <ul style="list-style-type: none">- Not easily discouraged or frustrated
2. High Intellectual Capacity <ul style="list-style-type: none">- Alertness- Inquisitive mind- Imaginative	2. Special Motivation <ul style="list-style-type: none">- Draws satisfaction from problem solving- Particular desire to be Intelligence Officer	2. Planning Skill <ul style="list-style-type: none">- Good manager of time
3. Analytical Aptitude <ul style="list-style-type: none">- Thinks logically- Capacity to synthesize- Capacity to hypothesize	3. Articulate <ul style="list-style-type: none">- Writes well and concisely- Speaks well and concisely	3. Self Discipline <ul style="list-style-type: none">- The "self-starter personality"
4. Meticulousness <ul style="list-style-type: none">- Thorough- Pays attention to detail- Precise in handling data	4. Resourcefulness <ul style="list-style-type: none">- The "digger" type- "Where there's a will there's a way"	4. Cooperativeness <ul style="list-style-type: none">- Capacity to work well with others
		5. Fast Learner <ul style="list-style-type: none">- 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 group 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.

occasionally be possible to harness such a person to a specific and narrow specialty where such zeal can be an asset; but this is seldom the case.

One approach to intelligence personnel recruitment is to begin by setting low age limits and then identifying the candidates with a genuine desire for education and self-improvement. Intelligence is a mind-stretching business—its targets change, its methodologies are constantly improving and require more and more innovative ideas to cope with the growing sophistication of organized crime. These are aspects of intelligence work that can attract the bright candidate and also simple conversational topics that can gauge the candidate's responsiveness to challenges.

a. **The Interview:**¹ It is usually beneficial to include a great amount of personal interviewing in the staff selection process. Beyond building the supervisor's confidence in a choice, the interview technique allows the quality of a person's mind and 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 prepared for by both parties. A useful requirement is that the candidate submit a brief autobiography in advance (usually no more than two pages) that contains at least one statement about career expectations in the agency. The requirement has several advantages:

- It discourages frivolous applications;
- It may surface dimensions of the applicant not revealed in the personnel file;
- It may give an early indication of writing ability;
- It impresses on the candidate the special nature of an assignment to intelligence.

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

Obviously, a good interview will concentrate on motivations. This is especially important for intelligence

work where the rewards are more often the satisfaction of unravelling a problem than money or direct participation in pursuing a 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 flounder, and cases may be rejected by the prosecutor. A law enforcement officer who has previously had investigative experience should be asked to submit copies of old written field reports. In a subsequent or follow-up interview, these can be used as the basis for a discussion of personal work habits, collection techniques, thoroughness in following up leads, and so forth. 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 is being considered.

b. **The Selection Process.** If two or more applicants could be measured against one another, it would be relatively simple to decide who should fill the vacancy. But this cannot always be done. 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 their own sense of standards and stick to them. The momentary need to add to an overtaxed staff should not be used as an excuse to lower the entry requirements 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 the slot remained unfilled until a qualified applicant was hired.

A problem of a different nature arises when an intelligence unit has a number of qualified applicants for one or two places. On the surface this is an enviable situation. The commander can hardly go wrong; but will he/she pick the *best* applicants by exercising careful self-examination of the selection technique?

The natural human tendency in these circumstances is to find reasons for *eliminating* rather than for *selecting* one or more applicants. This is a far more subtle, and often subconscious, process than that practiced 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 do not. The latter are eliminated with relative ease according to fairly uniform standards. If the qualities of an applicant remain in doubt after the initial cut, he or she can be asked to participate in the more intensive interviews and field or analytic exercises. Assuming, however, that all of these barriers have been successfully overcome, the selector is not on the spot.

¹One hurdle is not discussed in this chapter—the full-field background investigation of applicants. This is covered in Appendix E on security.

Until this point the selector has thought positively about the candidates who were successfully moving along the selection process. If he/she has been personally involved in the various stages of interviews and testings, the selector may even have envisaged how each of the candidates would fit in the system. "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..." But faced with choosing among several demonstrably capable applicants, the selector often begins to search 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.

The insidious effect of such a technique, of course, is that by emphasizing the search for weakness in the candidates, slight deficiencies become exaggerated in the mind of the selector: Two spelling mistakes by X very quickly turn into skepticism of X's ability to handle the English language. The on-duty analyst noted that applicant Y was "very curious" about the promotion possibilities in the unit, and hence may be dangerously ambitious. At the worst, this kind of thinking can lead to 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 a disservice by straining for reasons to eliminate qualified candidates rather than pinpointing the best of the good.

Selecting the best from 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 do competitors. If this is not the case, however, the determination becomes a little more complicated. 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/she do with spare time? How self-confident? Without resorting to self-deprecation, how honest is the person about himself/herself? Can he/she synthesize many and varied inputs? Can he/she take fragments of a conversation or the various elements of a biographic file and make generalized conclusions rapidly but undogmatically?

There are, quite naturally, many other qualities or characteristics 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 important attributes for the good intelligence officer: a broad range of interests because this may signify a flexible, inquisitive mind with a wider than average social interest; candor about himself/herself 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 trivial surrounding it.

c. **The Special Problem of Choosing the Intelligence Investigator.** Under normal circumstances, the intelligence investigator will be transferred into the unit from another investigative unit. He/she will have gained experience in the more traditional modes of investigative work and will be part of the normal career structure, looking forward to further promotion which may have to be out of the intelligence unit. The area of conflict is that the intelligence unit commander may have to fight hard for freedom to select from among the best investigators in the agency. Where none can be found that fit his/her needs, the commander 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 demands 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 major operating areas for the organized criminal.

But the "trained" investigator also presents a problem in the selection process. The best choice is an investigator who has done well at routine work but responds positively when the more complex investigatory work involved in fighting organized crime is discussed. The investigator must be a person who can both take direction and have sufficient initiative to develop new approaches to a problem. The trained investigator who seeks only the rapid arrest should be avoided. Such a person will not be able to survive a complex investigation that takes months and where the ultimate arrest is the responsibility of another unit.

The intelligence investigator must be able to work with the analyst. The investigator must be willing to take leads from the man or woman sitting in the office, to participate in the analysis itself, and to help guide the analyst in turn. In addition to factually correct reporting, the analyst must be able to develop a capacity for "first-cut" analysis, the development of an interpretation of the meaning of his/her findings. In fact, the analyst should relish this aspect of investigatory work.

3. **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 positions. The use of accountants and attorneys to collect 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, and psychologists, is unusual. 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 some generalizations may be made that 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.

a. **The Non-Specialist Analyst.** Many intelligence units in the country find 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, police work, the law, or even the methodology of data analysis; but if they are intelligent, precise, and anxious to explore new areas, 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, non-specialist analysts can be invaluable in designing filing and cross-referencing systems best attuned to the analytic process. The analysis they do will essentially 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 official institutions and libraries. In short, they will be applying logic deductive techniques effective in any context to the task of unravelling and (ultimately) exposing covert criminal activity.

b. **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 utilized. Naturally, an intelligence unit commander must determine the most efficient way to accomplish such analysis. If he/she is confident that the target group represents the only

sophisticated threat in the jurisdiction and that, if "rolled up," no other group is likely to come along and enter the vacuum, the commander may decide that it is best to use personnel from some other law enforcement agency in the locality. If there are no such specialists available, he/she may rely on specialists on a consultant basis. If a continuing problem is likely, then the unit commander must enlarge the staff to cope with this complex dimension of criminal behavior.

As noted previously, there are no hard and fast rules for deploying or employing specialists in an intelligence unit. But one managerial principle should remain uppermost in the commander's mind. A comprehensive plan must be drawn up as to how to use the specialists after the most tempting and immediate targets are dispatched. If there is no permanent, continuing use for specialists, they should not be hired in the first place. They are probably too expensive to employ as non-specialist analysts and even if so used, would probably grow restless and move on.

The imaginative intelligence unit commander with non-recurring requirements for in-depth studies or the occasional analysis of highly complex problems can sometimes use other community resources. Most major municipalities have more than one law enforcement agency. Hence two or more agencies working together in full faith and confidence could share the costs of one highly specialized analyst between them. Or an accountant 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 maintaining an analyst experienced in intelligence work.

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 often time-consuming for the agency that wishes to let a contract. Much depends, of course, on the rigidity of local laws governing such contracts, hiring, temporary employees, and "best source" agreements. Generally speaking, this kind of arrangement is most satisfactory when there is a specific task at hand that either requires special skills unavailable within the agency, or that, if tackled by the incumbent staff, 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 to determine 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 that

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, a study of the effectiveness of different loan shark statutes in other jurisdictions might have more long-range impacts 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.

c. **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 who is willing to spend some time exploring such schools, particularly those with modern departments of criminology, management, public administration, systems sciences, sociology, and so forth. Concerned scholars working in fields that at first seem to have little connection with law enforcement intelligence can be identified. They may be permanent faculty members or graduate students preparing advanced degree dissertations.

Approaching the campus is a delicate matter if the intelligence commander does not already have established contacts or friends. It is best not to 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 targeted on organized crime. This may arouse suspicions as to the commander's real motivations and create an atmosphere of hostility that, even though unjustified, deters scholars who would otherwise be interested in the needs of the unit. One ideal way to begin a dialogue 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 that person directly about his/her research. There are countless ways to engineer a discrete encounter with members of the academic community, but it is essential to use tactics that are above suspicion. The purpose of the visit must always be explicit and unquestionable: a search for intellectual assistance for a law enforcement problem of gravity and delicacy. Only a few scholars would rebuff such an approach.

Having identified a talented scholar (or scholars) on a local campus, the unit commander may use a graduate student or two on specific projects that threaten to consume too much of the time of the permanent staff. Some match between the graduate student's principal field of interest (or a subject related to a dissertation topic) would be ideal, but such a convenient arrangement is rare. Nevertheless, if the student or students in

question find the part-time work experience for the unit rewarding, a more permanent relationship may be formed. 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 course requirements by working 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 consideration of the implications involved by the unit commander. As a primary obligation, the integrity and security of the unit should be protected. However, if clearance procedures are demanded that are as strenuous as those required for permanent personnel, the commander may discourage good, young scholars from the law enforcement profession and may, in the process, lose a promising candidate as an experienced specialist in the intelligence unit. Clearly, a rule of reason must be applied.

First, the unit commander will be better able to harmonize these two quite different concerns if there are "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. Or such persons could be given an assignment almost wholly devoted to public sources, such as library reference materials, newspaper files, and so forth. Where such limited studies cannot be isolated from the normal working routine of the unit, the commander must, to protect the 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 are reciprocal, become involved in training 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.

d. The Problem of the "Non-Badged" Employee.

In some law enforcement agencies, where there is a long-standing bias against employing non-sworn personnel in other than administrative 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, but also from higher command echelons. 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 between sworn officers and civil service analysts, it is worth trying if for no other reason than few law enforcement agencies have 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, they 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 can be accomplished if well-disciplined minds stay at the task and are spared the normal interruptions of traditional enforcement duties.

Encouragement and rhetoric alone will not successfully unite the sworn officer and the civilian analyst. The supervisor must assist in the process and will be responsible for combining teams of analysts and investigators as suggested in Chapter VI. This will be a direct confrontation technique that can succeed only if the analysts rapidly prove their mettle.

But, in the longer run, the supervisor 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 educational advantages, then he/she must seek by every means possible to upgrade the educational requirements and levels of sworn personnel. If agreement is received for raising entrance requirements for sworn officers to the college degree level, the supervisor will continue to encounter resentment from sworn officers who did not enter the service with a degree. Hence, the supervisor must work to make it possible for those officers to be given educational opportunities. There are Federal

monies available for systematic upgrading of such personnel. If this phase of the personnel program is neglected, resentment of sworn personnel may be transferred from the civilian analysts to the incoming, highly credentialed rookie patrolpersons.

Finally, the supervisor must deal directly and aggressively with any present or prospective imbalance between compensation levels of sworn officers and civil service analysts, advocating 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 easy. But whether ultimately the supervisor succeeds or not in bringing about some measure of equity is less important than the fact that he/she demonstrated an attempt to succeed.

4. The Special Nature of Staffing the Intelligence Unit. It should be clear that the intelligence unit commander is more responsible than any other for the successful amalgamation of the work of different types of subordinates. Help may or may not be received from the personnel bureau on this potentially thorny problem but, in any case, the commander must be familiar with the regulations of the local civil service commission if the unit 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 seemingly intractable problems may not be as worrisome as they would appear at first glance, as long as everyone understands the differences in detail and does not 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 the freedom to fire unsatisfactory civilian members of the team. In some localities, civil service regulations operate to provide virtually perpetual job protection; it is in these jurisdictions where the most elaborate selection procedures will be necessary. The commander will rarely have the luxury of transferring an analyst "who has simply not worked out well" to another element of the agency. There may be no civilian openings or slots in other parts of the agency. He/she must either make a special training effort to increase the specialized skills of sworn personnel or become a proponent of autonomous status for the department.

a. Career Considerations for Intelligence Personnel.

The intelligence unit commander soon recognizes that the personnel management problems encountered are likely to be quite different from those of other elements in the department. 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 that subordinates will have to face springing from the nature of the work itself and the premium placed on continuity in the intelligence profession.

First of all, unlike most law enforcement personnel, intelligence professionals rarely enjoy concrete triumphs in conducting 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 person on patrol may, by quick thinking and an even-handed approach to a street brawl, be satisfied that he/she has headed off a dangerous confrontation; he/she may be told as much by the precinct captain. Not so for the intelligence professional. A district attorney may savor his/her name in newspaper headlines the day after the major criminal figure has been prosecuted and 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 unravelling of an organized criminal network of the indictment of a gang leader is seldom evident. Intelligence activity is rarely personally satisfying and rewarding to the professional. Indeed, small pieces of information are pieced together to make a larger picture. Other officers and other law enforcement agencies may contribute other portions of the picture until there is enough for a warrant, an arrest, or an indictment. The arrests and indictments are almost always made by somebody else, usually at a time and place unknown to the intelligence professional. Hence, intelligence is often an anonymous 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 glamour potential compared to the highly expert and highly publicized detective work that leads to the apprehension of a 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 subordinates. One practical and obvious approach is for the commander to keep informed about the uses of the intelligence produced by subordinates. This may mean no more than reporting

back to the analyst that the study produced was read by the chief. Or it may be that in talking with a junior attorney in the prosecutor's office the commander learned that a decision had been made to build a case against crime figure X or criminal activity Y, based on the investigator's efforts. The commander cannot assume that subordinates will know these things simply because he/she does. Hence, the connection between a piece of analysis, an investigation of some months past, or a study and the consequential event that took place outside the intelligence unit must be articulated. The commander must go further, making sure that superiors and fellow officers elsewhere in the agency understood this connection and that they appreciate the process involved.

Finally, the unit commander may discover that the experienced personnel under his/her 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, and planning, and (2) intelligence work is so specialized that few officers do it well, and those who do had best be kept where they are. For the civilian analyst, of course, movement from one division to another in a large agency may be an impossibility. Some commanders, when they recognize these seemingly intractable facts of bureaucratic life, accept them philosophically and rationalize, "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/she should, despite the cost to the unit, encourage the best officers to seek recognition, pressing hard for an occasional assignment *out of intelligence* for the best people. If officers are occasionally promoted, they will become missionaries for good intelligence support wherever they go. Although the skills are missed, the gain may be important. But the commander also has an obligation to those who remain, probably longer than comparably bright officers in corresponding divisions elsewhere in the agency.

There are two basic things the unit commander can and must do for such subordinates. First, he/she must fight hard for high ranks or positions in the shop. Here the case must rest on the wits of the men and women involved rather than on arrest statistics or even the numbers of organized crime leaders apprehended in the jurisdiction, since months may go by without a score.

The officer 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. Of course, to use this argument with an effective impact on supervisors, the unit commander must be confident that selection policies have indeed produced an exceptional team.

Second, the commander must ensure that within the intelligence unit the career of an officer or a civilian analyst is as varied as possible. This helps keep them active and interested. 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. Depending on the size of the unit, the opportunities for flexible deployment of intelligence personnel are there. It is up to the commander to exploit those opportunities.

C. Training

General reorientation of a law enforcement agency to an appreciation of intelligence requires a three-pronged training effort that is directed toward:

- the non-intelligence units;
- the personnel assigned to intelligence responsibilities; and
- the command level.

The largest category of training, including recruit, patrol, and investigative 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 as investigators or analysts, very practical instruction is necessary—how to collect, evaluate, collate, and analyze. But for the command level, the main objective should be to demonstrate 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 decision-makers.

But each category presents a different problem in developing program and course presentations. The first two may be dealt with fairly directly; that is, training programs for them—although perhaps quite different in content from what has traditionally been offered on the subject—can be fit into existing curricula 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 from 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 intelligence operations against organized crime are to have a meaningful impact—if they are to support strategic thinking as well as operations—then the role of intelligence must be clearly understood 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 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.

1. **Training for the Non-Intelligence Officer.** The objective of any course (or portion of a course) designed for the patrol force or other non-intelligence assigned officers should be to prepare them to understand and contribute to the intelligence process.

Most police academies now spend 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 concentrate on field report writing as an input to the intelligence process. It is little wonder that many 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 strange officers and civilians mysteriously pushing paper instead of making arrests.

a. **Intelligence Is Not a Mystery!** Clearly, then, any general training program for law enforcement officers must have, as one of its first goals, the elimination 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. This person should emphasize that the methods of collection, investigation, analysis, and so forth, employed in the unit are not at all the mysterious rituals some have imagined them to be. In fact, he/she should, where possible, offer the class a case study of how intelligence has contributed to the unravelling of an important criminal conspiracy. This kind of presentation should emphasize the laborious aspects of "making matches" between what had been considered unconnected people, places, or businesses. 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 is possible here, but arousing the awareness of the average law enforcement officer should be the main emphasis. He/she should be encouraged to think of the precinct or beat as a source of reportable information.

b. **Field Reporting.** 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 officers. No amount of exhortation will drag it from them unless they personally are interested in what they see about them and feel it may have value to others. It is for this reason that an effort must be made to induce police officers to think like observers. This approach may spark their imagination; simply appealing to them to record the unusual that they see on their beats will not.

c. **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/she 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 observations. The officer should know, for example, that certain businesses and service industries are particularly susceptible to organized crime penetration; he/she should know what activities of organized crime have recently been recorded in other cities.¹ The officer should understand that he/she has an obligation to become familiar with the known criminal

¹The pamphlet, "Police Guide on Organized Crime," published by the U.S. Department of Justice, contains a list of 20 indicators that suggest the presence of organized crime.

figures in the precinct and to learn as much about them as the precinct commander can relate. If the officer becomes an active reporter, he/she should know where and how ready access to the intelligence unit can be had.

2. **Training Intelligence Officers.** For those personnel designated as organized crime specialists in such fields as narcotics and vice, quite specific training is needed. 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, 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 interrelated 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 from job experience.

Manual skills requiring practice to develop dexterity can be learned fairly rapidly and, once learned, remain relatively constant at a level determined by physical factors and the quality of the training involved. Thinking habits or mental processes develop more slowly. Or, more accurately, introducing 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 may be perfectly well understood when the point is made in a 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/her thinking habits and develop mental disciplines to which he/she has not been accustomed. Thus, the first guideline for the intelligence officers' course should be to recognize the disparity in learning speeds. Much more course time should be spent on developing 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 techniques, and the like. This is not to say that one is more important than the other—only that the former takes longer to be assimilated—even for the quickest mind.

a. **Intelligence Theory and Organized Crime.** An introduction to the intelligence officers' course should begin with a few hours—probably no more than 5 or 6—devoted to a discussion of intelligence theory as it relates to organized crime. These will not be easy concepts to convey. 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 (or warning or danger signals) of intelligence and strategic (report on existing or potential patterns of activities) 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 undertake 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?"

The reason for enunciating this point must be clear to the instructor. He/she should be concerned in the training course that the intelligence unit be understood as filling a special and even unique place in the law enforcement agency. 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. If 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. In short, its effectiveness will be destroyed.

b. **Crime That is Continuing and Organized.** The next portion of the intelligence officers' training should be a fairly generous one devoted to the target itself—the types of crime in the jurisdiction against which intelligence will make the most effective contribution. It should concentrate on developing areas of criminal

activity, white-collar crime and public corruption as well as more traditional criminal areas.

A fundamental objective should be to stretch the student's thinking beyond the traditional ethnic image of organized crime. In many jurisdictions, and even at high levels in these jurisdictions, the comforting notion exists 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 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 bands of criminals cooperate with one another for specific ventures or in particular districts of the metropolitan area? If the answer to any of the 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, and sophisticated rackets involving the physical security industry 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.²

Clearly, no one intelligence officers' course can provide thorough training for coping with these potential danger spots in the local jurisdiction. What it can and should do, however, is provide officers with the tools for understanding the complexity of the city and rouse them to think about the possibility that organized crime may penetrate the city's economic and political life at an unconventional point. The faculties of local universities, particularly the departments of sociology or urban

²See particularly the pamphlet written by Herbert Edelhertz and publicized by the National Institute of Law Enforcement and Criminal Justice: *The Nature, Impact, and Prosecution of White Collar Crime*, May 1970 and the Chamber of Commerce of the United States, *White Collar Crime*, 1974.

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 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 that 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. 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 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 later be extracted. An audience of intelligence officers would be an excellent forum for a discussion—perhaps conducted by an attorney—of systematized approaches to anti-corruption measures.

c. **Emphasis on Analytic Technique.** As noted earlier, a major part of the intelligence officers' course should be devoted to the intelligence process. This must be thoroughly 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 re-evaluation. 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 to clarify within the process 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 the analyst should ask about all data that come his/her 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/she will be getting closer to an understanding of what is expected of 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: What other information would I *like* to have to complete the picture? What other information am I likely to be able to obtain relatively rapidly and economically—that 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) to broaden my understanding of the whole problem? Assembling all the pieces—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? Do the results present a clearer picture than the one I had 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 would-be analyst asks all these questions while exploring the materials on hand, he/she will begin to get a feel for the analytic process. Analysts should, of course, be put through these paces on a number of different kinds of 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, and gathering evidence of skimming operations, 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.

One final word on analysis is necessary. Nothing can take the place of a young, dynamic organized crime intelligence unit analyst entering the classroom equipped

with the basic raw materials from which he/she has assembled a major study or investigation. If the analyst can spread these materials among the students and then describe, step by step, how the analysis was conducted and how the final judgments that emerged from this process were fashioned, he/she will do more to shed light on the analytic mysteries than any other participant in the program.

d. **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 that are the end products of the intelligence process. These latter reports 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.

(1) **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, 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 value of the information he/she has passed on.

(2) **The Analytic Report.** The analytic report is another matter altogether. It is quite possible that not all participants 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. 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 combined into a paragraph or two. Ideally, a senior officer of the agency should be asked to present views on what is needed by way of reports from the intelligence unit, and how such reports should be shaped to suit a particular taste 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. Consider, 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 a New England 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 \$3,000.00. The borrower immediately paid \$600.00 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 \$3,000.00 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 is that a conclusion is a 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.

e. **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 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 resorting to special in-service courses offered by the local police academy, or even Federal training, such as the Basic Agent's School operation by the Internal Revenue Service. However, at a minimum, the intelligence officers' training program should make it clear to the students how such skills can be used to produce sound intelligence.

f. **Security Training.** Security is a special problem for the intelligence unit and must be covered in the training course. (See Appendix E for a discussion of this problem.) The intelligence officer must know why he/she is subjected to a much more thorough background investigation than that of other officers. The officer must understand why this is essential even though he/she 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/she will work and especially for the material in its files. The officer cannot even be completely free to talk to other officers in his/her own agency about some of the matters under consideration in the unit. He/she must understand the difference between dealing with unsubstantiated reports and allegations harmful to the subject persons, and 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."³ Security should also be presented to the intelligence officers as 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.

g. **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, a new security concept for the intelligence unit, plans for in-service training, and intelligence and trends in the law. What has

been discussed at some length in this chapter is simply a minimum upon which other topics could be added as particular local needs demand or opportunities arise. Even as a minimum, 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" some or all of the program 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 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 are not particularly widely known or understood disciplines.

3. **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, and so forth.

But in all cases the objective remains the same—to stimulate rigorous thinking about the relationship between intelligence and command-level decision-making. 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 immersion into the process itself by those involved in decision-making.

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 can be done with the mass of paper coming across his/her desk, or will not fully grasp why he/she is being asked to acquire two additional investigators for the intelligence unit, or how the overall effectiveness of the unit can be measured, or offer any reasonable resistance to the

³For further elaboration see Appendix A, "Guidelines."

public prosecutor who wants to "let up a little on hijacking investigations and concentrate on gambling." In effect, the officer 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 subordinates. Instead of being buffeted by all these forces, the officer should be prepared to use intelligence for his/her own command purposes and for support in controlling the assets on hand. The only way to do this is to comprehend the intelligence process and its potential for contributing to the basic missions of the agency.

4. Understanding Methodology and Process. So far the discussion has centered on intelligence as a product—that is, the informed judgment 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 recognize that in a real sense it is responsible for setting the qualitative standards of the agency. Shoddy intelligence will result in bad decisions, faulty strategy, or unrealistic plans. Therefore, training at the command level should aim at clarifying the evaluative and analytic elements of the intelligence process so that the command level can assert its responsibilities for quality control at points where it may expect to make some impact.

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.

The above may sound more like management training than intelligence training. This is because good intelligence results only when there is sound management of the information flow and active concern about its 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 intelligence unit, but that it bring in the most innovative and even experimental approaches in use wherever they may be found.

CHAPTER VI

MANAGEMENT OF A POLICE INTELLIGENCE UNIT

The management of a police intelligence unit is a most complex job, perhaps the most difficult assignment that can be given to a supervisor in a police department. Intelligence cannot be approached as a normal traditional police function. Usually it is out of the mainstream of the department and it has an investigative rather than an enforcement role. Its files and the information it seeks are not focused on cases and evidentiary material, but on suggesting new areas of crime on which the police should focus, or new approaches to old criminals in their old areas of crime.

The commander of an intelligence unit seeks help in defining the functions of the unit and in deciding the most effective way to operate. Intelligence units responsible for following criminal activity are relatively new in police departments. In the past they have operated primarily against subversive threats to the society. Currently, with LEAA encouragement, police intelligence units are focusing on "organized crime." It would probably be better from the point of view of most police departments if this could be changed to major crime. In that way the intelligence unit could assist the chief and the investigative elements of the department in their efforts against major criminal activity in their jurisdictions. Often while major crimes would be performed by organized, or at least semi-cohesive groups, the efforts of the intelligence unit would not be restricted to this.

The unit commander is faced with the problem of obtaining investigators from the department who will be willing to investigate but not make arrests. The unit commander must develop a flow of information through investigators and by negotiations with other elements of the department and other law enforcement units in the area. Then, the commander must insure that the information is properly filed, reviewed, and analyzed to be certain that the unit is contributing to more effective enforcement actions against major criminals. The unit commander normally will be faced with the problem of obtaining information from other units because he/she will never have enough investigators who can produce an adequate flow by themselves. Thus through his/her own efforts and those of the chief, the commander must convince the commanders of other investigative units in the department and other law enforcement units in the area that they will gain by sharing information with the unit. This means that the commander must develop a

system whereby information is shared in return. Very seldom can a one-way deal be made effective in the police intelligence operation. In short, the commander of a police intelligence unit must have the combined talents of a street-wise investigator, an expert puzzle solver, an efficient file clerk, a sensitive diplomat, and an effective police supervisor.

Perhaps the best way to display the management problems facing an intelligence unit commander is to review the functions of an intelligence unit. The functions discussed below must be performed regardless of the size of an intelligence unit if it is to operate effectively. However, size will affect the number of functions individuals will perform and the type of procedures used.

A. The Problems

1. **Collection.** The collection function determines the extent and nature of the inflow of information to the intelligence unit. The source of this information may be reports generated by its own investigators from other investigative units in the department and from other law enforcement departments in the area. The reports may be formal, in that they are hard copies of investigators' daily reports of surveillances and other investigations done, or informal, passed by word of mouth, in person, or over the telephone. Newspaper clippings would also be included. Regardless of sources, the effectiveness of the intelligence unit is determined directly by the amount and quality of the inflow of information.

The first management problem posed to the intelligence unit in this functional area is to determine what information the unit needs. Ordinarily the general fields of focus for an intelligence unit are established by the chief of the department. These might include all activities traditionally associated with organized crime, a few areas such as gambling, narcotics, prostitution, and pornography, or all major crime as defined by the department. Whatever the general areas designated, it is the commander who must decide on specific targets. These targets will be persons, groups of persons closely associated, or a geographic area in which there may be different types of crime being committed either by the same group or by several different groups.

Once having decided on particular targets, the commander must then decide what sources will be used to

obtain the information. In some cases, the commander's own investigators may be sufficient. In others, outside help may be needed from other elements in the department and, if available, from other law enforcement agencies. The commander must determine how to obtain this assistance, using diplomacy to avoid causing any of the agencies involved to become angry with the operation and stop the flow of information. And finally, as a matter of principle, the commander would hope to avoid duplication by several agencies focusing on the same target at the same time.

But in a real sense, in many units this approach might appear theoretic. The unit commander must be practical. Decisions must be made in the complex environment that includes unexpected special projects assigned by the chief or new, unexpected crises. If the intelligence unit investigators are well trained, they will often be relied on for special investigative missions, more than likely in an enforcement role. With investigative manpower always less than required, the chief must use what is available to respond to reports of major criminal activities. The ironic twist is that the more a unit is caught up in line activities, the more its value is recognized. Yet it can devote less effort to projects that are intelligence-focused. It may also indicate that the chief is not completely convinced of the value of intelligence, or at least that it is given a lower value than other more tactical/enforcement-related activities.

In such an environment, which too often exists, the intelligence unit commander is the only person who can (and must) keep aware of intelligence activities. Despite all the pressures, the commander must keep reminding the chief or an immediate superior of the requirements of the intelligence task and of the potential value of its output if he/she is permitted the time and resources to perform the intelligence function. An attempt must be made to keep some of the investigators probing for additional leads in priority intelligence areas. And if there are no investigators, the commander must keep maneuvering to get them. The normal flow of reporting will never totally fulfill the intelligence unit's requirements for information. It must probe for data to fill the gaps left in the data files. There must be no doubt that an intelligence unit commander is, in most departments, in a most difficult spot.

The unit commander is also responsible for establishing guidelines that will inform investigators of targets they may cover and under what conditions. These must be made explicit in order to protect the unit from subsequent charges of illegal activity. The commander then has the follow-on task of insuring that the investigators, in fact, observe the guidelines.

2. Collation/Files. The next task of the commander is to determine the manner in which the inflow of information will be handled. It must be received, recorded, reviewed, and indexed. This process involves insuring that members of the unit with responsibility for the subject covered in the report are given access to the report, and that the unit commander is made aware of all important matters referred to in the several reports. The commander must establish a procedure for this process which does not involve too much time on a day-to-day basis.

The unit commander must establish an effective filing system. It should be one that minimizes clerical work to the greatest extent possible while providing the analyst with an effective tool. The heart of the intelligence process is analysis, that is, answering questions of "so what" raised by particular types of crimes and associations among major criminals. Regardless of the title of the person in the unit who performs such functions, he/she will need all the assistance possible. Since the most important single tool the analyst has is the files, the way the material is indexed, filed, and organized is of great concern. Hence, the analyst should have a major role in developing this system.

A second major requirement for the filing system is that retrieval of information be easy. There must be a minimum time required for a clerk to enter the files and find whatever information is requested. It is important that the information filed and retrieved be marked to show its reliability and sensitivity. Only in this manner can information in the files be protected from misuse. Finally, the system must be as simple as possible to enhance accuracy of filing so that on retrieval there is assurance that all information relative to a particular subject is made available.

In order to provide guidance, and at the same time ensure the legality of files, the unit commander, on the basis of pertinent Federal and state laws, must develop specific guidelines that determine what material can be entered into the files, how it is to be organized, and finally how information that is no longer deemed essential is to be purged from the files. These activities will only be accomplished if there are specific rules developed and some program adopted by the unit that oversees the process. There must be some automatic warning that the time for purging has arrived. There should also be some manner of displaying types of information that can be entered into the files so that the file clerk has no excuse for entering incorrect or improper information.

3. Analysis. The analytic function poses a very difficult problem. Its importance has been discussed above. But its importance as a problem to the unit

commander is largely a result of its not being traditionally a specified function within a police department. It is the chain of thought that all investigators use in solving their cases; but ordinarily it is not considered a function separate from the normal course of investigation. In an intelligence unit, however, this function must be treated as a separate activity.

Who does the analysis is not as important as its need to be done. If there is a large 200-300 person unit, who does the analysis is found by organizing and detailing a group of police officers or civilians as analysts. This is their primary function. Where there is a small unit, perhaps 6-10 persons, analysis may be done by the unit commander. The commander may choose to review all reports and develop and test hypotheses by assigning certain avenues of search and targets to investigators. In either case, whether there is 1 person or 20, they are performing the same function.

The task of the unit commander can be eased considerably if he/she is given the opportunity to train analysts or put them through a training course. At the present time, such courses are sponsored by the California Department of Justice, the Dade County Department of Public Safety, the International Association of Chiefs of Police, and the Law Enforcement Assistance Administration. Essential tools of analysis will be given to the analysts at these courses and, provided there is a sufficient flow of information coming into the unit, the analyst should be able to make a major contribution to the activities of the intelligence unit in support of the department.

The fulfillment of the analytic function poses a dilemma to the unit commander. A decision must be made on the division of the analyst's time between supporting tactical operations and producing longer-term studies or reports. Effective support of other investigative elements of the department gives the intelligence unit recognition and support. It substantially helps to overcome the information flow problem. By leading directly to enforcement actions, it builds a rationale for its continued existence which can be used when the department's budget is under review. But the intelligence unit is the only one in the department with a mission to look at criminal activities across the department's jurisdiction. In so doing, it must try to warn the chief of potential new areas of criminal activity. In this respect it is essential to understand that estimating the future is one of the basic roles of intelligence and the analyst is charged with performing this task. The unit commander will continuously struggle to have personnel available to fulfill this role, especially if he/she is performing well in the tactical field. The chief of investigation in the department will be demanding that analysts and intel-

ligence investigators be assigned to help personnel in major cases.

The unit commander must decide how the unit is to disseminate its output. In part, this is specified by the chief and the procedures under which the unit was established. Ordinarily, on the tactical side, information is disseminated to department investigators and other commanders by telephone and by short memo in response to the request for whatever information the intelligence unit may have on a particular person or criminal activity. Usually these requests are specific and therefore the replies tend to be short. The longer-term reports that the intelligence unit produces may detail the activities of an organized group of criminals or provide a picture of major criminal activity in a particular area. These reports are often self-initiated by the unit and the distribution is then determined by the unit commander within the guidelines established by the chief and/or the department. In all cases, the intelligence unit should adopt an affirmative program, disseminating information and output of the unit as widely as possible within the constraints of sensitivity. The concept is to break with the tradition of holding intelligence information closely. From the point of view of law enforcement, information in an intelligence file that is not used is worthless.

The circulation of intelligence information outside the department poses a separate problem. The unit commander must decide who might receive material and under what conditions. In many cases, the department itself will set general rules to guide the unit commander. Nevertheless a decision must be made on how to apply the general rules in each specific request. Membership in the Law Enforcement Intelligence Unit (LEIU) assists the unit commander in solving the problem since he/she will know that other members observe at least minimum standards of security.

The major operational problems with which the intelligence unit commander must deal have been covered. In the paragraphs that follow some suggestions are made as to how intelligence unit commanders might successfully solve or overcome these problems.

B. Suggested Solutions

1. Relationship With the Chief. The essential element to the success of an intelligence unit is the understanding and support of the chief of the department. An intelligence unit is a staff agency to the department as a whole and therefore must have the support of the chief. Only if this support exists and is overt can the intelligence unit commander establish effective formal working relationships with all the other elements of the

department, in particular those that result in a flow of information to the unit.

The support of the chief, to be fully effective, must rest on his/her understanding of the role and mission of the intelligence function. If the chief does not appreciate what intelligence can do, the unit will continually be used for special projects. This will detract from its performance of intelligence-focused tasks. The intelligence unit commander must educate the chief when the value of intelligence is not fully understood, especially with respect to the potential contribution to be expected from analysis based on an information flow from all elements of the department. This can be a delicate proposition and is best approached by producing analyses that do contribute to enforcement action.

It is the chief who should define the objectives of the unit and, in consultation with the unit commander, establish an adequate staff. If the chief performs these functions, it becomes very clear to the department that the intelligence unit is a staff agency working for the boss. It should be noted that in some of the larger units it is felt impossible to have the intelligence unit work directly for the chief. The organization lacks room in the span of command. In such cases, it is essential that the intelligence unit at least report to the second-level supervisor, either a deputy chief or perhaps, as in many cases, the chief of the inspectional services.

It must be accepted that in many cases the intelligence unit is considered an interloper in the department. It is competing for personnel and other resources and, in some cases, it is directly competitive in that the unit continues to make cases. These feelings and situations must be taken into account and every possible effort made to minimize their potentially adverse impact on intradepartmental cooperation. The best approach to this by an intelligence unit commander is to establish a direct support base at the highest level in the department. This should be done even though some will view the relationship with the chief adversely. The unit commander is in a situation where he/she will be damned either way—but cannot win without the support of the chief.

As a practical matter it is not always easy for the intelligence unit commander to communicate directly with the chief or, if so, to have freedom to encourage the chief to think about the importance of intelligence. In many cases, the only time the intelligence unit commander meets with the chief is when the chief calls and either asks questions or gives a special assignment. At these times it would be difficult to bring up a generalized subject of "Chief, you ought to understand more of what the intelligence unit can do for you." A few specific suggestions of approaches that the unit

commander might try to improve the relationship with the chief and provide the chief with a better understanding of the function and value of intelligence are given below.

- **A Special Report.** The unit commander might try to produce a special intelligence report for the chief. For this to have any value, the items reported on must be significant, be presented concisely, and be the sole source for the chief. This can be achieved through the use of analysts even when the facts are called to the chief's attention by some other senior official. The intelligence unit commander, through analysis of the implications of this information relative to other information and analyses in the unit files, can provide a new viewpoint. By and large, the simple reporting of facts does not make a special report a useful tool from the point of view of the intelligence unit commander. Furthermore, it should not be a periodic report, but should be produced only when the intelligence unit commander has something to say.

- **Activities Report.** Another way to make the chief aware of the value and efficiency of the intelligence unit, especially in its relationship with the rest of the department, is to provide the chief with a weekly report of its activities and, in particular, its support of other elements in the department. This should include a total of answers to requests for information from every other person in the department. To give quality to this type of report, the aggregate number should be broken down into significant categories such as narcotics, major burglaries, hijacking, or whatever the important crime areas in the jurisdiction happen to be. This will emphasize the fact that the intelligence unit is on-line, supporting the department in its major criminal enforcement areas. The report should also include an aggregation of support given to other law enforcement units locally and elsewhere. If there is any significant breakdown that appears in this support, then this too should be removed from the aggregation. The report should also include whatever the intelligence unit has done specifically in terms of self-initiated action or activity directed toward targets determined by the intelligence unit commander after consulting with the chief and/or heads of other investigative units. This might include a statement of the progress in establishing the potential for major cases before they are handed over to enforcement.

This total report, by proper formatting, should take no more than one page; but it could become an important means by which the intelligence unit commander can remind the chief not only of the fact that the intelligence unit is busy, but also of its value to the department as a whole. It cannot be emphasized too

much how critical the last point is if the intelligence unit is to become fully effective. (For further discussion see "Keeping Score" below.)

- **Request for Support.** A third means for keeping in touch with the chief is for the intelligence unit commander, when support is needed from the other units in the department, to request this in a formal memo sent through the chief's office for approval and forwarded to the element from which the support is being requested. In this manner, the intelligence unit commander can keep the chief informed of unit activities and also the need for support from other units in the department. To the extent the chief agrees with this approach, the requests for support will become an order when the chief or his/her office approves them and forwards them to the element requesting the support. It is imperative, if this approach is adopted, that the intelligence unit commander prepare the way by discussing the request with the recipient before it is received to minimize frictions. The intelligence unit commander should always remember that support and assistance are needed from the rest of the department.

2. **Developing an Adequate Flow of Information.** The second essential element to the success of an intelligence unit is to obtain an adequate flow of information so the unit can be effective. The kinds of information have been discussed above in the chapter on collection. We are now concerned with how the unit commander, having gained the support of the chief that the unit must focus its efforts on certain selected criminal activities, actually arranges to get the information flowing into the unit. In most instances, it is not a straightforward problem, as most intelligence commanders know. In few cases can this information flow be achieved easily. There are all of the traditional problems of jealousy and unwillingness to share information, especially that obtained from informants or that which is involved in current cases. The following sections discuss a few approaches that may help unit commanders achieve a practical solution to these problems.

- **Direct Approach.** The simplest approach is to work directly on the chief and convince him/her that an enlarged flow of information is essential if the unit commander is to perform the intelligence function. The results should be an order to this effect. This is often most difficult to arrange if the unit has been operational for a number of years. On the other hand, it is by far the best way if a new unit is just being established. This is the time to convince the chief that if the new unit is to be effective in the department, it must have cooperation from the other elements in the department.

- **Test Case Approach.** Another less direct approach is to discuss the problem with the chief and/or

the immediate supervisor of the intelligence commander. Here the intelligence unit commander could suggest the need for further information even though he/she understands the reluctance of the other unit commanders to provide it. However, the commander believes that a great deal of help could be given to the other unit commanders in performing their duties as well as in helping the department itself if more intelligence information is available. The commander then would propose that the chief and the other investigative units agree on a test area. This might be auto theft, narcotics, gambling, or fraud. The idea is to pick the single area about which all units of the department would agree to channel all information into the intelligence unit as it is obtained. This would include the highly important operation of debriefing informants about criminal activities other than those for which they are ordinarily responsible.

The intelligence unit commander should not initiate this approach until a potentially successful area is selected. The commander would then assign the best analyst to work the material, seeking suggestions and leads for the enforcement unit responsible in this area. The commander would also attempt to surface in reports to the chief and other senior officers the relationship between activity in this selected criminal area and other areas of crime. The commander would do everything possible to show what the intelligence unit could do if it had an adequate information flow.

- **The Task Force Approach.** Another way to get at this test case approach would be to pick a particular area where a major investigation could result in a quality enforcement action (more than street level). The intelligence unit commander would outline the proposition and propose a joint or team action. A task force could be made up of personnel from the investigative unit responsible for the particular area of crime to which the intelligence unit commander would attach one or two investigators knowledgeable in the area plus an analyst. The command of the team, the intelligence unit commander would suggest, should rest with the enforcement unit. The idea would be to demonstrate that a major enforcement action could be brought off more readily and effectively by a continuous, close, coordinated effort between intelligence and the enforcement unit. It would also demonstrate what the intelligence unit does with information and how useful it is for a flow of information to come into the intelligence unit. At the end of this operation, the proposition would be made that the information the intelligence unit was getting about this particular area of criminal activity would continue. Then the intelligence unit commander could suggest a joint action in another area and so on until the department is convinced, and a large flow of information

would move into the intelligence unit on a more or less regular and automatic basis.

● **Keeping Score.** A less specific but still practical approach would be to improve the flow of information by reporting on what the intelligence unit does for the department. So often at the tactical level the intelligence unit answers telephone inquiries and helps investigators obtain information. This is done on a semi-informal, personal basis, and it takes up a great deal of time. Unless there is some means of recording and reporting on this activity, no one in the department appreciates the full extent of the intelligence unit's activities. This is because the tactical support is on a one-to-one basis and may never come to the attention of the supervisors of the investigators who are getting the help. Considerable time is also spent answering requests from other departments. This too must be recorded or no one in the department will know what the intelligence unit is doing.

The best way to approach this problem would be to institute a form in the intelligence unit whereby all telephone and other types of tactical support are recorded. This should, at a minimum, have the date, manner in which the assistance was given, certainly the name and unit to whom the information was supplied, and a short indication of what kind of material, perhaps recording the name of the subject on which the information was given. If this approach is adopted, the unit commander will be able to derive additional intelligence because, by this method, he/she will find certain foci of interest to investigators either in the department or elsewhere. The commander can then begin to ask the question, "Why this interest in these criminals?" The commander can also direct unit personnel to probe more into areas associated with the subject criminals and produce additional intelligence support for the investigators who originally requested the material. This form would become the basis for a weekly report that would be widely circulated in the department. It would indicate briefly the number of inquiries made to the intelligence unit, where they were made from, and the number of inquiries answered. By doing this, other elements in the department may begin to appreciate more fully some of the activities of the intelligence unit. This report could be the source of a specialized version for the chief as discussed above.

At this point we are only focusing on the tactical aspect of intelligence production. The strategic intelligence activities of the unit will become apparent to various supervisors and the chief through the publication of reports. But without a report on the tactical aspect, the unit commander will lose a great deal of understanding of the activity in which the unit is engaging. In many

units this results in remarks by members of the department such as "What good is the intelligence unit or what support are they providing to us," and "Since they're not doing very much there's no point in my going to the trouble of sharing my knowledge with them."

Note should be made here of the particular problem presented by the special intelligence or investigative unit that has been established by a state's attorney general or in a county or city district attorney's office. To be fully effective in most instances, they will need more information than can be developed by their own investigators. The major source ordinarily would be the local police department and, to whatever extent can be worked out, Federal agencies. The only manner in which the prosecutor can achieve the flow of information required is to establish a basis for formal cooperation. Normally the information flow is achieved on an informal basis with one investigator working with another over a period of time and having established a relationship and trust for each other. But this is not sufficient for major cases or for working on an intelligence basis where an attempt is being made to develop the potential enforcement actions against major criminals. A more regularized flow of information is essential. This probably can best be encouraged by negotiations between the prosecutor and the local or state police who have one or more persons established with the special unit. The presence of this investigator on the prosecutor's staff would ensure a two-way flow of information from the prosecutor's office to the police department and vice versa. Essential to such an agreement is the practical matter of sharing credit for any successful enforcement action. There should also be some agreement for mutual support in budgetary hearings to explain why the assignment of the investigators to the prosecutor's office is of value to the jurisdiction.

3. **Focus of Effort.** Having established the support of the chief and the guiding objectives of the unit, the next issue for the intelligence unit commander is to determine the method of operation. Almost without exception, the unit will have been given general areas of responsibility that press the limits of its capability. Thus, the unit commander must develop some approach that will establish priorities to ensure that the most important tasks get done. If not focused, the intelligence unit, with limited personnel, will do little more than name checks for investigators. The priority of effort should link the activities of the unit investigators with files and analysis. This encourages a fruitful interaction between the knowledge and techniques of the analysts and the criminal activities being reported on by the investigators.

But there are two distinct, interacting levels at which priorities of effort must be established. One relates to support of major investigations directed by the chief or head of the investigative element in the department. The second relates to the exploitation of accumulated information and analysis existing within the intelligence unit. It is assumed that tactical or direct support to the normal operation of investigators will be available without the development of priorities. But the latter will have to be taken into account in allocating personnel and duties.

Often as the intelligence unit proves its capability, the demands from investigators swamp the system. This is particularly true if the intelligence unit is participating actively in major departmental investigations. At the same time, there tends to be less appreciation of the value of strategic intelligence projects because their payoff in enforcement action may be a matter of months or even years away. For small units, the problem is even more difficult.

The management problem posed to the intelligence unit commander is to achieve an allocation of effort between the tactical and strategic demands placed on the unit, based on an explicit determination of priorities.

- Tactical means direct support to investigators, usually in the form of a response to a telephone or oral request for information about a specific person.

- Strategic means a focusing of information in files, new information developed by investigators specific to the criminal activity being explored, and an analytic effort to put all the information together in a hypothesis that lays out a potential explanation. The explanation can suggest relationships among key criminals, new areas of criminal activity by, as yet, unknown criminals, interrelationships between areas of criminal activity, and so forth. Strategic intelligence should look to the future as it is an initiating rather than reactive tool to get ahead of criminals.

Three management techniques should help solve this allocation of effort problem:

- The intelligence unit should minimize its involvement with action against street-level crime. Even in its tactical mode in assisting investigators in their current cases, the support for non-major cases should be largely restricted to name checks. The unit will not have the personnel to do analysis to assist the investigators on low level crimes. If possible, the investigative units should be told of this limitation and why. This will tend to minimize adverse reactions to the intelligence unit's minimum response efforts to less than major crimes. The collection plan effort described below will assist in relating this point to all elements in the department.

- The ability to provide direct, tactical support to investigators from other elements can often be enhanced and, at the same time, the pressures of intelligence unit investigators, analysts, and supervisors reduced by hiring and training file clerks and secretaries to answer telephone and written queries in addition to their own duties. An SOP should be written that describes in specific terms what they are to do, what categories of information they can deal with, and those for which they must obtain approval from a supervisor. The initiation of this approval will take some time because of the training requirement and because of the need to convince investigators from other elements of the department that these personnel, probably civilian, are to be trusted and are doing an accurate job in responding to requests for information.

- The development of priorities for the intelligence unit should, in a very real sense, be part of a system whereby the department establishes targets on a priority basis for enforcement action against major criminals. This approach insures that major criminal investigations have the full support of the intelligence unit's capabilities. On the other hand, it insures that the intelligence unit participates in the mainstream of the department's major criminal investigative activities and, as a result, will probably gain access to the flow of information it requires to be fully effective.

What is suggested here is a priority investigative plan that would be produced once a month. The draft of the plan would be produced in two parts. The first part would be developed by the investigative unit(s) of the department and would list major criminals to be targeted. They would be selected on the basis of their "worth" as major criminals and the probability that they would be arrested and indicted. If there is more than one investigative unit, then each would develop a list.

The second part of the plan would be produced by the intelligence unit. It would contain a list of no more than five alleged major criminal figures which the unit believes could eventually be targets for enforcement action. From time to time the intelligence unit could also suggest as targets a type of criminal activity that is growing or is new to the jurisdiction, an area where various criminal activities are growing, or a location where known and alleged criminals appear to be congregating. The unit's draft would include a statement of the major gaps in its knowledge of the targets and the assistance it would need from the other units.

This two-part plan would be circulated to the principal commanders in the department for review and, at a monthly meeting with the chief, the proposed actions would be discussed. The plan could be modified

at the meeting. But once it was approved by the chief it would become the priority target list for the next month. As a practical matter, some of the investigations would take more than a month and, at the time of their approval, it would be so indicated in the plan. However, these longer-term projects would have to be reviewed each month, and placed in competition with currently developing situations. This might result, for example, in a decision to delay or suspend some actions for a month or so while more pressing problems are cleared up.

The approval of the plan would require other units to assist the intelligence unit to the extent specified. It would also require that all information on the targets that develops in the course of other investigative work would be turned over to the unit. But in turn, the approval would also require the unit to give all support possible to the other investigative units in their efforts to build a case against the target criminals.

Within the intelligence unit itself, the commander can develop a draft priority list by utilizing the capabilities of investigators and analysts. The commander can task them at daily or weekly meetings to review the criminal activity in the jurisdiction and to suggest targets against which profitable intelligence becomes clearest. Intelligence is seeking to develop information that suggests avenues of approach to eventual enforcement actions. The intelligence unit is not developing an evidential base for the enforcement action. Thus, when priority targets are suggested they normally would be ahead or to the side of a major enforcement case the department has underway. The intelligence unit is trying to develop a basis for the next case beyond the current one or for other avenues of approach to other areas of criminal activity in the jurisdiction.

C. Supervision

The intelligence unit commander, having established a relationship with the chief and other seniors and having a plan of action that is approved, now must establish management procedures that will ensure that the unit functions effectively. Perhaps the best method for assisting in this is to hold daily meetings. If the unit is small, all members should attend—analysts, clerks, and investigators. If the unit is large, probably only one or perhaps two levels of supervisors would attend. The concept, however, is to ensure that the unit as a whole knows the targets, the activities of the unit, and the information needs. Not only do the investigators know their targets, but they know what other information could be important. This helps the analyst determine what analysis is most needed, and the file clerks to be aware of pieces of information they should call to the

attention of their supervisor. In other words, the approach is to consider all members in the unit as part of the team working together rather than operating independently.

With respect to investigators, it probably is best that the unit commander or at least the supervisor of the investigators either assign or know explicitly the daily tasks of the investigators. The same person should also receive a report at the close of the day detailing the activities of the investigators. The reason for the relatively close supervision is that in most cases the number of investigators relative to the job will be small and every effort should be made to ensure that the time of the investigator is spent as effectively as possible. Part of the process of achieving this effectiveness is to have their individual efforts reviewed collectively to avoid duplication.

D. Selection and Training of Staff

The ability of the intelligence unit to achieve its objectives rests with the quality of its staff. The person responsible for selecting the staff is the unit commander. This is one of the commander's most critical management functions. Staff must often be selected within a personnel system established for patrol and investigative activities and in which little thought has been given to the special needs of an intelligence unit. For example, the intelligence investigator must be willing to turn findings over to another person who eventually will make the arrest.

There is also the problem of selecting analysts. Police are usually more interested in enforcement action than in sedentary work. On the other hand, there are problems in hiring civilians. Police do not want to exchange information with non-badged personnel. Moreover, civil service guidelines often have no job descriptions that fit.

The best hope that the intelligence commander has in this field lies in the relationship with the chief. The commander must work from there to try to modify the personnel system to make sure that in the assignment of police officers to the intelligence unit, the intelligence unit commander has the right to accept only those that meet established standards.

With respect to the analyst function, there is enough evidence to suggest that a unit that includes both civilian and police personnel as analysts has a much stronger capability than one that has only police or only civilian personnel. What is most useful to the analyst unit is a mix of knowledge of the street with the more academically trained civilian analysts. They can exchange knowledge as well as techniques. The acceptance of the

civilian analysts by their police colleagues within the analytic unit assists in minimizing the problem the civilian analyst has in gaining acceptance into the department as a whole.

The operation of the files should be a civilian clerk function. It seems inappropriate to put police officers in a file room when they could be more effective on the street.

Once the right of selection of personnel is given, the unit commander must train these persons for the unique activities of the intelligence unit. To the greatest extent possible, all assigned personnel should be scheduled to go to a training course before they assume their duties in an intelligence unit.

The problem of establishing a training course is not easily solved. One solution is to try to reserve slots in the two schools now being supported by LEAA—one run by the California Department of Justice and the other by the Dade County Department of Public Safety. The only other solution is for a major unit or a series of small units to request assistance from a local college where courses in criminal justice are being taught. This suggestion applies principally to the analysts. The intelligence investigator is usually assigned from the other investigative units in the department and therefore has training as an investigator. What is needed at this point is to get this person to understand how an intelligence investigator operates and how to overcome problems regarding enforcement actions. There is a difference in the investigator's approach because the intelligence unit investigator is seeking to find potential avenues of approach to a criminal rather than the necessary evidentiary base required for enforcement action.

Solving white-collar crimes requires specialized training in accounting, legal matters, and financial operations. White-collar crimes involve following "paper trails." The ordinary activity and training of an investigator does not equip a person for this very specialized operation. Training in these fields can often be arranged through the local community colleges. The California Department of Justice has a course in economic crime.

E. Evaluation

At the present time there is much discussion about the need for evaluation. There are several suggested approaches in this manual, but the final decision must be made by the individual department. If the evaluation of the unit is to be performed by an outside unit, who or which one will be trusted by the unit commander or by the department? Would a state agency be accepted by the local and county departments? The problem of establishing a means for evaluation is very difficult. Even within the department, the willingness of an intelligence unit to expose its files to persons from the inspectional unit in an evaluation may not be easy to achieve. Yet periodic evaluation of the operation of the unit is essential. There is no other manner in which the chief and the unit commander can be assured that the operation of the intelligence unit is directed toward achieving the specific objectives assigned to it. There are no arrest statistics that can be used to evaluate the operation of an intelligence unit.

Short of any other evaluation system, it is suggested that the unit commander establish a self-evaluation system. (See Appendix G on Evaluation.) This would consist of a periodic formal review of the specific operation of the unit. These evaluations would give a basis for modifying or changing a commander's approach. It would apply to the process of producing intelligence but would have little to say about the quality of the output. This can only be established by the intelligence unit commander consulting the consumer about the product. That means that the commander must seek feedback from the chief, other senior officers in the department, and the investigative units that assist in the department and elsewhere. A simple questionnaire might be used to this end (see Appendix E). Since the intelligence unit is a staff rather than line unit, the only persons who can evaluate the quality of its output are those who use it. Intelligence can help lead to an enforcement action, but enforcement action can seldom be traced directly to an intelligence operation alone.

APPENDIX A

GUIDELINES FOR POLICE INTELLIGENCE UNITS

Police intelligence units must be aware of, and responsive to, the reactions of the courts, the Congress, and many state legislatures to the activities of Federal and certain state and local law enforcement agencies in the late 1960's and early 1970's. In general, the thrust of the court decisions and new statutes is to put considerable restrictions on the operations of police intelligence units and to suggest that further actions along these lines may be expected. In part, the courts and legislatures are reacting to certain publicized excesses and illegal actions on the part of law enforcement units. In part, they are reacting to the Watergate situation in which the credibility of government and governmental agencies was placed in doubt. But regardless of the reason, the restrictions present a new mode of operation to police intelligence units which must be recognized. If they are not, a unit stands to have its files made public and its operations challenged in case after case. As a simple matter of survival, it is essential that this situation be recognized and actions taken that are responsive to the new legal guidelines.

The new statutes and court decisions are focused in three areas of the intelligence process, the targets and modes of investigation, the information that can be kept in files, and the information that may be disseminated by the intelligence unit. The fact that the legal activity has focused on these areas has, in a sense, totally encompassed the intelligence operation because these are the focal points of the flow of information into the intelligence unit and its products out to the consumer. These regulations have an impact on the very basic nature of the intelligence operation. For these reasons, it is essential that intelligence units understand their implications.

At the present time the most stringent regulations are at the Federal level. These include the Freedom of Information Act of 1966, as amended in 1975, and the Privacy Act of 1974. The first act reflects a concern of Congress that all information available to the government, with certain exceptions for national security and law enforcement action, should be open to the public. The second, however, states that personal records, with certain exceptions, should only be made available after prior written approval of the person involved. In addition to the two Federal statutes, there have been

numerous Federal court decisions in this field. Several states have also passed laws similar to the Federal statutes, and state courts have taken into account the Federal court decisions.

It is the recommendation of this manual that law enforcement agencies generally take into account the restrictions posed by the Federal statutes, attempt to put their intelligence units' operation into conformity with these, and hope that the subsequent state laws are no more stringent than the Federal laws. At least by taking this position, the intelligence unit is in conformity with the current decisions on the subject of intelligence information and its gathering, filing, and dissemination.

The "guidelines" that are outlined below are not intended, in any sense, to be precise. They are suggestive of the type of reaction by intelligence that seems to be called for in light of the laws and court decisions mentioned above. The approaches are a combination of the author's concepts and those recently adopted by a series of state and local law enforcement agencies.

Specifically what is suggested here is that there be guidelines established by each police department or other law enforcement agency to govern the operation of its intelligence units in criminal law enforcement. Before adoption, the guidelines must be reviewed by legal counsel, either the department counsel or the local or state prosecutor. The guidelines must be approved by the chief and disseminated to the department. All of this must be understood as the terrain on which the chief has selected to fight. It must be recognized by all the chiefs that their intelligence units are subject to court actions. If the unit is to be efficient, it must know it has the support of the chief. It cannot operate when the investigators, the analysts, and especially the unit commander are in doubt as to the chief's support of their actions. It is possible that, in some cases, the individual investigator or unit commander can be put in a position of personal liability. The latter development obviously depends on the direction taken by state statutes. However, it must be noted that the Federal statutes stipulate that an individual law enforcement officer (personnel of an agency) may be held accountable and fined for handling records not in accordance with the provisions of the statute.

A. Guidelines for the Investigator

A new series of restrictions applies to the intelligence investigator. It is imperative that the intelligence investigator be aware of these and observe them so that his/her actions do not lead to a court action to open the intelligence files to public survey or damage a case for the prosecution. On the basis of Federal statutes and

recent court decisions, it would seem apparent that the intelligence investigator should have prior approval before launching into an investigation of a person, group, or a particular location at which alleged criminals gather.

• One example of a solution to the problem is that adopted by the Long Beach (California) Police Department, as follows.

CRITERIA GOVERNING INTELLIGENCE SUBJECTS

The following criteria define those individuals and organizations that may be considered for investigation by the Intelligence Section; or for which intelligence information may be collected. Investigations or information collected on subjects which do not adhere to these criteria require the express approval of the Intelligence Section Commander or the Chief of Police. Information collected may be used (only) for legitimate law enforcement purposes.

The principal criteria for collecting intelligence information or establishing a file on an individual or organization is that a legitimate and reasonable cause exists for initiating an investigation or developing an intelligence file.

ORGANIZED CRIME

Individuals who—

- 1) Are currently active in organized criminal activities in the City of Long Beach
- 2) Are currently active in organized criminal activities outside the City of Long Beach, and either reside in or frequent the City of Long Beach.
- 3) Have a strong criminal association with known organized crime figures.
- 4) Are known to be engaged in planning, financing, organizing, or committing organized criminal activities.
- 5) Have been convicted of a crime which lies within the Intelligence Section's purview.

Organizations located in Long Beach or affect Long Beach and-

- 1) Are involved in illegal activities.
- 2) Are financed, controlled, operated, infiltrated, or illegally used by crime figures.
- 3) Are legitimate business enterprises but serve as fronts for organized crime activities.

- 4) Are associated with organizations or individuals located outside the City of Long Beach that are involved in organized crime activities.

In certain instances where the nature of the criminal activity is not immediately known or identifiable, a preliminary investigation may be authorized by the Intelligence Section Commander to determine whether a legitimate law enforcement reason exists for continuing the investigation. A decision as to when such an investigation should be terminated will be made by the Commander or Sergeant in consultation with personnel involved in the investigation. Factors that will be considered in such an investigation will be the need for the investigation; whether sufficient reasons exist to continue the investigation; its importance or significance to the Section, Department, or City; the benefits to be derived; the manpower and cost; and the impact if the investigation is terminated.

• The guidelines must not only deal with types of targets, but also methods. Of particular importance are regulations governing use of electronic surveillance (where legal) and photographs. Another example of guidelines for investigators is taken from the New Jersey State Police Intelligence Bureau manual as follows:

A. The Bureau Chief is responsible for the proper and efficient administration of the Intelligence Bureau. It will be the responsibility of the Bureau Chief to insure that the procedures as contained in the policy guidelines are properly adhered to. The Bureau Chief will evaluate the intelligence process on a semi-annual basis to insure that any new legislative and/or judicial guidelines are being adhered to.

B. Collecting of Intelligence Data

- (1) Personnel of the Intelligence Bureau will only gather information on any persons or groups as set forth in the goals and objectives.

- (2) Electronic surveillance will only be conducted in accordance with the provisions of N.J. Statute 2A:156-A. The Unit Head of the Electronic Surveillance Unit will be responsible for insuring that the statutory guidelines are adhered to. Any violations of these guidelines will be brought to the immediate attention of the Bureau Chief (See S.O.P. #270).
- (3) Photographic surveillance will not be conducted without the authorization of the Bureau Chief and/or his designee. Such authorization must meet the following criteria:
 - (a) To identify any and all persons, either as members or associates of groups or criminal organizations, who are engaged in an illegal activity.
 - (b) To provide evidence of any illegal activity involving criminal organizations and/or persons or members of these criminal organizations.
- (4) All photographic surveillance will be reviewed by the regional unit supervisor and the Bureau Chief to insure that person(s) *not* deemed to be part of any organized criminal conspiracy are not recorded and placed in the files of the New Jersey State Police Intelligence Bureau. All photographs taken that do not meet the goals and objectives of this operating procedure shall be *immediately* destroyed. In the event it is determined that the photographs are in accordance with the provisions outlined, the intelligence officer shall attach a report identifying those person(s) in said photographs.
- (5) Personnel who are assigned the task of conducting "undercover" investigation into organized crime activity will be properly instructed as to the goals and objectives of the Intelligence Bureau.
- (6) All information received by personnel assigned to the Intelligence Bureau will be properly evaluated and the source of said information will be noted in the report. Such designations shall include "personal observations," "informant information," "media source" (and cite the name of the publication), etc. The information must

be properly evaluated in accordance with the prescribed guidelines.

• Further emphasis is given to the problems facing law enforcement agencies by a review of the many recent major Federal and state court cases pertaining to police intelligence gathering activities. A not-for-profit organization, Americans for Effective Law Enforcement, Inc. (AELE), is now seeking to collect such cases and to call police departments' attention to their implications. Given below is an example of the AELE conclusions on this subject published in December 1974. AELE does not intend that its findings be taken as legal advice but rather as pointers for further review of the legal situation in a particular jurisdiction, as discussed in the following:

Police intelligence gathering activities have been historically directed against two major groups: the crime syndicate and subversive activities. The former target consists of professional criminals who conspire or act in concert to violate laws proscribing gambling, prostitution, narcotics and drug use, and similar offenses. Hijacking, the infiltration of legitimate businesses, extortion and bribery are related crimes perpetrated by organized crime figures.

Subversive activities refer to those persons or groups who commit sabotage, acts of terror, kidnapping, bombings, arson and lesser offenses for primarily political purposes. Often-times the principals in politically motivated crimes involve themselves in or assume leadership of political action groups that ostensibly seek reform through peaceful methods such as picketing, protest assemblies and rallies.

Other common but less traditional police intelligence activities involve the investigation of labor racketeering, burglary rings, juvenile "gang" activities of a criminal nature, and corrupt practices by public employees.

For the purpose of this brief, no distinction will be made in discussing case law respecting the activity sought to be investigated. Distinction will be made, however, when the gathering methods employed or the data accumulated bears no realistic possibility of eventual criminal prosecutions. Readers should assume, with this caveat, that the activity questioned applies equally to organized crime, subversive and other targeted investigations.

DEFENSE PRACTICE POINTERS*

In general, uniformed police officers may attend meetings that the public is invited to.

The interest of public order and safety is sufficient reason. *MOHAMMED v. SOMMERS*.

The purpose of the attendance must be a legitimate concern for public safety or order, and not to promote hostilities. *LOCAL 309 U.F.W. v. GATES*.

Police officers may openly photograph demonstrators, protesters, and attendants at public or semi-public meetings.

The mere presence of officers does not cause a chilling effect. Cite *LAIRD, BALDWIN, ARONSON, DONOHUE, ACLU, HANDSCHU* and the two *VVAW* cases discussed.

Overt photography or surveillance may not be used to harass individuals.

Injunction relief will lie against such action, *GIANCANA* and *GALELLA*.

Damages may be awarded. *SCHULTZ* and *ELLENBERG*.

Police officers may conduct covert surveillance in public places.

Observations, from public places, through open windows are permissible, see *HOLLOWAY, JENKINS, and ASHBY*.

Binoculars may be used, *HODGES, JOHNSON* and related cases.

Flashlights may be used, *MARSHALL, U.S. v. WRIGHT* and related cases.

Officers may enter upon open fields to conduct surveillances, *HESTER, CARR, and ST. v. STANTON*.

Officers may walk down open corridors, and lawfully observe or overhear incriminating things. *U.S. v. LEWIS, GIL, ST. v. PENNA, PONCE* and related cases.

Officers may conduct clandestine surveillance in the public part of restrooms.

Covert watching of open stalls and urinals is permitted. *PEO v. YOUNG, PEO v. HEATH, and MITCHELL*.

A suspect has an expectation of privacy from visual surveillance in a locked stall. *BRITT and BIELICKI*. Note *SMAYDA* exception as to unlocked by closed stalls.

The use of undercover agents, informers and infiltrators is lawful, absent underlying motives of harassment.

An agent may assume a false identity and pretend to be interested in criminal activity. *LEWIS v. U.S.*

A citizen informant may be recruited, and urged to gather information helpful to the police effort. *HOFFA v. U.S.*

Officers may pose as students or members of apparently legitimate organizations and institutions. *GABLEY* and *SOCIALIST WORKERS PARTY*.

If officers infiltrate a group in bad faith, or in reckless disregard of the rights of attendants, and do so to oppose the political philosophies of the group by making arrests, an action will lie. *LYKKEN v. VAVREK*.

The identity of informants will be preserved confidential in civil cases as well as criminal ones. *METROS* (civil), *McCRAY* (criminal).

Class actions are not created simply because diverse groups desired the courts to grant the same relief to all. The courts refused to certify a class in *BALDWIN v. QUINN, HOLMES v. CHURCH, and VVAW v. BENECKE*.

Conclusionary allegations of subjective harm fail to meet the necessary tests which complaints must contain under the doctrine of *LAIRD v. TATUM*. See *VVAW v. NASSAU CO. P.D., ARONSON v. GIARUSSO, VVAW v. BENECKE, HANDSCHU v. SPECIAL S.D.,*

* In most instances, only the first name of the case is mentioned. Refer to the following list of cases for the full name, cite and page number in this brief.

N.Y.C.P.D., and most recently, PHILADELPHIA, ETC. FRIENDS v. TATE.

This brief was researched and prepared by Wayne W. Schmidt, of the Supreme Court, District of Columbia, Illinois, and New Mexico Bars. Mr. Schmidt is Operating Director of AMERICANS FOR EFFECTIVE LAW ENFORCEMENT, INC., and also supervises the AELE LAW ENFORCEMENT LEGAL DEFENSE CENTER; he formerly was a supervising attorney with the International Association of Chiefs of Police (IACP). He also served as Operating Director of the Police Legal Advisor Program of Northwestern University School of Law and as Legal

Advisor to the Chicago Police Department's Bureau of Inspectional Services. He received his Master of Laws degree from Northwestern University in police legal matters, his J.D. from Oklahoma City University, a B.A. in government from the University of New Mexico, and a Diploma in English Law from the City of London College of Law in England. Research assistance was provided by Lt. Walter Jacobsen, U.S.N., who served, while on military leave, as a legal research associate with AELE. Lt. Jacobsen attended Suffolk University School of Law in Boston, and will be assigned in due course, to the Office of the Judge Advocate in the Navy Department.

INDEX OF MAJOR CASES

(Referred to in the Defense Pointers)

American Civil Liberties Union v. Westmoreland, 323 F. Supp. 1153 (N.D. Ill. 1971) Sub nom, A.C.L.U. v. Laird, 463 F. 2d 499, 500 (7th Cir. 1972), cert. den. 409 U.S. 116, 93S. Ct. 902

Aronson v. Giarusso, 436 F. 2d 955 (5th Cir. 1971)

Bagley v. City of Los Angeles Police Department, No. 71 Civ. 166 (C.D. Cal. 1971)

Bieliicki v. Superior Court, 371 P.2d 288 (Cal. 1962)

Britt v. Superior Court, 374 P.2d 817 (Cal. 1962)

Donohoe v. Duling, 330 F. Supp. 308 (E.D. Va. 1971)

Giancana v. Johnson, No. 63 C 1145 (N.D. Ill. 1963).
Sub nom Giancana v. Hoover, 322 F.2d 789 (7th Cir. 1963)

Gil v. State, 394 S.W. 2d 810 (Tex. 1965)

Handschu v. Special Services Division, 349 F. Supp. 766 (S.D.N.Y. 1972)

Hester v. United States, 265 U.S. 57 (1924)

Hoffa v. United States, 385 U.S. 293 (1966)

Holmes v. Church, 70 Civ. 5691 (S.D.N.Y. 1971)

Jenkins v. State, 248 So.2d 758 (Ala. 1971)

Johnson v. State, 234 A.2d 464 (Md. 1967)

Laird v. Tatum, 408 U.S. 1, 92 S. Ct. 2318, 33 L. Ed. 2d 154 (1972)

Lewis v. United States, 385 U.S. 208 (1966)

Local 309 U.F.W. v. Gates, 75 F. Supp. 620 (N.D. Ind. 1948)

Lykken v. Vavrek, 366 F. Supp. 585 (D. Minn. 1973)

Metros, v. District Court, 441 F.2d 313 (10th Cir. 1971)

Mitchell v. State, 170 S.E. 2d 765 (Ga. App. 1969)

Mohammed v. Sommers, 238 F. Supp. 806 (E.D. Mich. 1964)

People v. Heath, 72 Cal. Rptr. 457 (App. 1968)

People v. Young, 29 Cal. Rptr. 492 (App. 1963)

Philadelphia Yearly Meeting of the Religious Society of Friends v. Tate, 382 F. Sup. 547 (E.D. Pa. 1974)

Ponce v. Craven, 409 F.2d 621 (9th Cir. 1969)

Schultz v. Frankfort M. Accid. & P.G. Insur. Co., 139 N.W. 386 (Wis. 1913)

Smayda v. United States, 352 F.2d 251 (9th Cir. 1965)

Socialist Workers Party v. Attorney General of the United States, 95 S. Ct. 425 (1974)

State v. Penna, 241 A.2d 385 (1967)

State v. Stanton, 490 P.2d 1274 (Ore. 1971)

United States v. Lewis, 227 F. Supp. 433 (S.D.N.Y. 1964)

United States v. Wright, 449 F.2d 1355 (D.C. Cir. 1971)

Vietnam Veterans Against the War v. Benecke, 63 F.R.D. 675 (1974)

Vietnam Veterans Against the War v. Nassau County Police Department, 10 Crim. L. Rptr. 2152 (E.D.N.Y. 1971)

B. Guidelines: Types of Information That Can Be Kept in the Intelligence Unit Files

The principal point to be made is that the unit commander must be able to give a good reason for the items of information in the intelligence unit's files. The unit commander must be able to answer a court

challenge with an ability to demonstrate that any information retained in the intelligence files is pertinent and relevant to the mission of the department. Furthermore, the subject of the information either is a criminal as a result of actions and former convictions, or the person's pattern of association is clear and reasonable cause for considering him/her a potential criminal. The

validity of the filing system is further protected by having a specific program for dealing with information, the validity of which is in doubt but which is of sufficient significance that the unit commander believes it should be retained while its value and implication are investigated. Finally, the unit's standard operating procedure contains instructions for reviewing the files and purging from them information that is no longer relevant, either because of age or because after a stipulated period there have been no references to the person or the location.

Perhaps the single most important test of the relevance of information introduced into the intelligence files is that it has bearing on the mission assigned to the department. An example of this is stated in the New York City Police Guidelines, "Procedure Public Security Activities of the Intelligence Division:"

"Such information must be evaluated as bearing a substantial possibility of making a contribution to the goals of the intelligence division, to provide necessary intelligence to enable this department to perform its legitimate police service function. All information not meeting this criteria must be rejected and will not be stored in the public security card file."

Another way of stating the relevance standard is that used by the Illinois Bureau of Investigation in its "Criminal Intelligence Division Guidelines," as follows:

Information may be included in the intelligence information system when it is relevant to an organization or persons suspected of being, or having been involved in activities which violate the criminal laws of: the State of Illinois, the United States, or any jurisdiction in the United States, which would be a violation of the criminal laws of the State of Illinois. As a general guideline, a suspected person must be someone who is involved in circumstances which would arouse a reasonable suspicion of a prudent and alert police officer. If it is determined that information received is not relevant, it will be destroyed prior to entry into the system.

But not only must the information on a person or location be relevant to the mission of the department, there must be some way of judging the reliability of the information. Allegations are made for many reasons, some of which are intended only to bring harm to an innocent person. It is essential that an intelligence unit do everything possible to exclude such allegations from its data.

The best approach to the problem of reliability of information is to establish a system whereby both the

source and the information given by the source are graded. It is essential to consider both sides of the problem since a source may be highly reliable, but the particular piece of information the person is reporting on is not of the highest quality, in part, because it was passed on by a second- or third-hand source. On the other hand, the information may be accurate even though the source has no record of being a good one. Thus it is not unusual to have a report which is graded high according to the source and low according to the estimated validity of the information, or where the source is considered unreliable and the information seems valid. The intelligence division must not enter questionable information into its files. If it is deemed of sufficient value an investigator should be assigned. For lesser important items, they can be retained for a period to see if other information is received. It is assumed that in the first instance there will have been a check of the intelligence and other department files.

An example of how this problem can be addressed in guidelines is given by the Intelligence Bureau Manual of the New Jersey State Police which states:

All intelligence reports will indicate the source of information from which the data was obtained. The individual intelligence officer will evaluate the source of information as to its accuracy and validity.

Attempts will be made by the intelligence officer submitting the data to substantiate the information to other sources.

In the event the intelligence officer is unable to substantiate the data contained in the report, the individual business or corporation will be indexed on a salmon colored index card. The information contained on said report will be audited biannually by the analytical unit.

In Chapter III another approach is given to recording reliability of the source and the accuracy of the information in the report. The aim is to ensure that the reliability classification will always remain with the information whenever it is used. This is of critical importance if some months later the information is being used by new or different personnel. Without an index the data might be given a higher validity than, in fact, they should be.

One of the most difficult problems to deal with is that of information which is questionable and yet has enough potential validity to cause the intelligence unit to wish to retain the information. The approach suggested in this manual is that the unit establish a

temporary file into which such information can be placed until its validity can be determined. To make this file potentially viable in a court situation, it is imperative that the information, while in the file, should not be disseminated to anyone outside the department and if its validity has not been established in a relatively short time (such as 6 months), the information should be removed from the files and destroyed. In no case should the information in this category be introduced into and become part of the main intelligence file unless its validity is confirmed (or at least given enough support to cause the unit commander to keep it).

The Americans for Effective Law Enforcement, Inc., have reviewed some cases relevant to the material to be kept in file. They are as follows:

Suits which challenge the compilation of intelligence data can fall into two categories:

Taxpayer suits alleging the waste of governmental funds, which have been uniformly rejected, with few exceptions.

First Amendment challenges based on an alleged "chilling" effect on those whose names are retained.

As to compilation, a mere subjective "chill" or the speculative threat of future harm is not justifiable under the Civil Rights Act, 42 U.S.C. §1983.

The Supreme Court decided this rule in LAIRD v. TATUM in 1972; see also FIFTH AVENUE, ETC. v. GRAY.

State courts will not second-guess the necessity for various types of compilations if the overall purpose of the collection supports a legitimate goal of law enforcement. ANDERSON v. SILLS.

The subject matter of the files is not a justifiable basis for relief.

Possession alone of adverse or derogatory information, even if inaccurate, is not a tort. FINLEY v. HAMPTON.

The adverse and irrelevant information must be used to deny constitutionally protected, present right. IN RE LABADY.

Wide discretion is given authorities in deciding what kinds of information to collect, and its relevancy to their missions. LAIRD v. TATUM; ANDERSON v. SILLS; FIFTH AVENUE, ETC. v. GRAY; LAW STUDENTS, ETC. v. WADMOND.

(For the cases which are the source for this roundup, see the listing in the AELE material given below in the section on dissemination.)

Regardless of the validity of the information in the intelligence unit files, it must be subjected to periodic reviews to determine its relevancy to current criminal activities. No longer can information be kept in the files and saved on the basis that someday something will come up and the name will be of great use to the unit. Generally speaking, this has been more of a belief than an actuality. One entry in the files about a person years in the past can be of little assistance in a current case. This is not to say there has not been the occasional occurrence when an old item kept in the file has been of value in a current case. However, this odd occurrence does not provide defense for keeping all material entered in the files without review.

Review of information filed requires standards. One approach is that suggested by the New Jersey State Police Intelligence Manual which states:

The files of the Intelligence Bureau will be audited on an annual basis by the Analytical Unit. Any information that has not been updated in a three-year period will be purged from the master index file of the Intelligence Bureau. This information will be transferred into a suspense file wherein the intelligence officer who submitted the original report will be contacted and requested to provide an update of the information contained in the report. In the event the intelligence officer does not submit an update within a 90-day period, the report will be purged from the files of the Bureau. A record indicating the index numbers will be maintained, reflecting what report number has been deleted from the system.

The Sensitive Information File will be audited on an annual basis. The Bureau Chief will be responsible for designating a senior officer within the Intelligence Bureau to review, re-evaluate and/or eliminate any data that does not meet the criteria as established in Section II, #V-G. In the event the senior officer recommends the information contained in the Sensitive Information File *declassified*, the data will be transferred to the master-index file and the procedure as established for auditing and purging of information will be followed.

The decision to eliminate intelligence data from the indices of the Bureau will be based upon the following considerations:

- a. How often has data been requested on the subject in file?

- b. How valid is the data?
- c. Has the data been confirmed by other sources or is it unsubstantiated?
- d. Does the data meet the goals and objectives of the Bureau?
- e. Can the data be obtained from another source?
- f. How long has the data remained in file?
- g. Could the data be useful in the future?

Data will be purged from the indices of the Bureau when it has been determined by the Bureau Chief and/or his official designee that one or all of the following conditions exist:

- a. The data is no longer *relevant* or *necessary* to the goals and objectives of the Bureau.
- b. The data has become obsolete thus making it unreliable for present purposes and the utility of updating the data would be worthless.
- c. The data cannot be utilized for any present and/or future strategic or tactical intelligence studies.

In the event there is a question as to the legality of retaining any intelligence information, the Attorney General's Office will be requested to render a legal opinion.

Another approach is that adopted by the Riverside (California) Sheriff's Department:

The control of purging intelligence information of low value and erroneous data is crucial due to the sensitivity of the information. It is for this reason that a viable check and balance system be initiated in order to insure that only certain information will be purged in accordance with the criteria established herein and that an accurate record is maintained which is easily retrievable.

No file will be purged unless *all* of elements 4, 5, and 6 are present, along with one or more elements of 1, 2, or 3.

Elements

- 1. No criminal background

- 2. No association with a known organized crime figure, outlaw motorcycle, military or subversive groups
- 3. No file entry for five years from the last file entry
- 4. Recommendation for purging by an investigator
- 5. Approval for purging by supervisor
- 6. Approval of purging by Chief Deputy

If *all* elements for purging are met, the information to be purged will be destroyed in a paper shredder to insure positive destruction.

The 5x8 card initiated when subject's name was entered into file will *always* be maintained and appropriate entry on that card indicating the date and initials of persons approving the purging will be so recorded.

All intelligence files will be reviewed annually by an investigator of the Special Investigations Unit of the Riverside Sheriff's Department and he will make recommendations to determine if and/or what files will be purged.

It is recommended that guidelines on purging include the following:

- A definition of information that is no longer relevant.
- A stated time period for file review.
- An order that purged material should be destroyed so it does not fall into the wrong hands. An exception to this would be material appropriate to a case in which event the information could be sealed and put in storage files.
- A decision as to whether a listing of destroyed material should be kept with the name of the person so ordering. This will probably be a matter of statute or court decision so the intelligence unit should research the matter.

C. Guidelines Controlling Dissemination Outside the Department

The most pointed focus on the operation of police department intelligence units by courts and legislatures is captured by the questions, "Who gets access to the information contained in the police department's intelligence files?" and "To whom is the information disseminated?" Police intelligence units themselves have

long recognized this as the critical issue. Some have tried to minimize the potential difficulty by sharply restricting distribution. Others have relied on the personal approach, circulating information only to known and trusted persons. The Law Enforcement Intelligence Unit approach is primarily based on this latter concept. The pressure to disseminate is a product of the belief that information on criminal activity that remains in the files and is not used is worthless. It is not worth the effort of gathering it and putting it into the files in the first place.

Specific rules governing dissemination are essential. One approach, in terms of guidelines, is that taken by the New Jersey State Police in its intelligence manual which states:

In order to protect the constitutional rights of those persons contained in the files of the New Jersey State Police Intelligence Bureau, strict controls will be maintained in the dissemination of information contained in said files. The following procedure has been established for the dissemination of intelligence data:

1. **General Rules and Regulations** - All members of the division shall treat as confidential the business of the division. They shall not impart information regarding departmental business to anyone except for whom it is intended, or as may be directed by the Superintendent, or under due process of law. They shall not talk for publication, not be interviewed, nor make public speeches on police business except by permission of the Superintendent.
2. All requests for intelligence data will be entered on the subject's index card. The entry should reflect the agency making the request and the date of request. This procedure will facilitate the determination on whether to purge any information and to assist in coordinating investigative efforts.
3. Prior to the dissemination of any intelligence data, the Bureau Chief will consider the following:
 - a. the accuracy and reliability of the data
 - b. whether the dissemination of the data can compromise the identity of a source of information
 - c. the type of information being requested, i.e., criminal history, general intelligence data, and so forth
 - d. the requester's right and need to know

Guidelines state and give the procedures whereby information can be distributed within the State Police and other law enforcement agencies, but state specifically, "that information contained in the files of the New Jersey State Police Intelligence Bureau will not be disseminated, formally or informally, to any non-law enforcement agency or individual."

Another set of guidelines have been developed by the Illinois Bureau of Investigation, as follows:

Extra-Bureau Dissemination

- Intelligence information will be disseminated only to specifically designated representatives of law enforcement agencies and to those state, Federal, municipal, and local governmental agencies who can demonstrate a definite need to know. Information which does not bear a substantial relationship to the legitimate responsibilities of the requesting agency will in no instance be disseminated from the Intelligence files.
- Requests for information will be submitted in writing on the form designated by the Special Agent-in-Charge, Intelligence Division.
- Prior to dissemination of information in the Intelligence files, all of the following factors must be evaluated and analyzed:
 - a. nature of the information requested - criminal record, raw intelligence, etc.
 - b. source of the information.
 - c. classification of the information.
 - d. agency requesting the information.
 - e. reason for the request - i.e., the use the requesting agency will make of the information, e.g., investigation, prosecution of a serious criminal nature.

These and all other relevant factors must be considered in arriving at a determination concerning the possible dissemination of information in the Intelligence files and the type and amount of such information to be disseminated. The evaluation of these factors will determine the requesting agency's need to know. The initial determination will be made by the Information Control Officer, subject to review by the Special Agent-in-Charge, Intelligence Division, or the Superintendent.

- Information contained in the Intelligence files will be transmitted in writing to governmental and law enforcement agencies over the signature of the Special Agent-in-Charge, Intelligence Division or the Superintendent.
- When tactical urgency and time demands preclude written requests for information from Intelligence files or written replies thereto, telephone requests for such information will be honored, if made by properly authorized agency representatives of those approved agencies. Extra-Bureau dissemination criteria will still apply.

To ensure the legitimacy of the request and to preclude unauthorized dissemination of Intelligence information, the following procedures are to be followed:

- a. Telephone call will be made by the recipient of the request to the requesting agency to verify the authenticity of the caller and the request.
 - b. During the normal business hours, the senior analyst or Intelligence liaison agent will evaluate the request and approve same if appropriate. During other hours, the Intelligence Staff Duty Officer will handle urgent telephone requests.
 - c. A record of the request and of the information dissemination (if any) will be made in the appropriate Intelligence file.
 - d. In all cases, the Superintendent, the Special Agent-in-Charge, or the Senior Analyst, Intelligence Division, are to be notified of the request and disposition.
- Information disseminated under these procedures will have the following restrictive statement, prominently stamped on the cover letter or read to the requesting party:

“THE INFORMATION FURNISHED IS DISSEMINATED PURSUANT TO THE INTELLIGENCE DIVISION PROCEDURES OF THE ILLINOIS BUREAU OF INVESTIGATION AND IS THE PROPERTY OF THAT BUREAU. CONTENTS MAY NOT BE DISCLOSED TO ANY PERSON OR ORGANIZATION EXCEPT WITH THE EXPRESS PERMISSION OF THE SPECIAL AGENT-IN-CHARGE, INTELLIGENCE DIVISION, OR THE SUPERINTENDENT, ILLINOIS BUREAU OF INVESTIGATION.”

The Americans for Effective Law Enforcement also has some cases showing trends in this area, as follows:

Law enforcement agencies may freely exchange intelligence data among themselves.

Dissemination is appropriate if the recipient agency has a potential use for the information. LAIRD v. TATUM; FIFTH AVENUE, ETC. v. GRAY; ANDERSON v. SILLS.

Expungement orders do not affect raw intelligence files or their dissemination, unless they are directly related to the expunged arrest or are mentioned in the order itself (or the statute on which they may be based).

Dissemination of arrest and conviction records must conform to the requirements of recently promulgated LEAA regulations.

A state or Federal statute, court order or rule, or executive order of the governor is necessary to authorize dissemination of criminal history data to non-criminal justice agencies, private organizations, and individuals.

Enforcement of this section is by fine and cut-off of funds.

Dissemination of raw intelligence data to public agencies, private organizations, and individuals is not illegal.

LEAA regulations do not cover intelligence information.

Release of derogatory data in police files is not per se an invasion of privacy. See VOLKER, KOLB and PURDY cases as to adverse effects of retention.

Complicity in violation of 28 U.S.C. §2000 (e), the Equal Employment Opportunity Act, is a probable exception to this rule.

Dissemination of derogatory data about an individual or group, if untrue, could subject the offending officer to civil damages.

The usual rules relating to libel and slander cases would apply.

Exchange of information among law enforcement agencies is PRIVILEGED. See LAIRD v. TATUM, ANDERSON v. SILLS, and FIFTH AVENUE v. GRAY.

The Civil Rights Acts do not permit recovery for either libelous or slanderous conduct. MOREY v. INDEPENDENT SCHOOL DIST., 312 F. Supp. 1257, 1262, aff'd 429 F. 2d 428 (Minn., 8th Cir. 1969); JERVEY v. MARTIN, 336 F. Supp. 1350,

1354 (D. Va. 1972); MAYBERRY v. MARONERY, 337 F. Supp. 601 (d. Pa. 1971).

The Federal courts will not entertain a suit challenging public disclosure of intelligence data, because of its lack of justiciability. PHILADELPHIA YEARLY MEETING, ETC. v. TATE.

A suit charging wrongful expenditure of funds does not state a cause of action under §1983. OTTO v. SOMERS, 332 F. 2d 697, cert. den. 379 U.S. 1002; LOVE v. NAVARRO, 262 F. Supp. 520 (D. Cal. 1967).

CASES

Alliance to end Repression v. Rochford, No. 74 C. 3268 (N.D. Ill.)

Anderson v. Sills, 256 A. 2d 298, 265 A. 2d 678 (N.J. 1970)

Baker v. Howard, 419 F. 2d 376, (9th Cir. 1969)

Carter v. Gallagher, 452 F. 2d 180 (D.C. Cir. 1972)

Fifth Avenue Peace Parade Committee v. Gray, 480 F. 2d 326 (2d Cir. 1973)

Finley v. Hampton, 473 F. 2d 180 (D.C. Cir. 1972)

Greater Houston Chapter, American Civil Liberties Union v. Welch, Civ. No. 75-H-59 (S.D. Tex)

Gregory v. Litton Systems, Inc., 316 F. Supp. 401 (C.D. Cal. 1970), mod. 472 F. 2d 631 (9th Cir. 1972)

Herschel v. Dyra, 365 F. 2d 17 (7th Cir. 1967)

In re Labady, 326 F. Supp. 924 (S.D. N.Y. 1971)

Kolb v. O'Connor, 142 N.E. 2d 818 (Ill. App. 1957)

Laird v. Tatum, 408 U.S. 1, (1972)

Law Students Civil Rights Commission v. Wadmond, 401 U.S. 154 (1971)

Menard v. Mitchell, 430 F. 2d 486, mod. sub. nom.

Menard v. Saxbe, 498 F. 2d 1019 (D.C. Cir. 1974)

Purdy v. Mulkey, 228 So. 2d 132 (Fla. App. 1969)

Voelker v. Tyndall, 75 N.E. 2d 548 (Ind. 1974)

Walker v. Lamb, 254 A. 2d 265 aff'd. 259 A. 2d 663 (Del. 1969)

The above examples pose several difficult decision points for the police department. These include policies on dissemination to non-law enforcement agencies, what is meant by right-to-know and need-to-know, and how an agency can insure that recipients of its material will treat it properly.

With regard to the issue of dissemination to a non-law enforcement agency, Wayne A. Kerstetter, Superintendent of the Illinois Bureau of Investigation, says,

"There is a difficult public policy issue regarding dissemination to non-law enforcement governmental agencies. These agencies often have a clear and

articulable interest in obtaining files in order to discharge their organizational mission. For example, an agency contemplating awarding a grant to, or entering a contract with a person or business, has a clear interest in knowing whether that person or business has a history of being involved in schemes to defraud the government. The information contained in the intelligence files may well reflect, not convictions, but patterns of association from which reasonable inferences of involvement can be drawn."¹

This poses a very difficult dilemma, for if the information is not disseminated, a potential criminal may get a contract. On the other hand, if it is disseminated to a non-law enforcement agency, it may be deemed inappropriate or illegal by a court and thus struck down with an award made against the intelligence unit for having passed the information. Further consideration of this issue will undoubtedly occur in the courts and the various state and Federal legislatures. Intelligence units should keep aware of developments especially if they disseminate to non-law enforcement agencies.

It is ordinarily accepted that a law enforcement agency has a right to know about a criminal or alleged criminal activities in other jurisdictions. But this fact should not be enough. The agency requesting the information should want it for a reason—a case under consideration. This is need-to-know. Considerable discussion has been aroused by the phrase "need-to-know." What it means literally is the person requesting the

¹Wayne A. Kerstetter and Lewis M. Nixon, III, Special Agent Illinois Bureau of Investigation, *Police Intelligence Guidelines: A Response to Legal and Legislative Challenges*, given at the National Organized Crime Conference, Washington, D.C., October 1975.

information is involved in a case, an investigation, in which he/she believes information on the particular person or location is relevant to his/her activity. It is difficult for a person not involved in the investigation to determine the correctness of the asserted "need-to-know." Thus, generally speaking, the need-to-know must be taken on the word of the officer engaged in the investigation and the important element would be the fact that he/she has a right to know, based on his/her being a law enforcement officer.

Finally, there is the problem of how a recipient agency treats the information received. In the approaches of both the New Jersey State Police and the Illinois Bureau of Investigation, there is an effort to require the recipient not to transfer the information to another agency.

In the manual above, it has been suggested in several places that the agency disseminating the information take steps to cover itself by insuring that the receiving agencies understand the sensitivity of the information they are receiving and the manner in which the originating agency wishes the information to be handled. The originating agency should make it clear to the recipients of its dissemination that agencies failing to observe its guidelines will be stricken from the dissemination list. While this may seem overly harsh, it should be kept in mind that improper use of intelligence information can lead to very harmful impacts on a department's intelligence files. The trail from the agency or person misusing the information can be followed directly back to the unit from which the information was obtained and can be the beginning of a discovery action.

APPENDIX B
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 toward 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 meeting 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 questions might be started. They are drawn from a list prepared by Vincent Piersante and William Dunham for the Organized Crime Division, Attorney General's Office, State of Michigan.

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 hangouts for known racketeers that are regularly frequented by public officials or police officers?
5. Do you know any payoff persons?
6. Do you know 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 bookmaking operations?
4. Do you know the names of these 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 (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 that uses a wire communication facility including telephones?
13. Do you know any layoff persons or set ups?

HIJACKING

1. Do you have any information about any hijacking operation?
2. Do you know of any thefts from intra- 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) Aircrafts
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 that may develop information of 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 of employees and remittance to a union without written authorization from employees concerned
3. Employer payment of dues from the employer's own assets, that is, dues not checked off from employer's wages subject to written authorization
4. Union officials with direct or hidden interests in companies employing members of that union or in companies that 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 scales
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. Non-working 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" person?
 - 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 business?
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. Failing 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 affected or tried to affect 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 person and owned by a racketeer?

12. Do you know of any mob-connected taverns that 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 victim?

2. If so,

a. Who is the loan shark?

b. Who does the person 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 or implied? (By whom?)

h. What is the background of suspects, their vehicles, and so forth?

i. Do you know of any musclemen or collectors for loan sharks?

MAFIA-COSTA 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 that 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 specialties

e. Familial connections

f. Criminal associates

g. Police and public official connections

5. Describe his/her organizational activities.

6. Does he/she have an in-state or an out-of-state residence?

a. How often is it used?

b. What means of travel does this person ordinarily use?

(1) In-town

(2) In-state and out-of-state

(3) Travel agency

(4) Visits Canada (give details)

7. Does he/she own an airplane or a boat?

8. Does he/she 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 muscleman?

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, marijuana, 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. Is the subject's manner of sale and delivery

a. Hand to hand?

b. By a front person?

c. By telephone in the transaction?

d. Subject as a middleperson?

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 the supply of narcotics?

13. Obtain from the source any information relative to subject's description, vehicle, residence, telephone number, and so forth.

14. Are you aware of any members of 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 persons
4. Who are the people who handle the 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?
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 C

OPERATIONAL PROCEDURES FOR AN INTELLIGENCE INFORMATION CONTROL AND FILING SYSTEM

A. The Role of Information Control

All intelligence reports, from whatever source, should come through an information control where they are given an accession or control number, logged in, and circulated to a person in the intelligence unit responsible for reviewing the document.

1. **The Accession or Control Number.** An essential element of the filing system suggested here is that an accession number be given to all documents entering into the information control. By accession is meant that new information is being entered into the system. The accession number is the key to the indexing, filing, retrieving, and control of dissemination of information in the file system.

- The accession number serves several purposes simultaneously. It gives a serial number for filing purposes and forms the basis for indices telling about the source and substance of the material.

- An accession number system can be constructed as follows:

yy snsnsn sss xx rr ccc

in which:

yy - two digits to give the year. This assists in purging operations. The month and day are not necessary since a record should be kept of the series of accession numbers issued each day.

snsnsn - six digits are shown here. The number used depends on the estimated flow of documents in a year period. The serial numbering restarts at the beginning of each year.

sss - three digits for indicating the source of the report. The index system should include the several elements in the intelligence unit, other units in the department, and other agencies—local, state, and Federal—from whom information is received. Different elements within the intelligence unit are indicated since it is suggested that all analytic reports should also be indexed into the file system. These would be in addition to the normal flow of reports from intelligence unit investigators.

xx - two digits are reserved to record the sensitivity classification given to the information by the originator. It is essential that this information ac-

company indexing of the information so that its future dissemination can be controlled.

ccc - the last three digits are optional. If the file system does not call for abstracting and indexing by category of criminal activity, then this number can be added to the accession number to show the principal criminal activity (or the principal criminal activities) mentioned in the report.

- Part of the accession number can be handled by a stamp that automatically rotates after each use. This takes care of the “yy snsnsn” digits. The balance must be added by hand or by individual stamps.

2. **Logging.** Logging is a recording device. It should be kept to a minimum.

- In the simplest method, if the accession numbering approach is used, the clerk merely writes down the accession numbers issued each day.

Ordinarily, much of the information flow into an intelligence unit is normal agent reporting. There is no need to log it separately since a record will be made by the supervisor.

- Another important reason for logging the accession numbers issued each day is to produce information on the volume and source of reporting.

The total flow of reports per day, per week, and per month establish a basis for determining the size of staff required. Moreover, these records will show the extent to which any element of the department or another agency is furnishing reports to the intelligence unit. This can be used by the liaison staff to check on the extent to which agencies are sharing their information.

- A unit may wish to keep track of special, unique reports.

3. **Distribution.** In most cases, intelligence reports will be sent directly from Information Control to an analyst's desk.

- The unit commander, with assistance from the analyst, will develop a method for indicating to Information Control how the material is to be circulated.

- This direct flow will minimize the administrative work in the analysis section and ensure that the flow of reports is not held up by accumulation on a supervisor's desk.

B. Indexing

It is suggested that the analyst have the responsibility to determine the disposition of all intelligence reports received in the intelligence unit. The files are the analyst's most important tool. He/she should have the responsibility for what goes in them and how it can be retrieved. When there is no analyst, an investigator, a file clerk, or in some cases, a supervisor should handle this task.

The analyst will determine which reports are to be saved and which are of no value. He/she will determine how the material is to be indexed. These responsibilities will help the analyst to become the most knowledgeable person in the department in his/her assigned field. However, the guidelines for analyst activities should be set by the unit commander. The supervisor is more knowledgeable of the concerns of the department than is the analyst and can best insure that the files are useful to the department as a whole.

The analyst receiving a report from Information Control will read the report.

- If the information is useful and the persons named are known criminals or the allegations are from a reliable source or in keeping with other reports, the analyst should mark it for indexing (see below).

- If the information is valueless, it should be so marked and returned to Information Control so that the accession numbers issued can be cancelled. This provides a general record of reports destroyed, at least in terms of originating agencies or elements. This information can assist the unit commander in efforts to record and/or improve the quality of information received.

- If the validity of the information on a person is questionable, the analyst has two choices. If he/she knows or believes, on the basis of knowledge of criminals in his/her area and their activities, that the information is of little value or is too difficult to verify, then it may be classified as worthless and sent back to be destroyed.

On the other hand, if the analyst has some basis to believe the allegation has some merit, he/she may decide to retain it. But since the validity is in doubt, the analyst will mark the information to be filed in the *temporary file*. As discussed in Chapter III, information so filed should:

- Not be disseminated outside the department
- Be held for no more than a stipulated period of time (6 months) unless it can be verified by investigation of subsequent reports
- Not be indexed in any way into the main file until its validity has been resolved.

- Be sent through Information Control for cancelling its accession number and destruction if it is not verified in the stipulated period.

- Be indexed into the main file if it is verified.

- In all cases discussed above, if the report has information relative to more than one analyst's area of interest, the analyst to receive the report first has the responsibility to circulate it to other appropriate analysts. This rule must be followed even though the first analyst decided the report was of questionable or little value.

All analysts that read a single report have a collective responsibility to indicate how the file staff is to index and file it (see suggested file forms to be used below). Specifically, the analysts must

- underline all names and locations to be indexed
- state specifically the criminal activity to be indexed, giving the category and subcategory(s). (This is important as a future aid to the analyst using the information in the files.)

- prepare a brief abstract of the report giving names, addresses, and what happened. This is the key to cross-indexing between criminal activities, criminals, and locations.

The abstract can be used on three forms. The criminal activities index is its primary use. But where there is a Biographic Key Data form on one or more persons referred to in the report, the abstract can be used to record this fact on the backup (Form B-1) to the Biographic. Similarly, the same abstract can be used with the Location Key Data file.

- Request that a Biographic Key Data form (Form B) be initiated on a person in the report if the analyst feels it necessary.

- Request a Location Key Data form (Form L) be initiated on an address in the report if the analyst feels it necessary.

Where there is a large flow of reports, of which only a few are normally retained or where the disposition of categories of the reports can readily be predetermined, the analyst can share this responsibility with a file clerk. The analyst should remain responsible for the review of reports by the file clerk.

The analyst will be responsible on the basis of the flow of intelligence reports to perform certain other functions:

- bringing to the attention of the unit commander reports that contain information that appears to be of importance.

- developing collection requirements to be forwarded to the investigative staffs of the other elements, in the department and outside, that can assist

in filling information gaps. If the unit has adopted the collection plan approach, these requirements will be submitted as requested under the plan.

- developing a system for answering requests for assistance from other elements of the unit, other units of the department, and other law enforcement agencies. The system should furnish as much information as possible so long as the sensitive status of the material is not violated and no files are given to unauthorized persons.

At the same time, the process for answering requests for tactical assistance should emphasize speed and accuracy of reply. If there is to be a liaison effort to emphasize exchange of information, straight talk is essential. It should also take legal guidelines for what information can be exchanged into account.

C. The Operation of the File Room Staff

The file room staff will be responsible for establishing and maintaining the file system approved by the unit commander. The staff will promptly index and file all reports sent by the analysts. In so doing, the instruction of the analysts must be carefully followed.

The suggested basic index categories to be included in the file system are as follows:

Name File	Form NF
Location File	Form LF
Biographic Key Data	Form B
Sources Biographic Key Data	Form B-1
Location Key Data	Form L
Criminal Activity Key Data	Form CA

The files of these several forms should be such that they are readily accessible for making additional entries. All material on these forms should be typed. The analysts may also request that other index files be established including: aliases, license numbers, and telephone numbers. However, the alias index file can be part of the name file with the alias cards filed alphabetically. It is suggested that the intelligence information reports, once indexed, be filed serially, based on the accession number. Some form of separation into groups of 100 will assist in future retrieval.

A temporary file should be established. It will consist of reports on persons about whom there is no other information in the main file and the investigator has indicated serious reservations on the report about the accuracy of the source on this particular subject. The reports should be filed alphabetically according to the name of the subject in question. Where a single report has more than one subject, some are known criminals, and one or more fit the category described for the temporary file, it should be dealt with as follows:

- The names considered valid should be indexed in the normal manner in the main file and the report itself filed in the main file.

- The report should be marked in some manner (clip, color pin, and so forth) to indicate that one or more names referred to must be treated in the manner prescribed for those in the temporary file. The names themselves can actually be circled in pencil or indicated in some other manner.

- A reference to the basic report should be placed in the temporary file in the appropriate alphabetical order of the name of the subject in question. If there is more than one, each name should be so referenced.

The decision on the disposition of material in the temporary file is a responsibility of the analyst. If the analyst has taken no action by the expiration of the holding period, the file clerk will retrieve the material from the file and give it to the analyst for review. It is the file room's responsibility to review the temporary file regularly to determine if any material has reached the expiration date. Final disposition of material in the temporary file will be dealt with as follows:

- If the information in question is not confirmed within the holding period, following analyst review, the report plus any index card referring to the material should be destroyed. No record should be kept, since at this point the unit must act as though the material never existed.

- Where the information is confirmed, the report should be indexed as indicated. (It will have to be sent back to the analyst if he/she did not mark the report when it was initially reviewed.)

As reports are received, the file room staff will treat them in the following manner:

- With respect to all names underlined on a report, the file clerk will first check to see if any have a Form B, Biographic Key Data. If so, the report will be indexed to it, as contributing information to Form B directly, and thus be indexed on a Form B-1. (See suggested attached forms.)

- If there is no Form B, the file clerk will index the name on a Form NF, Name File. When filing the Form NF, the clerk should check to see if other form NF's have been made out on the person. If there is a number, the clerk should call this fact to the attention of the supervisor or the analyst. The accumulation of these forms may indicate that an important new criminal is emerging and a Form B is needed.

- The file clerk will check the addresses underlined against the Location Key Data File (Form L). If a form has not been initiated, then the file clerk will fill out a Form LF, the Location File index. He/she should check to see if other Form LF's have been filed against

the address. If there are several, it should be called to the attention of the supervisor or the analyst.

- Finally, the file clerk will index the report to the Criminal Activity File (Form CA) if so directed by the analyst. If in the filing of the new material the clerk sees several other reports of a similar nature (or other suggestive correlations), he/she should call this to the attention of the supervisor or the analyst.

- If the report is marked for the Temporary File, the file clerk will handle the material as previously discussed.

- The file room staff will make up and keep current a loose-leaf notebook for each analyst (or for several analysts in a single room) containing xerox copies of the material in the index files on Forms B, B-1, L, and

CA. These are for the analysts' use when reviewing current material.

The supervisor of the file room staff will be responsible for certain other activities:

- developing a control system for the file room so no one but members of the staff or the analyst section is permitted entry and no one but the staff has access to the files.

- developing a system whereby analysts will be assisted in keeping track of gaps in intelligence information, especially in terms of Biographic Key Data and Location Key Data.

- taking the initiative to develop a system for purging the files of old and irrelevant material.

Form NF

Last Name First Middle

Address

I.D. No. DOB

Nickname/Alias

Activity:

Accession Number

Date of Activity in Report
month/day/year

Form LF

ADDRESS Street Number

Type of Premise

Precinct

Activity:

Accession Number

Date of Activity in Report
month/day/year

See: L Form
B Form

BIOGRAPHIC KEY DATA

- (1) NAME:
- (2) ALIASES:
- (3) DESCRIPTION: PICTURE
SEX: COLOR:
DOB: POB:
HGT: WGT:
EYES: HAIR:
OTHER:
- (4)
- (5) POLICE I.D. NO:
E# OTHER:
B#
KG#
FBI#
NYSIIS#
- (6) NON CRIMINAL I.D. NO'S:
SOCIAL SECURITY #:
DRIVERS LIC. #:
TYPE: EXPIRES: STATUS:
OTHER:
- (7) RESIDENCE:
PRESENT: SINCE: PCT.
TYPE:
- TELEPHONE NUMBER & SUBSCRIBER:
SUMMER/WINTER:
TELEPHONE NUMBER & SUBSCRIBER:
- (8) AUTOMOBILES:
PLATES: REGISTERED OWNER: TYPE/COLOR/MAKE:
1. EXP.
2. EXP.
3. EXP.

(9)

(This form should be on heavy paper, such as banks use for keeping accounts. It should always be kept up-to-date by using white-out and typing in new information. Deleted material should be noted on Form B-1.)

(10) ASSOCIATES:

(11) HANGOUTS:

PCT:

(12) PRINCIPAL CRIMINAL ACTIVITIES:

KNOWN:

SUSPECTED:

(13) BUSINESS/EMPLOYMENT:

ADDRESS:

(14) FAMILY:

FATHER:

MOTHER:

WIFE:

CHILDREN:

OTHER:

BROTHERS:

SISTERS:

(15) NON FAMILY:

GIRLFRIEND:

ADDRESS:

CHILDREN VIA THIS UNION:

(16) PREVIOUS RESIDENCES:

(17) SENSITIVE AREA:

1. BANK(S):
2. ACCOUNTANT(S):
3. LAWYER(S)
4. DOCTOR(S):

(18) EDUCATION:

(19) MEDICAL HISTORY:

(20) BACKGROUND & MISCELLANEOUS INFORMATION:

FORM B-1

INDEX - SOURCES OF BIOGRAPHIC KEY DATA

Key Data Item Number	Revision Original Key Data (mark with x)	Data of Activity in Report	Accession Number	Brief Abstract Subject Source Report

FORM - L

LOCATION KEY DATA

Name of establishment (if any) _____

Address _____ District or Precinct _____
(Street) (Number)

Actual or ostensible business conducted at address _____ Telephone Number _____

Owner of property/building _____

Leasor of property/building _____

Accession Number	Date of Activity in Report	Subject Source Report

FORM CA

CRIMINAL ACTIVITY KEY DATA

Category Group _____

Subcategory _____

Accession Number	Date of Activity in Report	Subject Source Report (to include as appropriate complainant, names, address, mode of operation, etc.)

EXAMPLES OF CATEGORIES AND SUBCATEGORIES
OF CRIMINAL ACTIVITIES

<u>Category</u>	<u>Subcategory</u>	<u>Subcategory</u>
BOMBS/BOMBING		
CORRUPTION	Attempted Bribery Policy Public Officials	
COUNTERFEITING		
CRIMINAL ACTIVITY BY SELECTED AREAS	Chinatown Area Fulton Market Area	
EXTORTION		
FRAUD	General Bankruptcy Checks Credit Cards Insurance Property Welfare	

<u>Category</u>	<u>Subcategory</u>	<u>Subcategory</u>
GAMBLING	Cards	
	Dice	
	Horses	
	Policy	General
		Cuban
		Chinese
	Sports	
GANGS	Chinese Youth Gangs	
HOMICIDE	Militants Against Police	
	Organized Crime Members	
	Other Major Criminals	
KIDNAPPING	Organized Crime Members	
	Other Major Criminals	
NARCOTICS	General	
	Major Violators	
		Heroin
		Cocaine
		Barbituates
		Other
ORGANIZED CRIME FAMILIES/GROUPS	General	
	Luchase	
	Bonanno	
	Gallo	
	Gambino	
	Colombo	
PORNOGRAPHY		

<u>Category</u>	<u>Subcategory</u>	<u>Subcategory</u>
PROSTITUTION		
RECEIVING/POSSESSION STOLEN PROPERTY		
SHYLOCKING		
THEFT/HIJACKING	Autos/Major Rings Goods in Transit Heavy Building Machinery Securities Warehouses	Electronics Meat Electronics

APPENDIX D.

THE COMPUTER AND THE INTELLIGENCE UNIT

A. 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 and reviews the various uses of a computer, namely, information storage and retrieval, collation, and analysis. This appendix does *not* attempt to develop or to suggest programs nor to probe the technical attributes of computers. It does emphasize the need for thorough and detailed planning of the manner of output desired before programming is initiated.

There is no doubt that when the intelligence process is computerized the intelligence unit will become more efficient. But this will induce a cost. Resource planning and allocation must take into account a series of expenditures, including:

- An initial cost-effectiveness study to determine the advantages expected to accrue to the unit.
- The development of the "software" or programs to determine how the intelligence information will be available.
- The large task of reviewing existing files to determine which ones and what content of each should be put into the computer's data bank.
- The development of computer-related information report forms.
- Operational costs which will include:
 - A proportionate share of the cost of the computer.
 - A share of the cost of the computer personnel, including:
 - computer operators
 - programmers (contract or hire - to refine and update programs through time to keep abreast of changing circumstances)
 - punch card operators or typists to input data as they become available

This appendix offers little assistance in giving guidelines for these cost analyses and only a small amount has been published that will guide such calculations. They 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 focuses on the computer because the authors believe that it offers the most flexible and, hence, the most effective system in the long run. Whatever approach is adopted, it is recommended that, from the first step, arrangements be made for eventual conversion to a computer. This applies to the indexing systems adopted, the data input forms, and, in particular, to developing information element codes.

For those concerned that the computer will 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 entered and the instructions given to it through the programs that tell it what to do with the information in its storage tapes or discs. The computer cannot require that additional information be collected, nor can it make its own analyses. Its output can only show gaps in the data bank and its programmed collation can only assist analysis. But past experience certainly indicates that the presence of the computer, once its capabilities are appreciated, will press the unit to gather more information and to make the reporting compatible with the input programs.

B. Conditions Favorable to Conversion to the Computer

Two major criteria should be kept in mind when considering the possibility of computerizing the intelligence unit:

- The availability of a secure computer
- The level of existing or potential organized crime activity and the volume of information on it

1. **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 Appendix E for a discussion of the problems of security, particularly 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 are discussed below.

2. **Volume of Data to be Handled.** By themselves, the information storage and data handling requirements of most, if not all, intelligence units do not seem large enough by themselves to support a computer operation. However, if an agency has already acquired a computer or is planning to do so for handling the general files and controlling its patrol forces, there should be active planning to get a "piece of the action" for the intelligence unit.

However, before the conversion exercise is executed, the intelligence unit commander should determine the amount of information received by the unit and how efficiently it could be handled with improved manual techniques. As part of the analysis the commander should project the potential volume of information flow. The changeover from a hand-operated system to a computerized one is relatively costly. 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 cut-off date from which point all information will be collected in a format compatible with the computer while retaining and using the old files in their hard-copy form. A compromise approach would be to combine the cut-off date with a review of old stored information as new cases develop. Where data from the old files are relevant, they could be put into the computer.

One point to keep 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 below.

C. 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 the operation of the unit with a computer will have to be much more sophisticated 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 searching for patterns and 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 requests to produce "interesting" but not very useful sets of figures and correlations.

1. **Collection - Information Flow.** The computer will help the unit 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 the most recent information (tactical intelligence) and have it collated with filed information without pulling a series of hard-copy reports and performing a time-consuming hand collation. Similarly the analyst can obtain the assistance of the computer in day-by-day efforts to correlate bits of information and develop patterns of activities of organized criminals (strategic intelligence).

One decision that will have to be made is whether the totality of the remarks in a report will be inserted in the computer, be abstracted, or only 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, punch card operator availability, potential developments in the organized crime threat, and so forth. 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 III for a discussion of this problem.) Unless this is done, there will be no way to separate sensitive from non-sensitive material when printouts are made of data in the computer. Since each element of intelligence information does not have the same degree of sensitivity, it will be essential to have some system of classification 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 substance and that this evaluation be coded and attached to the data location. Once data are inserted into the computer, it is time-consuming to recall and develop an evaluation. But they must be evaluated either before or after; otherwise, when printed out, all data will appear to have equal validity.

2. **Collation.** The computer adds many dimensions to the collation potential. By coding the information as it is filed, it can be associated with other information of a similar nature and, through programming, associated with other types of information to present aggregations that can subsequently be used to develop patterns, associations, and trends.

The most important area of improvement will be in cross-indexing. A single report from an investigation that contains information on several different persons, locations, and activities can be broken up and entered in a manner that associates them with others of a similar nature. The names and locations can be checked to see if they are already on file. 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. Furthermore, the information can be obtained from the computer by requesting the name of the person, the activity, or the location. It should also be noted that use of a computer eliminates the danger that someone will inadvertently walk off with a hard copy of a report and thus create a gap in the files.

Of course all of the above will not happen automatically. A program must be written that will file the inputs in their correct location and be able to retrieve them, either as a unique piece of data or in proper association with similar or associated data. The unit must obtain the service of a programmer as a new permanent employee, train one of its own men, or turn to a computer software company on a contract basis. Programming and file maintenance are not a one-time operation. As information begins to accumulate on a new area it may have some significance for other files already in the computer. The programmer must understand the problem and develop the requisite instructions for the computer so that it will associate the new and old file information and give it back in a format useful to the analysts and investigators.

3. **Analysis.** The computer can also offer great assistance to the analyst. Through programming and 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 laboriously (and may in fact overlook).

In particular, the computerized files will help develop 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, and so forth. Figure 1 depicts a hypothetical file on hijacking that is designed as an example of a data base that can be constructed and 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 by 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 1 attempts to demonstrate the scope of information that can and should be available to the analyst in an area of organized criminal activity. It also shows how, through programming, the basic data can be organized. The elements shown in CAPITAL letters on the first page of the figure are, in a direct sense, the totals and subtotals. 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), the *modus operandi* used, the value, and so forth. This is the raw material for developing hypotheses on how a particular group of criminals is operating and may indicate new areas where the group may attempt its next strike.

The information on the right-hand side of the second and third pages of the figure is the input data. It would be highly desirable if the unit developed formatted pages to be used by the investigator or debriefer. These pages would list the questions to be asked and would insure that the subject was covered and the desired information obtained. The questions themselves could be coded on the form that would 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/her probing of 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.

4. **Security.** Computer security means protecting the data file against access by unauthorized persons and 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

FIGURE 1
EXAMPLE-SUMMARY PRINTOUT CATEGORIES AND INPUT INFORMATION

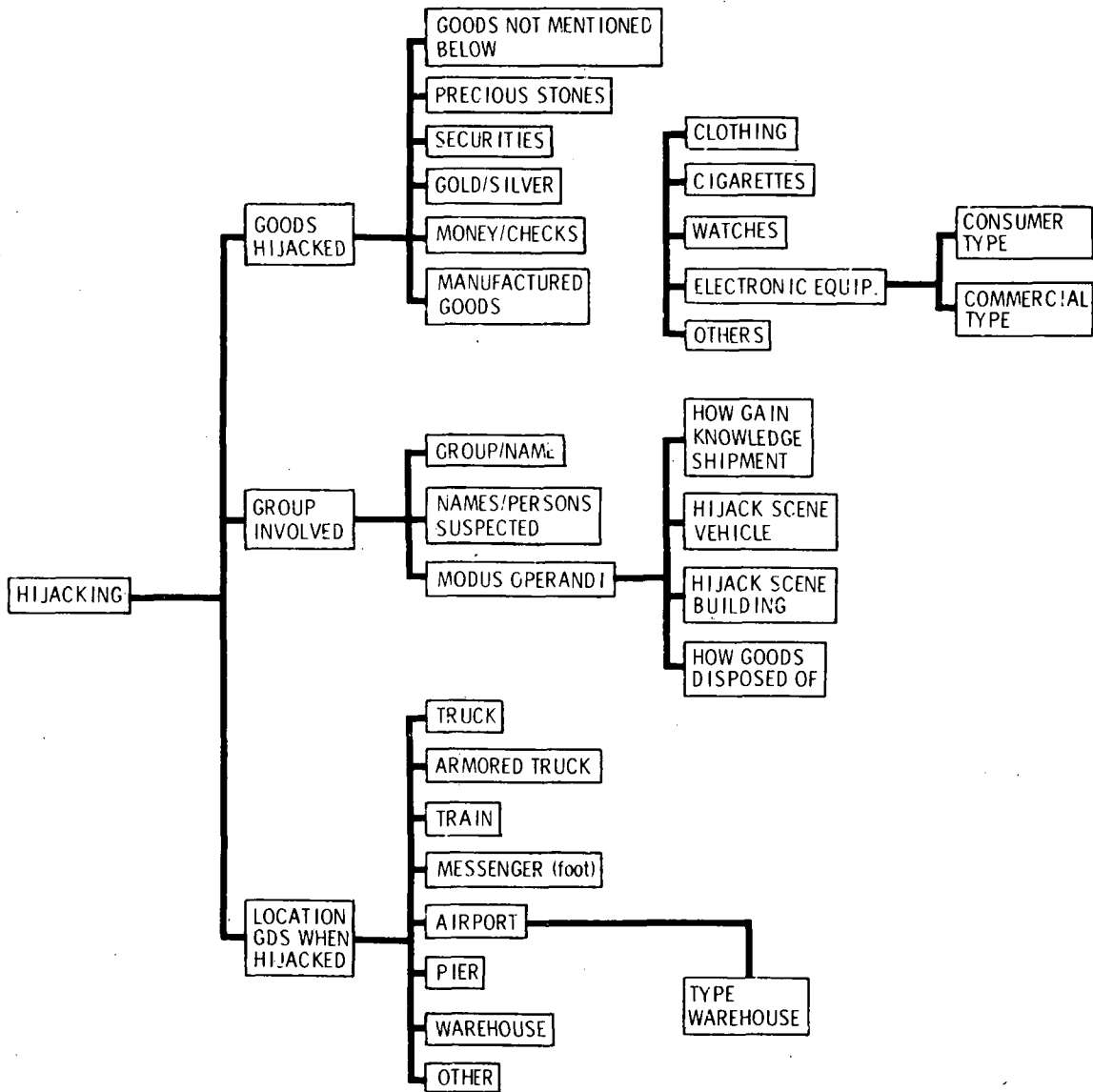


FIGURE 1 (Continued)

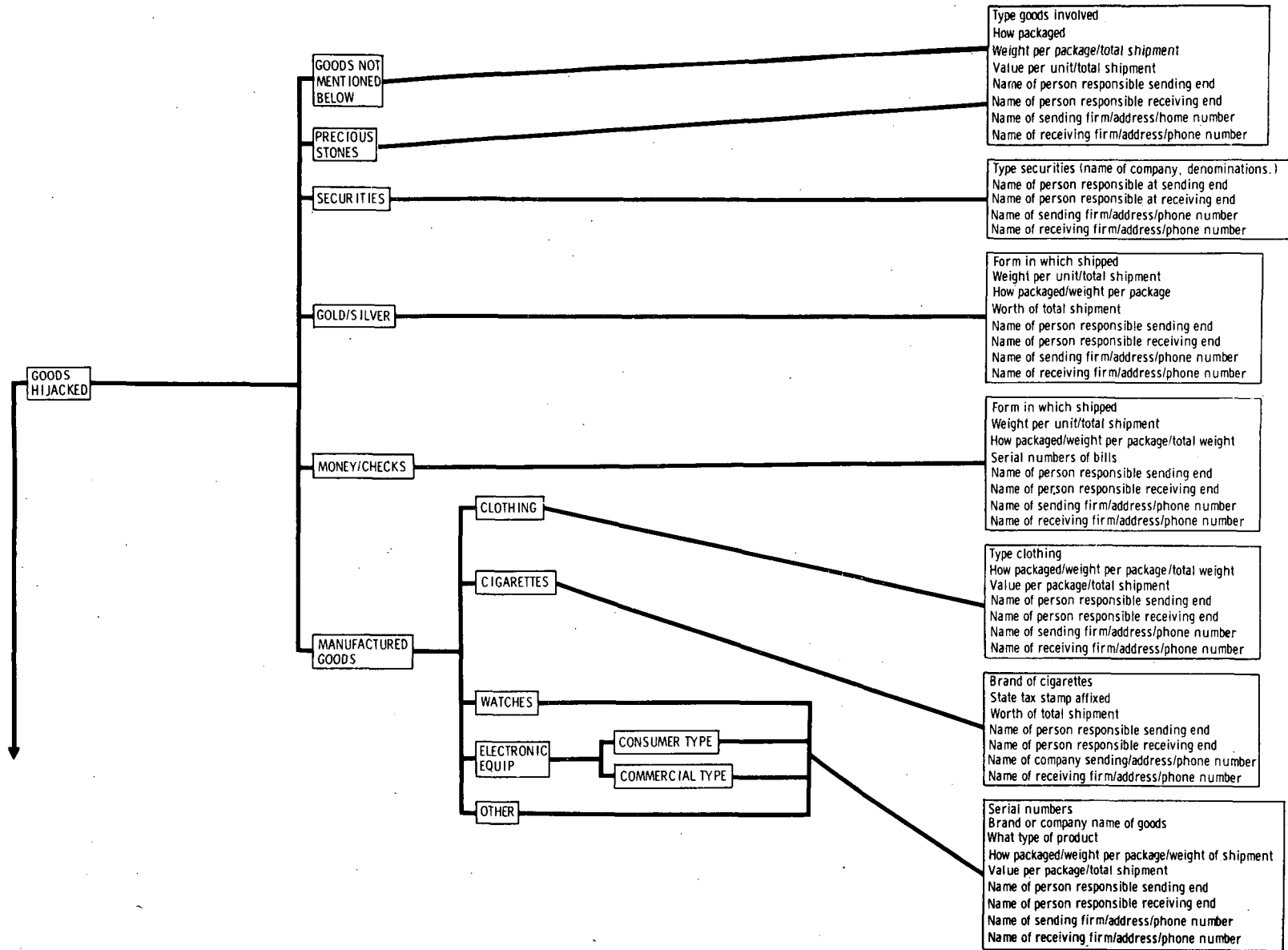
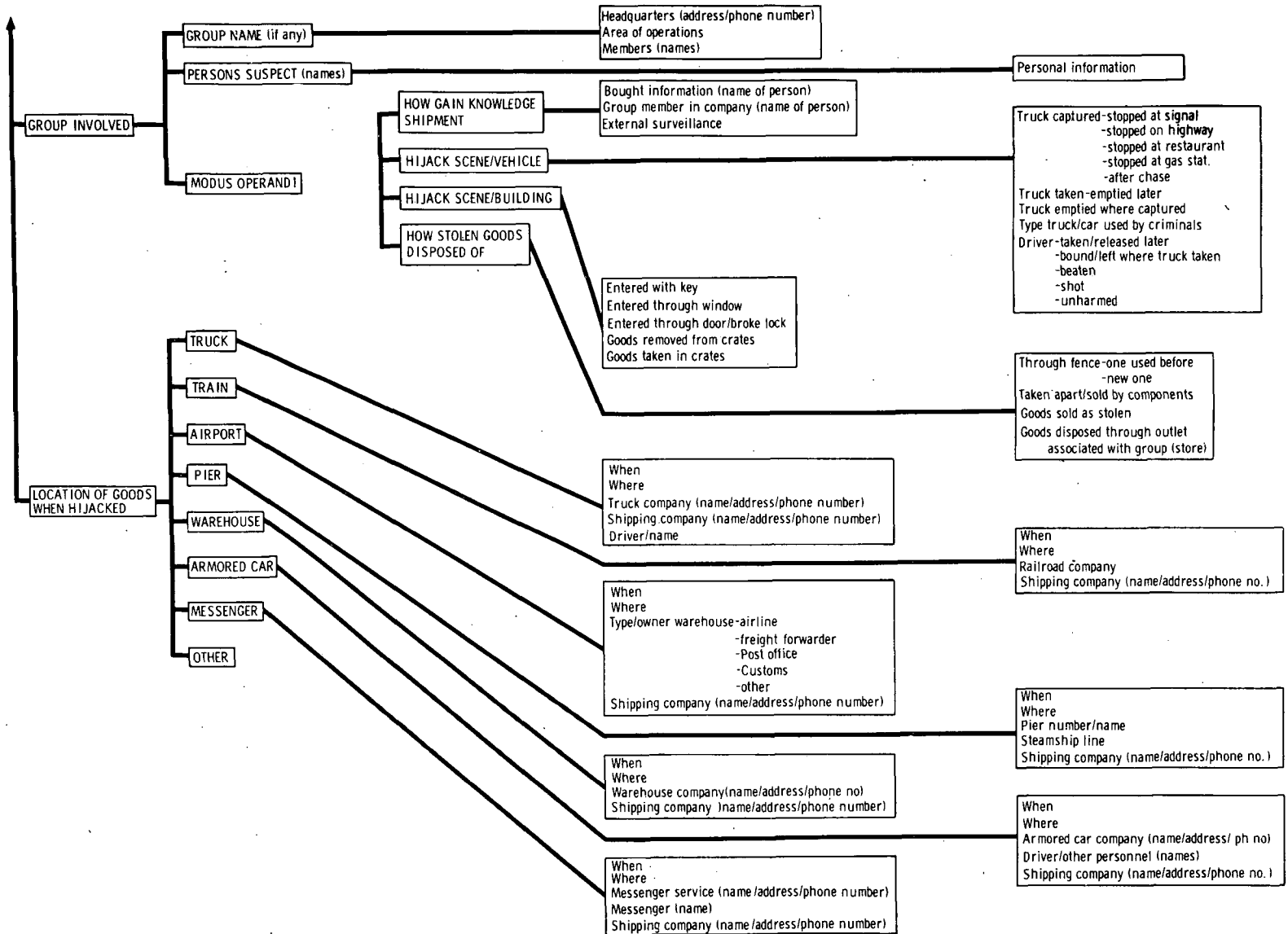


FIGURE 1 (Continued)



location and the simultaneous use of the computer by other elements of the agency. The problem is often further complicated if the computer is part of a system that 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 simultaneously access a common data base. In such a system each individual user can obtain only the information he/she is allowed to see, and any information entering the system is safeguarded from public disclosure. However, the degree of security will often result from the amount of funds available. The system designers must determine the value of the information and design safeguards commensurate with that value. In the paragraphs that follow, consideration is given to the various areas the system designers should consider in developing security for a particular computer installation.

a. **Physical Site.** The computer facility should be physically protected from intruders. This may involve no more than a guard at the door or may involve guards and double-locking doors with a TV camera between them. In the latter system the persons desiring entrance are held between two locked doors while they are identified over the TV circuit. The computer should also be located below the ground floor to prevent unauthorized persons from entering through windows to help alleviate electromagnetic radiation problems.

b. **Personnel.** All personnel associated with the operation and maintenance of the computer facility should be investigated. Ideally this will already have 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 misuse by unauthorized persons. However, if it is impossible to have intelligence personnel in the computer facility at all times (that is, when it is in operation) then every effort should be made to have intelligence tapes and discs locked up. This is pos-

sible if these files are not to be used on an on-line basis.

There are several areas to be watched with respect to security problems with computer room personnel. 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 person can change the logic of the hardware so that a certain sequence of instructions will bypass 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 review carefully all system modifications after they are performed and to insist that employees work in pairs.

c. **Security of the Information in the Computer Data Banks.** Security of the computer's data bank and its operation is a complex matter and should require the help of 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 out-station terminals the right to input and request data directly from the data bank.

A usual approach to maintaining security of computer data banks is to have a key-word method of entry. The intelligence computer files can be programmed to respond only to a key (code) word. This can be changed daily if so desired. The computer can be programmed not to print out the key word. But this approach, unless it is highly sophisticated, will only protect the non-determined probe. Physical security of data files, tape or disk, together with that of the entry consoles, is the most effective approach.

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 E

SECURITY

A. Introduction

Security of personnel, office and files, and operations is a special problem for the intelligence unit. Security is a particularly sensitive concern because of 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/he has recalled all books on loan, and has every volume in its rightful place on the shelves. She/he thereby achieves total control in a fluid, operational situation, but, of course loses 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.

The purposes of security in an intelligence unit are to ensure that information on file is protected against access by unauthorized persons and 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: to enhance the morale of the law enforcement agency as a whole by providing strong resistance to corruption and to encourage 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 ensure that all members of the unit are trustworthy and are in no manner acting as agents for organized crime or any other lawless element. The unit must adopt physical security methods that ensure that only authorized personnel have access to the files. Steps must be taken to ensure that the area cannot be penetrated easily when no personnel are on duty. Personnel should apply rigorous security precautions when performing their duties. This applies generally to operations in a dangerous area, when they operate in plain clothes or as undercover agents, and specifically when they use radio communications where there is always a risk of revealing their location or other information that would help 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 concerns allegations, unverified reports of activities and associations, and other matters not necessarily evidential. For example, the investigator cannot always be sure of the relationships among a number of people observed individually entering a given location, allegedly for 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 such observations 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 then are the security objectives. They may be better understood by listing objectives not sought by security policy.

- 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. The intelligence unit must perfect guidelines for passing reports outside its control. Such guidelines will generally concern the reliability quotient of recipients. But the purpose of determining levels of reliability is to ensure that the appropriate people receive the reports, not to prevent them from being read.

- Security must *not*, under any conditions, be used to conceal an intelligence unit's employment of illegal techniques, such as electronic surveillance, where it is not permitted according to the statutes of the particular jurisdiction. In such a case, security would

simply be contributing to a more disastrous show-down when, as is inevitable, the use of illegal means is revealed.

- Security must *not* be used to conceal reports either from the jurisdiction's political leadership or from 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. However every effort should be made to severely limit the numbers of persons outside the department that will have access. Nor should security be used to conceal or cover up mistakes or corrupt activities by members of the unit or the agency.

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

Security in any organization, whether it be military, diplomatic, or police, focuses on three aspects: the necessity to assure the personal security of the organization's staff, the development of means to protect records and facilities used by the agency, and operational security when communicating and when in the field of an operational problem. These various facets of security are discussed below.

B. Personal Security

Any intelligence unit must be assured that its own members are trustworthy and that they are good "security risks." The security of a person can only be determined by probing past actions, attempting to determine how the person will react under certain circumstances, and assessing current associations and social patterns. While the background investigation is by no means a perfect system, 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 is the only method available.

1. **The Background Investigation.** A background investigation should probe all aspects of a person's life, both professional and personal. The investigation should seek indications of a lack of character or integrity in either context. A person who lacks integrity in his/her personal life (in dealings with friends and family) will tend 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 are

especially important when associated with a position in intelligence. (See suggested Guidelines for a background investigation at the end of this appendix.)

Whether or not the intelligence unit is responsible for performing the investigations of its own new personnel, it must be aware of the principles that guide such an investigation.

First, 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 of 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 gauge the character of the landlady? What was the relationship between the subject and the landlady? Had they had other differences that might help explain her attitude toward 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/herself about the subject's social life? In short, evaluation and careful checking 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 developed in evaluating sources of derogatory information. In the example cited above, it is insufficient for the investigator merely to report about an inability 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 taken to substantiate or discredit the landlady's testimony, then elements of evaluation have been implicitly included in the picture.

The recipient of the report can compare the details of denials or agreements by the neighbors and associates of the subject with the landlady's accusations. This is perhaps an obvious point, but is one often missed by field investigators because of the long-standing 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 a sense of fairness. The investigator who reports on the irascible landlady may be fully

satisfied that she is a "vindictive old bag," but if there is no latitude in the reporting system to allow for such an observation, the investigator is forced into giving a distorted, albeit "objective," report on the subject.

Third, the investigator must not allow "fairness" to preclude his/her consideration that the subject might in fact be a rogue as suggested by the derogatory information. This is the basic reason for carefully checking derogatory information. If an investigator is unable to satisfy himself/herself 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/she is justified in recommending further investigation into the allegation. If nothing further turns up that corroborates or negates the charge, then the subject 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 discussion is best. Very often the subject's responses will give the investigator new leads to trace down; sometimes 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/her consent) about the allegation can be useful. 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/she can help refute the allegation, his/her candidacy will be foreclosed. This may be considered tough policy, but given the position the person 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 associates. (See Figure 1 for a sample financial questionnaire.) The financial dealings are important, if for no other reason than for determining whether the candidate is in financial difficulties which might make him/her susceptible to a bribe by someone intent on learning information about the intelligence unit's operation. A similar circumstance may occur where a person's personal life might be subject to blackmail, causing him/her to betray a trust.

2. Update of Background Investigation. It is also important to have a specific program for updating background investigations. Updating is necessary simply because people do get into trouble even though, 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 person, 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 that 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 "pay-off." In the second instance, heavy borrowing could mean either a "pay-off" or the development of a situation in which the subject could become susceptible to an offer of "help."

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 the person's other activities, especially of 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 occur at 1-, 2-, or 3-year intervals. Every person newly applying for a position in the intelligence unit, whether by transfer in the agency or from outside, should be told that the update is part of the requirement for service in 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

FIGURE 1
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:

3. Income (Continued)

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 _____

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 a subordinate at any time. The commander, after all, is responsible for the overall integrity of the unit. If he/she suspects that a colleague is "turning sour," it is best not to wait until the routine updating background investigation comes up or take a chance that the "suspect" will be picked in the next background investigation update. For if the commander waits, he/she cannot be confident of the trustworthiness of the unit. The agency, as a whole, may be exposed to serious damage.

3. Polygraph. In those jurisdictions where it is permitted, the polygraph can be of great assistance in evaluating the integrity of a prospective staff member. By its use, the unit can make sure that the subject is not hiding some past action that might cast doubt on his/her capability and, especially, on his/her 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 the person is attempting to conceal past actions, he/she can deny ever doing such a thing. Then the interrogator (and, especially the unit commander, particularly if he/she is really interested in getting the subject on the 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/she may be subjected to the polygraph, need not feel personally offended when the test is given. More importantly, the candidate probably will not apply in the first place if he/she has something to conceal and knows that it might keep him/her 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.

4. 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 in the requirements for security, why it is important, and the often tragic results that can follow a breach of security. They should understand that people from their own unit, especially those working undercover, or their informers, can be put in jeopardy by security violations. (More specific data on training can be found in Chapter V.)

C. Physical Security

The objective of physical security is to ensure the personnel of the intelligence unit that no unauthorized persons will have access to their working quarters or files. 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.

1. 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 trustworthy. A log should be kept of all non-unit people that enter the intelligence unit's area and physical means should be used to identify these persons before they can enter the area. In particular, there should 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 2 and 3 for sample office layouts.)

During a normal working day, one person should always be responsible for recognizing and admitting persons to the intelligence unit area and another for watching over the files. At night, if no one is on duty, the room must be secured by 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. (For a description of the several security measures that should be taken, see the sample intelligence unit office on the preceding pages.)

FIGURE 2

A SAMPLE SECURE OFFICE LAYOUT

A sample office layout, which demonstrates the physical security principle discussed above, is shown in the figure. The number items on the layout are explained as 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-hours-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 inadvertent or planned acquisition of data to which the intruder has no business.
 - 3a. During the hours that the office is open and staffed, 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, and so forth.
 - 3b. Access to the intelligence unit's space is through a door electrically controlled by the receptionist.
 - 3c. 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 a temporary replacement).
 - 4c. If at all possible, the file clerk (and possibly analysts who work closely with this person) 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 who 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 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, if only in cubicles, not only as an effective working area, but also to provide better security for the materials used and people interviewed. Compartmentalizing 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 since he/she probably will have papers to keep under personal control. The commander will need to confer privately with visitors from within and without the agency because of the sensitivity of the material being imparted.
 - 7a. It is suggested that a safe be available in the commander's office. This will insure the security of highly sensitive material and information that is for the knowledge of the commander alone (or for those members of the staff determined 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 privacy is, in fact, maintained when the door is closed.

FIGURE 2 - A SAMPLE SECURE OFFICE LAYOUT

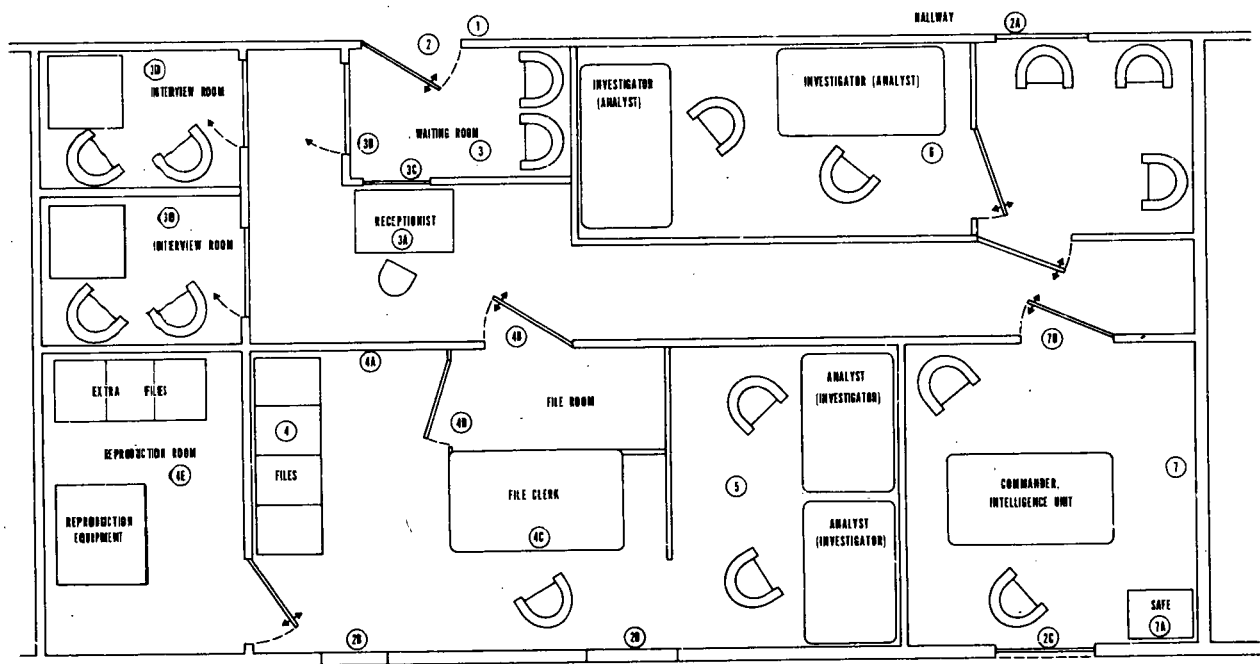


FIGURE 3

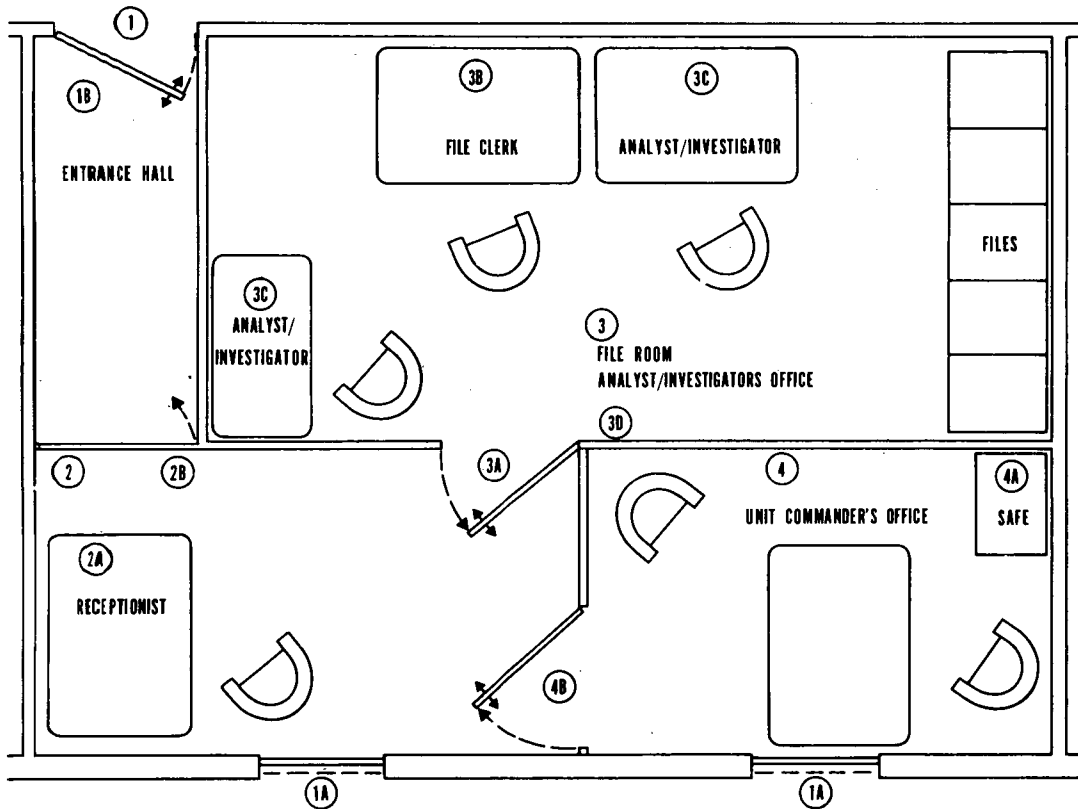
A SAMPLE OF SECURE OFFICE LAYOUT - SMALL UNIT

The sample layout for a small unit follows the pattern and principals set down for the larger unit, is shown in Figure 2. The layout in Figure 3 was designed for a three to five person 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-hours-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 inadvertent or planned acquisition of data to which the intruder has no business.
 - 2a. During the hours that the office is open and staffed, 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, and so forth.
 - 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 a temporary replacement).
 - 3b. If at all possible, the file clerk (and possibly analysts who work closely with this person) should be the only person allowed access to the files, and if 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. Furthermore, 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 since he/she probably will have papers to keep under personal control. The commander will need to confer privately with visitors from within and without the agency because of the sensitivity of the material being imparted.
 - 4a. It is suggested that a safe be available in the commander's office. This will insure the security of highly sensitive material and information that is for the knowledge of the commander alone (or for those members of the staff determined 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 privacy is, in fact, maintained when the door is closed.

FIGURE 3 - A SAMPLE SECURE OFFICE LAYOUT - SMALL UNIT



2. **The Files.** The files themselves, if in hard form, can be kept in ordinary filing cabinets. There is no need to use safes or special locking devices if the room itself can be secured. If there is a problem in securing the room, then the files should have locking devices. In any event, sensitive material 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 that they have classified as sensitive.) Ordinarily sensitive material should be kept in the intelligence unit commander's office but, if not, the lock combination should be available only to the commander or perhaps to one or two other senior members of the unit.

3. **Security and the Computer.** There are special problems for the unit that has its own computer. In addition to the security of the unit's area discussed above, the computer and its data must be protected. The first concern must be for the consoles through which the computer's information is queried and inputs made. Whether there is only one console or a series of remote stations, access must be restricted to authorized personnel only. When further control is deemed necessary, computer programs may be coded to restrict retrieval to those who know the code. Not only to ensure security but also for proper evaluation of inputs, all inputs should be inserted into the computer by the intelligence unit rather than directly from outstations. In other words, the computer should be programmed to refuse outstation inputs. Similarly, 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 modify existing information. Special care is required since data in the bank often require review and correction. They may also require purging where the subject of the information is incorrectly identified or 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 staff member 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 non-dedicated computer, that is, one owned by another department that 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 D.)

4. **Security and Privacy.** A major function of the security system of an intelligence unit in a police department is to protect its information from misuse. The privacy issue, when it relates to intelligence files, is a more difficult and urgent problem than when it relates to routine police records, the so-called "rap sheets." In the case of intelligence records, much of the information will be unverified and therefore may contain allegations, references to associations, and even analyses of potential activities, whereas routine police records are official documents. Much of intelligence material may never be tested in the courts and 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.

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 such as credit card bureaus, banks, employment agencies, personnel departments, and so forth. Care must be taken on a case-by-case basis to avoid giving such information to law enforcement agencies that have a record of not handling such material in a confidential manner. Secondary disclosure can be as damaging to the individual as disclosure by the primary agency. (For further discussion on privacy, see Appendix A.)

5. **Organization of the Office for Security.** To ensure the implementation of security policy, it is essential in the intelligence unit that someone be given specific responsibility. This person 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. The security officer must be responsible for seeing that the standard operating procedure 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.

D. Operational Security

Security also has a definite role in the operations of the intelligence unit. The intelligence investigator must take measures to ensure that his/her specific activities at a particular time and place are known to as few persons as possible. The investigator searching for indications of new criminal developments will want to have his/her efforts remain completely unnoticed, if at all possible.

The analyst does not want anyone outside of the unit to know of his/her concentration on the development of a particular pattern of criminal activities about which the investigator has as yet no hard evidence by relatively certain indications.

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 ensure that no electronic eavesdrop devices are in place. If possible, the office should be given one or more non-agency 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 non-official 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 between the field and office. 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 radios 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 of an investigative rather than 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 ongoing operational 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 standard operating procedure of the intelligence unit that it always operates as though other elements of its agency were penetrated. Obviously, this element of the procedure itself should be held closely to avoid antagonizing other officers.

The commander of the intelligence unit must also provide for the security of the unit 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 unit personnel operate in pairs, or have another officer cover the person doing the investigating.

E. The Responsibility of the Unit Commander

As is 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 security rules for the unit. The commander must see to the arrangement of the office and press to have space secured in a different manner than any other in the agency. The unit requires special cars, and communications require special consideration. Unit personnel 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 in all these actions and policies, the commander will probably need 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 the commander's particular attention to ensure that security is effective.

ATTACHMENT 1

GUIDELINES: BACKGROUND INVESTIGATION OF APPLICANTS – INTELLIGENCE UNIT¹

STAFFING BACKGROUND INVESTIGATION

INTRODUCTION

The intelligence unit must maintain an unequalled standard of excellence in its personnel and their performance. The degree of success 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 eligibility for a position of public trust. Any doubts as to the applicant's suitability will be resolved in favor of the intelligence unit.

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 process an applicant for employment successfully and maintain a high level of professionalism, the agent conducting the investigation must keep the following in mind at all times:

Maintain Professional Attitude

1. Be deeply motivated and aware of responsibilities.
2. Be adept at gathering all facts possible.
3. Possess a sense of fairness and respect. Report all facts, both for and against.
4. Evaluate the facts carefully.
5. Be a good interviewer.
6. Be tactful, diplomatic, and patient.
7. Put aside personal compassion.
8. Maintain a professional and moral responsibility to the agency.

Review the Application

1. Determine if all information has been provided. If application needs 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.

Report Derogatory Information to the Supervisor Immediately

1. Develop derogatory information fully.
2. Be certain reports reflect unbiased and complete inquiry.
3. Evaluate information immediately to determine whether further investigation is warranted.

NOTE: The investigator's character, ideals, standards, personality, and ability to understand others will have a tremendous impact upon the evaluation of background findings.

¹The Guidelines presented here are, for the most part, those developed by the Florida Department of Law Enforcement for its use in applicant investigations.

THE BACKGROUND INVESTIGATION

General

1. Advise the interviewee of 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. Be certain the interview is voluntary.
5. Be certain the investigation is 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, make personal contact with the interviewee. Appointments should be made prior to an interview whenever possible. In lieu of personal contact make telephone inquiries and/or send letters.

Objectives

1. Determine if an applicant is qualified for employment with the intelligence unit.
2. Keep the following points in mind throughout the investigation, which may predict success or failure in the position:

Character and reputation
Loyalty
Associates and/or relatives
Qualifications and ability
Emotional stability
Social adaptability
Health

Areas to Investigate

1. *Criminal records*

FBI files
Agency—DIA files
Agency—NCIC files
State/Motor Vehicle/DL files
County Judge's Office

Subversive files
Criminal and Civil Court records
Police warrant files
Sheriff and Local PD 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-travellers

Teachers
Employer
Neighbors
Other

4. *Employment*

Dates
Type of promotions
Rate of pay
Description of duties
Abilities (aptitude & initiative)

Attendance record
Recommendations
Ability to get along with others
Reason for leaving

5. *Education*

Dates attended
Any disciplinary action
I.Q. rating or test 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
Leisure time
Ability to budget and live within means

7. *References*

Personal contacts whenever possible.

8. *Military service*

- a. There is a 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 Co.)

Amount of payments
Public records or pending civil action

10. *Health*

Family doctor—hospitals—clinics
Check neighborhoods

Sources of Information

1. State investigative bodies (e.g., State Police, Beverage)
Federal investigative bodies (e.g., United States Justice Department; Treasury Department)
2. County and Circuit Clerks office, U.S. District Court Clerk
3. Probation and Parole Department
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 investigation staff
14. Hospital and medical records (doctor's records)
15. Bureau of Vital Statistics
16. Records bureau of Federal, State, County, and City PD'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 members (e.g., labor, fraternal)
23. Banks
24. Retail businesses
25. Church—baptismal records
26. Neighborhoods
27. Industrial Commission

Additional Information

1. *Personal history* (verify)

Birth	Divorce	Adoption	Legal name change
Marriage	Death	Separation	

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 and date of birth of spouse)
- 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 \$100.00
- i. Parents' name if applicant single
- j. Credit check to be made in all areas resided in by the applicant or his/her 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 the 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/herself, 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
 - Police precinct
 - 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, and so forth.
- b. If reserve, determine whether ready or standby.

NOTE: If standby, ascertain standby 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 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 disloyalty, 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. Customs 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

• teletype

• letters

• personal contact (local law enforcement agencies)

b. FCIC—wanted check

c. NCIC—wanted check

d. FBI—applicant only (initiated by personnel)

e. Verify all report 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

REPORT OF INVESTIGATION

Heading

1. Title

2. Dates covered

3. Recommended disposition

Synopsis

1. Introductory information
2. Personal history
3. Arrest record
4. Financial investigation
5. Education
6. Employment
7. Personal and develop references
8. Neighborhoods

GENERAL INFORMATION REGARDING THE SYNOPSIS

1. When using applicant's name, use full name. If name used 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 typewritten synopsis and termed a partial background investigation.

APPENDIX F

ANALYST MANUAL

This manual is designed to set up the duties of an analyst (or whoever is designated to perform the analyst's duties) if the function of analysis in a police intelligence unit is to be accomplished. It lacks specificity since it addresses activities that differ from one department to another because of the differing organizational structures and activities of the unit. Moreover, in some units analysts perform clerical functions and in others become involved in investigations. The manual argues that certain activities must be performed if there is to be analysis and points out techniques that will be useful to the analyst in performing this function.

The analyst's activity can be grouped into three general areas:

- Building a base of information about assigned areas of criminal activity.
- Responding to requests from investigators for immediate assistance on their particular investigation— a function normally termed "tactical intelligence."
- Producing analytic reports as requested (or as self-initiated by the intelligence unit's commanding officer or analysts) that explore a particular area of criminal activity in depth—an activity normally called "strategic intelligence."

It is essential that the unit commander makes sure that the analyst has time for analysis. The analyst must be able to answer the questions "So what?" and "What is the meaning of this information?," otherwise the intelligence unit is not fulfilling its function.

A. Building the Information Base

While the analyst is not responsible for gathering information, he/she has a major responsibility for ensuring that it is entered into the intelligence files in a way that makes it readily available for analysis. The analyst also develops other sources of information that enable him/her to do the job more effectively. These include:

- Reading the newspaper and recording various activities associated with the analyst's area of crime. These are not necessarily criminal events, but might include articles that suggest the development of a potential area for crime or a target a criminal might find highly lucrative. The analyst should also read various

police and other law enforcement periodicals to keep up with developments in other jurisdictions and associated areas of criminal activity. Criminal activity will often spread from one jurisdiction to another. By reading about new patterns of crime, the analyst can be prepared to examine incoming information and detect developments in his/her own jurisdiction.

- Analysts should establish friendships among the investigators in the department and in other departments in the area so that the investigators can develop an understanding of the value and competence of the analyst, while the analyst, in turn, can gain some insight into street activity and develop a better feel for criminal activity.

- Wherever possible, the intelligence commander should seek agreement from the investigative elements to debrief informants and arrested persons. In most cases, criminals have knowledge of more than one specific criminal activity. Police departments tend to organize their officers by criminal activities such as narcotics, gambling, homicide, and others. The criminal, on the other hand, will engage in any criminal activity that appears profitable.

- The analyst should be responsible for determining what information from a report goes into the files. The analyst should ensure that the indexing being performed includes critical items such as names, addresses, locations, and above all, criminal activity.

- The analyst should build some information tools of his/her own. It is not suggested that he/she start a special file but, as incoming reports are read and ideas strike him/her, the analyst should record them in some orderly manner. These thoughts then can be referred to later and developed further as more information becomes available. For example, the analyst might write down, for his/her own use, several hypotheses. They may be too tentative to bring to the attention of the supervisor; but the analyst should continue to probe in this manner. Tentative link diagrams that give a plausible view of the associations among various criminals may also be maintained. They may initially be based on very sparse information and should, therefore, not be incorporated into the main files or brought to the supervisor's attention. Maintaining the diagram will help the analyst in reading and understanding the day-to-day activity.

- Finally, and perhaps the most important tool, is a running list of information gaps. As the analyst reads the report and begins to develop tentative hypotheses, he/she will be aware of information that is needed in order to prove or disprove the ideas gained. These information needs should be set down in a tentative manner so that when the analyst becomes sufficiently convinced of the hypothesis, he/she can present them to the supervisor. At that time the analyst should be prepared with a list of questions for the supervisor and, if approved, sent on to investigators in the intelligence unit or other investigative units to answer. These tools will help the analyst determine patterns of activity and linkages and to organize information.

B. Responding to Tactical Requests

A principal function of analysts is to respond to requests from investigators in the field for name checks and other information in the intelligence files. This is an essential function and the extent to which it should be done by analysts rather than clerks is determined by the intelligence unit commander. The commander's decision will be based on the caliber of the clerks and of the analysts, the number in each category available, and the extent of the workload posed by the investigators. It is essential that the unit commander be aware of this problem and understand that this activity is the main competitor with time for analysis. If the analyst never has time to ponder uninterruptedly about an area of criminal activity, he/she is unlikely to ever be effective. In most units this is a critical problem usually unrecognized and the productivity of the intelligence unit is severely damaged.

The analyst, in answering the tactical requests of investigators in the field, should try to do more than simply provide a person's name that is in the file. If the criminal is operating in his/her area of responsibility, the analyst should give the investigator not only the criminal's associates and areas of operation, but also a hypothesis about the activities of the criminal. He/she must indicate how confident he/she is with the hypothesis and the extent to which there is supporting evidence.

All calls for help must be recorded in order to give the intelligence unit information on a case that is being followed. On the other hand, it is essential that the intelligence unit record all assistance it gives. The compilation of actions in response to tactical requests will also help the unit commander answer the question, "What does the intelligence unit do?"

C. Intelligence Reports—Strategic Intelligence

Strategic intelligence is important because it is often the only place in the police department where criminal activity is analyzed in depth. The results are an essential input to the planning of major enforcement actions. A strategic intelligence report will present what is known on the subject criminal activity, what information gaps exist, and suggest points on which to focus. This section shows the analysts' specific steps in writing a strategic report, including:

- Surveying information sources
- Formulating hypotheses
- Designing a collection plan—identifying information requirements
- Collecting/Collating
- Analyzing
- Writing the report

Intelligence and Hot Carpets—An Example. The chief has received a letter from the local Chamber of Commerce that a wholesale carpet dealer has complained that he suspects someone has been distributing stolen carpets. The dealer has no idea who is dealing in stolen goods, but his sales to retailers have fallen sharply while retail volume has increased slightly. He was told by one of his best customers that he, the retailer, had been able to buy quality goods from an unnamed source at a substantial discount. The wholesaler, familiar with suppliers in the area, knew that such low-priced carpets could not be profitably handled by his competitors and brought this to the attention of the Chamber of Commerce.

The chief forwarded a request to the intelligence section to do a report on the problem. Analyst Joe was assigned to it.

1. **Surveying Information Sources.** A strategic intelligence analysis (study or report) normally will be initiated by requests from the chief or other senior officers. However, the intelligence unit should have the right to initiate. In response to such a request the analyst will first consult the most readily available sources of information. Although the nature of such sources will certainly vary widely among analysts and among departments, some sources should be available to all.

The first sources of information the analyst will consult are the files of the intelligence unit. In our sample case, the analyst would first examine the criminal activity data file (described in Chapter III) for information on the disposal of stolen goods. The analyst should

also check other functional files which may be applicable such as the address index file. If the analyst suspects that a particular criminal may be involved, the analyst will consult the person's biographic data file.

Analyst Joe checks the criminal activity file on disposal of stolen goods-furniture and finds that the only information relating to carpets were a few reports resulting from Sunday swap meets. Investigating officers noted that one regular seller occasionally had several new carpets among his wares. These could not be identified as stolen property but their new condition and low price prompted the filing of the report. Neither the name index nor biographic data file contained any further information on the swap meet dealer. He had not been seen at the swap meet for 3 months. Analyst Joe next checks his files on hijacking but finds no information relating to stolen furniture. The address index file reveals nothing on the carpet store mentioned in the Chamber of Commerce report.

The second step in a general information survey is to consult other analysts and investigators who may have information on the problem at hand. Sources of information outside the intelligence unit but easily accessible can be consulted. In cases where the activity was started by a report from a police officer or a complainant, a debriefing interview with the source often provides useful information.

Personal files and other information sources within the intelligence unit are no further help in probing the suspected activities of the carpet retailer. With permission from the intelligence unit CO, Analyst Joe contacts the complainant through the Chamber of Commerce and arranges for an interview since the principal indications of illegal activity thus far are the wholesaler's suspicions. Before recommending any further investigative activities, Analyst Joe would like more evidence. From the interview he learns that the wholesale dealer has been one of the highest volume salespersons in the area for several years. In the past few months, however, many of his customers have reduced or cancelled their order from him. The owner of the retail store which had prompted the initial complaint was a long-time customer who assured the wholesale dealer that his new supplier was a legitimate salesman with whom he had dealt in the past.

2. Formulating Hypotheses. Procedures for identifying information requirements for strategic intelligence are less straightforward. In general, a hypothesis will

direct the collection of strategic information. It is particularly important to impose order on requests for strategic information since the utility of such data is not easily ascertainable and it is easy to end up with vast amounts of useless data obtained at great cost.

A hypothesis states the analyst's judgment of the meaning of the situation with which he/she is dealing. Usually an initial hypothesis (or hypotheses) is developed when facts and pieces of information are relatively few and may be doubtful or contradictory. The hypothesis is a logical reconstruction of the subject activity or event which appears to give the best fit for known information. A hypothesis must be dynamic in that it is constantly reviewed as new information is received. Facts must not be forced into a hypothesis just because they sound good or fit a particular belief of the analyst. The analyst may keep several hypotheses going for a period until pieces of definitive information are developed that eliminate some or all but one hypothesis.

Analyst Joe now develops his initial hypothesis. He believes that:

- The illegal trade in carpets is substantial and well organized.
- The carpets are obtained in large lots by hijackings or breaking into warehouses.
- The rug theft is being accomplished in another jurisdiction and then brought into his area on order.
- Experienced rug salesmen are involved.

3. Designing a Collection Plan. The hypothesis not only focuses the thought of the analyst but also becomes the basis for development of a rational collection plan. If the commander of the intelligence unit accepts the hypothesis, the analyst and/or the investigators can see what information must be developed and in what order. Thus, a priority structure is created.

Since there is no evidence of local hijacking activity, Analyst Joe recommends that requests for information on major theft of carpets and fencing activity be sought from state and local law enforcement agencies in the textile and carpet manufacturing regions. He also recommends the uniformed patrol units and the burglary investigative units be alert for deliveries from rented trucks, or other unusual activities around the suspect carpet store and other large carpet dealers. Analyst Joe asks the wholesale dealer to provide him with financial data that document the declines in his sales and also requests from the Chamber of Commerce data on retail carpet sales in the area. The commander of the intelligence unit approved

Analyst Joe's recommendations and took the necessary steps to implement them.

4. Collecting and Collating. Ideally, the analyst will be minimally involved in field collection of information. He/she will be responsible for collating incoming data which have been specifically requested. Also, the analyst should regularly review selected newspapers and other periodicals. The relationship between collation and analysis of data has been emphasized throughout this manual. Summarizing and organizing information is the first step in conducting intelligence analysis. The hypothesis is again the key to the procedure, providing the initial clues and background information by which new data are organized.

Sales data provided by the Chamber of Commerce and the wholesale dealer support suspicions that stolen carpets are being sold in the area: wholesale orders from many of the larger retail stores have declined while retail sales by those stores have increased slightly. A review of local newspaper advertisements over the past year revealed that some of the largest retail dealers have been holding significantly more reduced-price sales in the past few months. Reports from law enforcement agencies in other jurisdictions indicated no hijacking activity involving carpet shipments had been reported. However, it was reported that the investigative section of the state police in a carpet manufacturing region was investigating scattered reports of increased pilferage from carpet factories and warehouses.

5. Analysis. The three steps involved in analysis were discussed in Chapter IV. These are:

- Summarize relevant information
- Compare the summary with a set of expectations derived from an initial hypothesis
- Explain the results of the comparison

The analyst summarizes and organizes the data and compares them with his/her hypothesis. If the data are consistent with expectations, the hypothesis is supported. If the data are not consistent with the analyst's expectations, the hypothesis must be modified or reformulated. If the hypothesis is supported, explanation consists of elaborating that explanation given by the hypothesis. In cases where the hypothesis is not supported, the possible explanation implied by that hypothesis has been eliminated and explanation is undertaken by modifying or reformulating the hypothesis and specifying new information requirements.

Information which has been collected thus far indicates two things:

- Suspicions of illegal traffic in stolen rugs have been confirmed.

- The initial hypothesis that a hijacking ring was operating in surrounding areas was not supported.

Comparing retail and wholesale sales data revealed that rugs are being supplied to and sold by local dealers outside normal channels. It also appears that stolen carpets are being obtained through systematic small-scale thefts from a number of manufacturers rather than by hijacking. The means by which the stolen rugs are acquired and distributed is not certain and answering these questions will occupy much of the next phase of the investigation. A possible hypothesis, suggested by the widespread nature of the pilferage, is that employees of a legitimate wholesale dealer are paying workers to steal rugs and selling them to retail stores. In conclusion, Analyst Joe states that more intelligence investigation is needed before an enforcement investigation is initiated. Specifically, he recommends that:

- Other local retail and wholesale carpet dealers be investigated,
- Other jurisdictions in the area be alerted in an attempt to determine the extent of the racket,
- His findings be passed on to the state agency which is currently investigating pilferage, and
- A new section in the fencing file be opened on this alleged means of disposing of stolen goods.

In some cases, the intelligence investigation would have discovered sufficient indicators of criminal activity to warrant a recommendation that an enforcement case be opened. The decision rests in part on the apparent validity attached to the intelligence analysis and information, the "SOP" established in the department, and the workload of the investigation unit.

This example illustrates that the way in which information is organized can be almost as important as the content of that information. Two principal pieces of information in this example—drops in wholesale carpet sales and small-scale but widespread pilferage at plants and warehouses—do not appear to be particularly important by themselves. When viewed together and compared, these data indicate the probable existence of an organized group of criminals involved in the theft and disposal of carpets. The comparison of data has also been illustrated. The three steps involved in the analysis of this example are summarized in Table 1 below.

TABLE 1
An Example of Analysis

<u>Summarize</u>	<u>Compare</u>	<u>Explain</u>
<ul style="list-style-type: none"> ● retail sales data ● wholesale sales data ● newspaper advertisements ● reports of hijacking ● reports of pilferage 	<ul style="list-style-type: none"> ● current wholesale vs. current retail sales ● past wholesale vs. present wholesale ● past retail vs. present retail ● apparent supply of carpets vs. apparent demand for carpets 	<ul style="list-style-type: none"> ● alternative to hijacking as source of stolen goods ● means of distribution through legitimate retail outlets ● means of access to plants and warehouses ● techniques for inducing systematic pilferage

D. Techniques of Analysis

This section presents a discussion of association charting using transaction matrices and link diagrams and an introduction to the use of statistical techniques in intelligence analysis. The discussion of the latter is, of course, incomplete. No attempt is made to instruct the reader in the use and interpretation of particular statistical measures and formulas. A bibliography of introductory texts in statistical analysis for the social sciences is included so that the reader may pursue further what can only be mentioned here.

1. **Association Charting.** As presented here, association charting is a form of interaction analysis, employing geometric or tabular forms of presentation. These techniques are most often used to represent observed or suspected associations among criminals. Association charting may also be used to show relationships among events, places of business, organizations, stolen goods, or virtually any combination of these or other subjects of interest to law enforcement personnel.

Three basic means of presenting such relationships are given here:

- **Transaction matrix**, showing the number of interactions among subjects (see Figure 1).

- **Strength of association matrix**, showing an estimate of interactions or strength of association (see Figures 2 and 3).

- **Link diagrams**, graphically displaying associations among members of a group (see Figure 4).

The purpose of each of these representations is to clarify the complex relationships among persons, organizations, and activities which characterize organized crime. These techniques help the analyst by enabling him/her to graphically depict complex criminal interactions. Each event is considered individually and inserted into the matrix or diagram one-by-one.

An example of the use of these techniques is presented below. Table 2 displays the narrative information from which the matrices and diagrams are constructed. The sources and especially the readability of such information are important. Narrative descriptions of activities may be abstracted from field reports, intelligence files, informant tips, newspapers, and so forth. If the analyst intends to construct a link diagram, it will be much easier first to construct a transaction or strength-of-association matrix.

In constructing a strength-of-association matrix (Figure 1), the analyst must decide how to score the differences in strength of association. The simplest approach is to use a two-category approach and score each link as strong or weak. This device can also be used to reflect uncertainties regarding the links among subjects. Where the evidence is reliable that, for example, two businesses, A and B, are connected but the relationship between each of these and a third is

Figure 1. Transaction Matrix

	Sid	Al	Phil	Janet	Herb	Henry
Sid						
Al	3					
Phil	2	10				
Janet	2					
Herb	2	1	14			
Henry	4			1	3	

Cell entries are the number of observed interactions.

Figure 2. Strength of Association Matrix

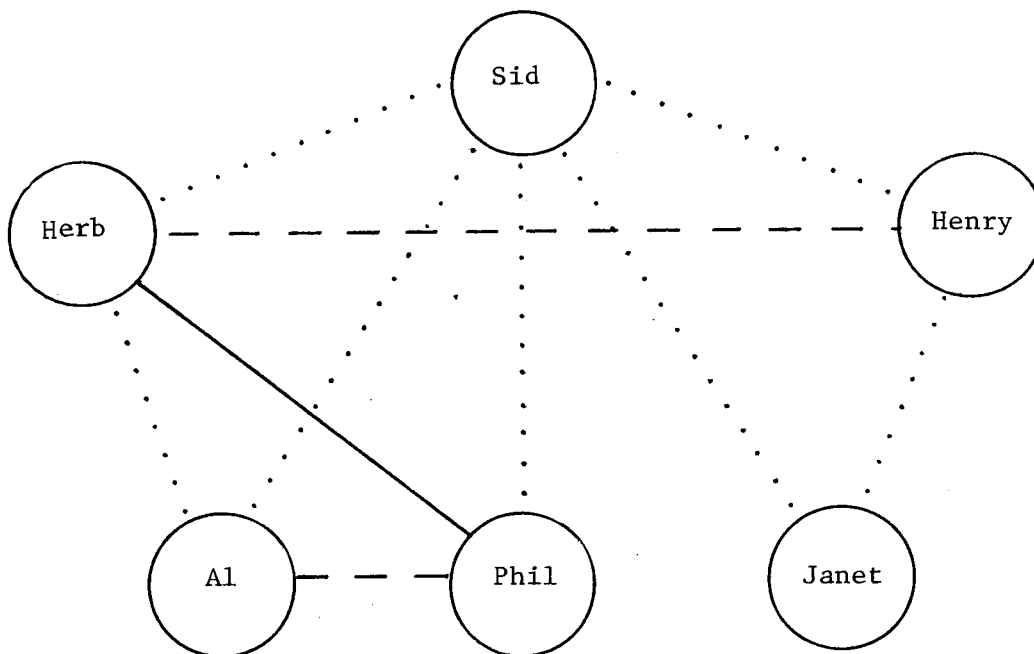
	Sid	Al	Phil	Janet	Herb	Henry
Sid						
Al	1					
Phil	1	2				
Janet	1					
Herb	1	1	3			
Henry	2			1	2	

1 = weak association
 2 = moderate association
 3 = strong association

Figure 3. Strength of Association as Affected by Reliability of Information Factor

	Sid	Al	Phil	Janet	Herb	Henry
Sid						
Al	1					
Phil	1	2				
Janet	1					
Herb	1	1	3			
Henry	1			1	2	

Figure 4. Link Diagram



Strong Association _____
 Moderate Association - - - - -
 Weak Association

uncertain, the pair A-B may be scored as "strong" while the pairs A-C and B-C are scored "weak." In the example presented in Figure 2 there are three possible scores for strength of association; 1 indicates the weakest link, 3 the strongest, and 2 a moderate link. When reliability of information is considered it would only cause Henry's connection with Sid to be placed in the weakest category rather than in moderate. The relationship with most questions is that of Herb and Henry. A day of fishing indicates closeness. But the report of Herb and Henry meeting once a week (with Sid) is of low reliability. This weakens the estimate of strength in the relation. If it becomes important to determine these relationships more specifically, the Herb-Henry one would seem a good place to start. The steps involved in association charting are summarized in Table 3.

2. Use of Statistical Techniques in Intelligence Analysis. The analyst should become familiar with the fundamentals of statistical analysis. The potential value of statistical techniques for intelligence analysis is great. More generally, the analyst will be concerned with quantitative methods that include statistics. Quantification is defined here as the assignment of numerical values to verbal concepts. Quantitative methods in general and statistics in particular can be used to:

- Summarize a large body of data into a small collection of values
- Discover new relationships in the data
- Confirm that relationships in the data did not arise merely because of happenstance
- Test hypotheses and explanations by confirming them with empirical evidence

TABLE 2

Activities of Sid Shark and Associates over a 2-Week Period

Reliability
of
Information*

- (1) Each weekday Sid lunches at Gus' Grill. Over the past 2 weeks he has been joined by Al three times, Phil two times, and Janet two times.
- (2) Phil meets with Herb for a couple of hours each afternoon at Herb's Lounge.
- (3) Herb and Sid are joined once a week by Henry.
- (3) Sid has met Henry on two other occasions in Henry's office at the Friendly Finance Corporation.
- (1) Herb and Henry went fishing together for an entire day.
- (1) Al and Phil both work at the Packing House.
- (3) Janet has visited Henry's office once.

*Legend: (1) Highly reliable

(2) Probably factual

(3) Possibly factual

• Inform readers about what the data indicate¹

In summarizing, statistics are used to reduce a large number of observations to manageable proportions. A statistic or indicator is calculated to reflect some particular characteristic of the larger body of data which it represents. Of course, some information is lost in summarization. No single statistic can accurately represent 100 observations. For example, the familiar concept of the average, or mean, is used to represent a large series of numbers. The mean indicates the average value of the collection of numbers as a whole, but it does not necessarily accurately reflect the value of any single number. By summarizing the series of values using the mean, the analyst loses the information provided by each individual value. There are methods of estimating the information lost through use of a summary statistic such as the mean. Standard deviation is a measure of the average difference between the mean and each individual observation. It gives the average error involved in using

¹ After Tufte (1974: 1)

TABLE 3

Association Charting—Checklist

- Organize information sources
- Abstract activities of interest (See Table 2)
- Tabulate interactions among subjects in a matrix format
 - Take reliability of information into account (See Figure 3)
 - Determine strength of association scores (See Figure 2)
 - Enter numbers of interactions (See Figure 1)
- Transfer the matrix cell entries to a diagram; show number of interactions and/or strength of association between pairs (See Figure 4)

the mean to represent individual values. However, the standard deviation is not a perfect indicator of each individual difference between the mean and each individual value. The point behind these cautious remarks is that the benefits of summarization are not cost-free. Given very large numbers of observations, the use of summary statistics becomes mandatory, but the analyst should not lose sight of the possible misrepresentations fostered by the use of summary statistics.

Discovering new relationships within a body of data depends as much upon the insight of the analyst as it does on the use of statistics. However, summary statistics and other types of indicators can highlight relationships which may be obscured by masses of data or irrelevant information. The simplest indicators are often the most appropriate when initially exploring an area of investigation or collecting data. For example, percentages are familiar but very important indicators whose value lies in standardizing raw numbers of observations. More complex measures of association indicate the extent to which numbers measuring different concepts vary together; whether they increase together, decrease together, or whether one increases as the other declines.

Inferential statistics enable the analyst to determine whether findings reflect relationships that exist in the activities from which data were drawn or whether those relationships *may* be due to chance fluctuations in the sample of data the analyst is examining. Inferential statistics cannot provide a conclusive answer regarding the statistical significance of observed relationships. They do enable the analyst to evaluate the probability that observed relationships are due to chance. The use of any inferential statistics, however, requires that several rather constraining assumptions be made regarding the source of sample data and the means by which those data were selected. These assumptions are not often satisfied by the data and collection methods available to intelligence analysts.

Procedures involved in testing hypotheses have been discussed earlier in the appendix and in the chapter on intelligence analysis. Statistical indicators can be especially useful in this area by providing explicit criteria for testing the hypothesis. As discussed above, analysis consists largely of comparing empirical evidence with a set of expectations. These expectations are generally derived from hypotheses and may be expressed quantitatively and subject to statistical comparison against actual data. Again it may not be possible to meet the assumptions required in using inferential statistics, but the analyst should become familiar with these techniques. Even if inferential statistics may not be used, quantitative indicators can still be of value in testing

hypotheses. Expressing the hypothesis in a manner amenable to statistical tests establishes unambiguous criteria for comparing observed data with expectations.

The value of statistics in clearly presenting information is enormous. There are no languages in which concepts may be expressed more clearly than mathematics. Statistics not only enables the analyst to express information succinctly; it also provides evidence against which the reader may compare the conclusions presented in an intelligence report. It should also be noted that certain statistical indicators represent concepts that are very difficult to discuss otherwise. Measures of correlation and association have no verbal counterparts. Similarly, it is impossible to present the information contained in a single percentage table in less than several pages of tedious text.

a. **Statistical Techniques—An Example.** In the example presented above, the intelligence analyst examined financial data on retail and wholesale carpet sales. On the basis of observed increases in retail sales and decreases in wholesale sales, the analyst concluded that carpets from an unknown, possible illegal, source were being sold in local retail stores. The data presented in Tables 4 and 5 show how the analyst was able to reach this conclusion.

The entries in Tables 4 and 5 represent hypothetical sales data for a retail and wholesale carpet industry. Column A shows raw sales volume for each month in 1974. In Column B a seasonal adjustment factor is given that reflects the difference between average sales in a particular month and average monthly sales over an entire year. For example, retail sales in January are normally only 89 percent of the average monthly sales for a year. (If average monthly sales for the year were \$100, the average sales in January would be \$89.) This seasonal adjustment weight allows a businessman to evaluate monthly sales while controlling for seasonal fluctuations above or below average. Column C lists corrected monthly sales. The numbers in this column are the sales volume in Column A divided by the adjustment factor in Column B. This operation yields a figure which is directly comparable to average monthly sales distributed over an entire year. Column D presents expected average sales for each individual month. These figures are derived by multiplying the seasonal adjustment weight by the monthly average given in Column E. If raw sales for each month were exactly equal to average sales for each month then each entry in Column A could be equal to each corresponding entry in Column D, and each entry in Column C would equal the monthly average given in Column E. In dealing with the problem at hand, the analyst is interested in documenting differences between wholesale and retail sales. Since it

TABLE 4
Retail Sales Data

	<u>A</u>	<u>B</u>	<u>C</u>	<u>D</u>	<u>E</u>
	Raw Sales \$ 1974	Seasonal Adjustment	Corrected ¹ Sales \$	Expected ² Sales	Monthly Average ³ 1973
January	57,200	.89	64,300	56,800	63,780
February	68,600	.98	70,000	62,500	
March	54,900	.82	67,000	52,300	
April	47,200	.72	65,600	45,900	
May	52,000	.91	57,100	58,000	
June	71,000	1.09	65,100	69,500	
July	70,200	1.04	67,500	66,300	
August	77,500	1.06	73,100	67,600	
September	75,500	1.07	70,600	68,200	
October	118,700	1.71	69,400	109,100	
November	59,600	.92	64,800	58,700	
December	58,100	.80	72,600	51,000	

¹Corrected Sales = Raw Sales/Seasonal Adjustment

²Expected Sales = Monthly Average 1973 x Seasonal Adjustment

³Calculated by summing over an entire year and dividing by 12

can be seen from Tables 4 and 5 that there are significant monthly variations, these data must be standardized before meaningful comparisons can be made. As discussed in the preceding paragraph, standardization in this case involves comparing observed sales data with expected sales data given seasonal fluctuations. Table 4 indicates that retail sales have been somewhat greater than those expected, given past sales volume as a guide. Table 5 shows that wholesale rug sales have been significantly less than expected. These comparisons are graphically presented in Figures 5 and 6. In each figure, observed sales are taken from Column A and expected sales are taken from Column D in Tables 4 and 5.

It is obvious that there is a wide discrepancy between the apparent supply as indicated by the sale of wholesale and the supply of carpets available to retailers in the area as indicated by their sales. These data support the original complaint by the wholesale dealer, and the analyst intensifies the investigation based on these findings.

b. **Statistical Techniques—A Bibliography.** Introductory works on statistics and quantitative methods are numerous. There is not, however, an extensive body of literature dealing explicitly with quantitative methods useful to law enforcement personnel. The treatments of statistical techniques for use in the social sciences do provide material which is probably closest to that

TABLE 5

Wholesale Sales Data

	<u>A</u>	<u>B</u>	<u>C</u>	<u>D</u>	<u>E</u>
	Raw Sales \$ 1974	Seasonal Adjustment	Corrected ¹ Sales \$	Expected ² Sales	Monthly Average 1974
January	36,300	.82	44,300	36,200	44,140
February	32,000	.72	44,400	31,800	
March	38,000	.91	41,800	40,200	
April	41,300	1.09	37,900	48,100	
May	39,000	1.04	37,500	45,900	
June	39,300	1.06	37,100	46,800	
July	37,000	1.07	34,600	47,200	
August	49,800	1.71	29,100	75,500	
September	26,800	.92	29,100	40,600	
October	22,400	.80	28,000	35,300	
November	28,500	.89	32,000	39,300	
December	21,800	.98	22,200	43,300	

¹Corrected Sales = Raw Sales/Seasonal Adjustment

²Expected Sales = Monthly Average (1973) x Seasonal Adjustment

required by intelligence analysts. Texts on economic analysis and econometrics and those dealing with accounting methods may also be useful in police intelligence; but these books tend to be more difficult as introductory works and more focused toward the specific requirements of those disciplines. A bibliography of statistical texts and less formal handbooks are vehicles for self-instruction while others are designed for classroom use. All of them, however, present concepts and techniques that are very useful in intelligence analysis and are given in the Bibliography.

E. Reporting Intelligence

Once the analyst has reached conclusions, he/she must report findings. These can be short or lengthy, oral

or written. With the exception of quick name checks, the analyst should always provide more than bits of raw information by giving the information some meaning and reporting this, even in an oral report, to an investigator. If the bulk of the reporting of the intelligence unit is nothing but bits of information without analysis, there is little excuse for the expense of analysts, let alone the unit itself. If all a department wants is an ability to check names in a file, then all that is required is a file room, some name files and file clerks, not an intelligence unit.

The format and contents of reports, especially the longer, strategic variety are set by the requirements of the consumers. Where a report is requested by the chief to assist in planning, the requirements would be those indicated by the needs of the planning element. If the

Figure 5. Retail Sales Volume

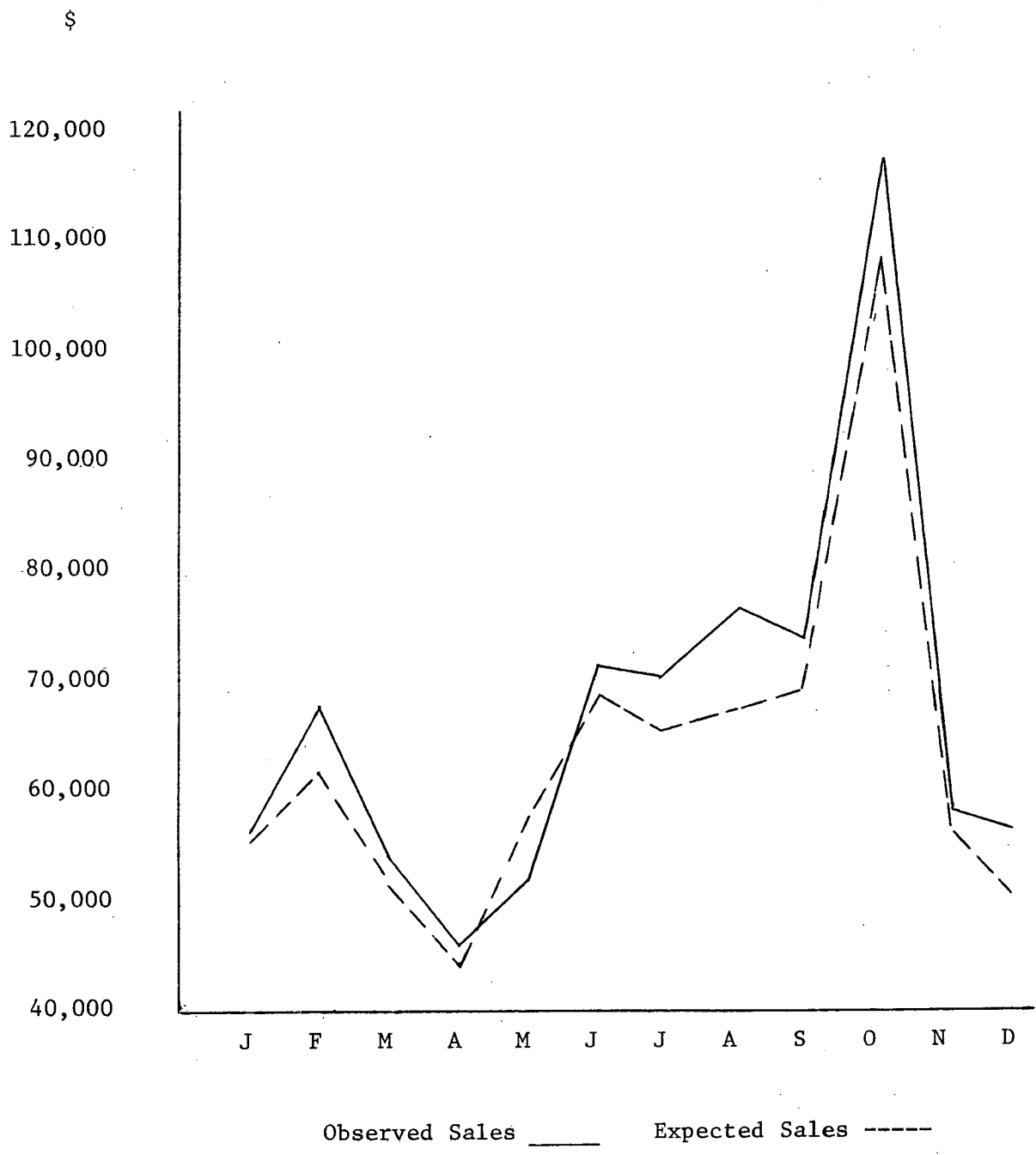
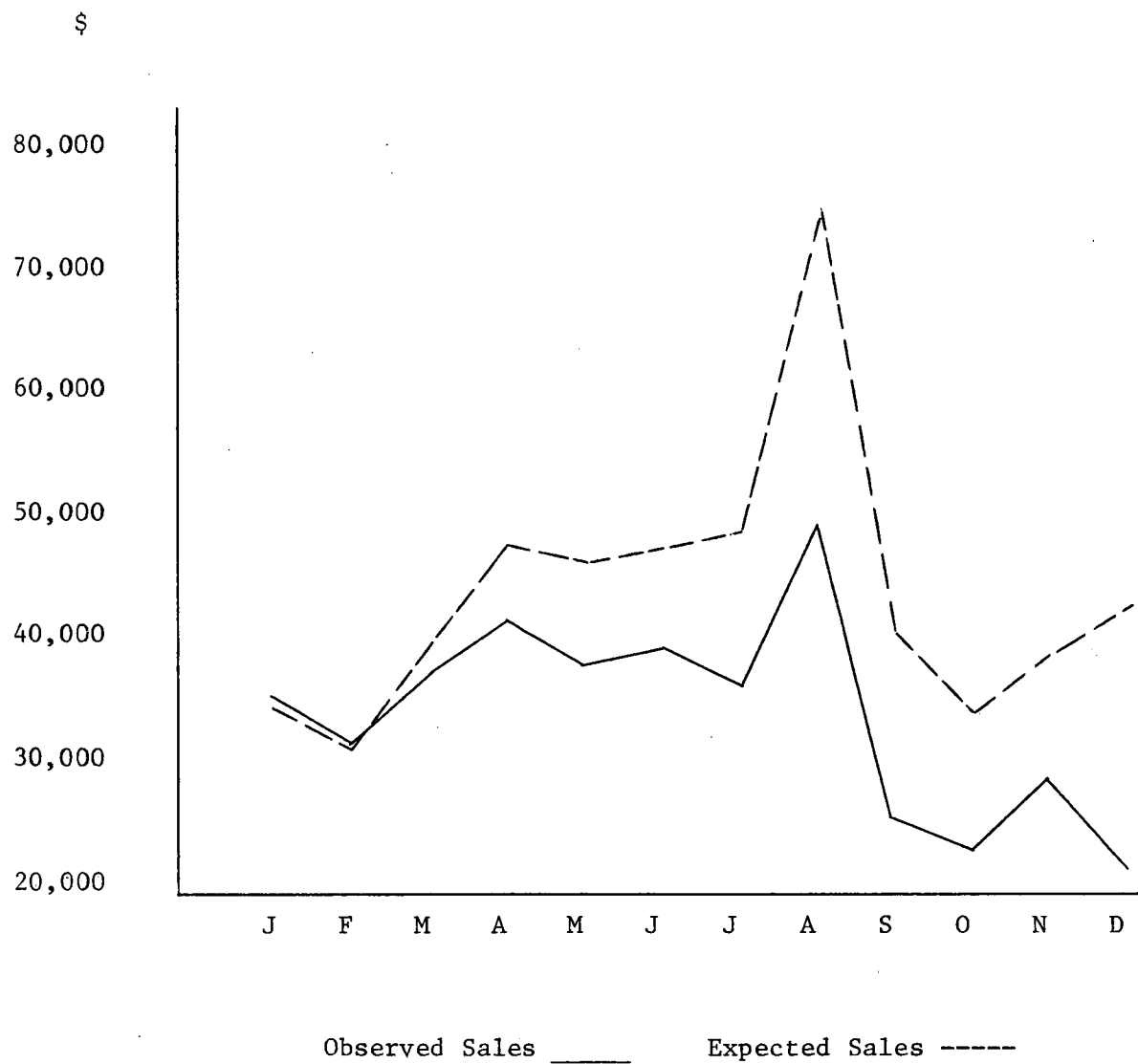


Figure 6. Wholesale Sales Volume



chief wants periodic strategic reports on selected areas and types of criminal activity, he/she will normally indicate what should be covered. Where the report is self-generating by the intelligence units, the format and content should be set by the commander based on judgment and feedback that have been received relative to past efforts.

Wherever possible, the intelligence unit commander should try to have input as to how the intelligence report is presented. One approach is to provide a brief statement in the beginning of the conclusions and recommendations that the chief can read quickly. If he/she is interested, he/she may then ask for an oral briefing on the rest, or simply ask questions. But when this report is sent to the operational units, it should have more extensive material. The investigators will want to know the sources of validity of the information before accepting the hypothesis in the report. Furthermore, they can use help determining what additional information would be needed to develop a case that would result in an arrest.

The suggested format and contents of an intelligence report are as follows:

- **Conclusions.** The conclusion section presents the results of the analysis. It should not be confused with a summary of the facts and allegations on which the conclusions were based. The conclusions answer such questions as: What is the significance of the information? What is the meaning for the department? Is there criminal activity involved? What is the relationship between the subject of the report and other types of areas of criminal activity in the jurisdiction? Is there a case or not?

- **Recommendations.** If the intelligence unit believes there is a case, then it should recommend how to

approach the problem of evidence gathering and case building. If there is no case yet, what should be done? Should the unit continue to gather information? Should the subject be put on the back-burner until other developments occur? Should the assistance of other local or Federal units be requested? Should the case be turned over to a Federal agency? At the time the intelligence unit's report is finished it knows more about the subject than anyone else in the department; hence its views are important.

- **Summary of Information.** This is a synthesis of the most important elements of information without repeating all the details. The details will be in the intelligence files and available when a decision is reached on the next step.

- **Sources and Reliability of Information.** The analyst should give whatever information he/she has on the validity of the information available when the report was drafted. It is difficult for a chief or other readers to appreciate the value of conclusions unless they have some way of judging the reliability of the information basic to the report.

- **Principal and Alternative Hypothesis.** The reader will also be greatly helped if he/she can see the range of hypotheses the analyst considered before choosing the one presented in the conclusions. It is also important to understand explicitly why the analyst chose a particular hypothesis.

- **Missing Information.** This is an essential base upon which the conclusions and recommendations rest. It tells the reader explicitly what further information will be needed if the hypothesis selected is to be proved. It also points out missing information which must be found if a successful enforcement action is to be launched.

APPENDIX G

EVALUATING THE INTELLIGENCE FUNCTION

Evaluation involves the development and application of measures of effectiveness. For a staff function such as intelligence, this poses a particularly difficult problem. An evaluation, to be comprehensive, must include the operation of the intelligence process—collection, collation, analysis, and reporting—and the value of the output to the consumer. No matter how effectively the various activities within the intelligence unit are meshing, unless the output meets the tactical and strategic requirements of the department, the unit is wasting its time.

In evaluating the process, the measures must go beyond simple numbers like the size of files, the number of reports received or issued, or the total man-days spent in reviewing reports. Rather, the commander should think in terms of capability. He/she might test the ability of the system to produce analyses with a minimum of file-search time. The commander might analyze the operation in terms of ability to detect new operations of the organized criminal before they start or before anybody else detects them. This is difficult, but the function of intelligence is to warn of new developments and to suggest areas where the organized criminal might turn next.

The intelligence unit commander needs his/her own measures of effectiveness because his/her responsibility is different from the line commander's. A traffic unit can be judged by how traffic flows. Enforcement units can be judged on the number of arrests, number of convictions, and the trends in crime. But an intelligence unit makes no arrests and acts only to support other units of the department. Therefore, it has no fixed, hard achievements to be judged.

Who should do the evaluation? From one point of view it is difficult for anyone outside the unit to evaluate its operations. Its functions tend to be unique. There is the problem of security of information. It is hard to gain acceptance of the idea that someone from outside the unit would do an evaluation. This would mean non-intelligence personnel being given access to the information in the files, contrary to all training of the unit personnel. On the other hand, it is difficult for the commander to evaluate his/her own operations objectively.

The systems suggested below include several alternatives. Self-evaluation of the unit is discussed. Evaluation

of product by users, who are by definition outside the unit, is also discussed. There are two approaches to evaluation of the functions in the intelligence process. Either could be used by the unit commander, the department's inspection unit, or someone contracted from outside.

Regardless of the approach adopted, the data for evaluation of output must be sought from the users. In seeking user evaluations, the commander must also remember that the users of an intelligence unit's product may be other than elements of its own department. This further complicates the task of evaluation. Hence, there will be a non-intelligence unit input to an overall evaluation of the unit. User participation in evaluation is critical. Intelligence not related to the main problems of crime as defined by the senior officers in the department makes relatively little contribution to the efforts of the department. In those cases where the intelligence unit is pointing to new areas of crime, it will be effective only if the rest of the department gets the message and understands and accepts the requirements posed by the analysis. Intelligence is a staff function. It can only contribute to the line effort if effective communication exists with the key line functions.

A. Evaluation Approach

There are two approaches to evaluation of the intelligence process. One is a formal, collective self-analysis by the members of the unit. The second is a formal evaluation of the performance of the unit in terms of functions. The evaluation of the quality and usefulness of the unit's output is a separate and distinct operation. Both of these should be done on a monthly basis. Since most departments want monthly reports from units, this will provide the intelligence unit commander with data for his/her report.

1. **Monthly Intelligence Unit Self-Analysis.** The commander of the intelligence unit should meet with principal assistants, or better, the whole staff, once a month. At this meeting, 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 crime activities and threats to public order 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?

- If the answer is no, then: Why not? Is analysis failing to keep track of activities of major criminals? Are investigators focused only on low-level operations? What developments have been learned from outside agencies? Have they been followed up?

- Are there reports or rumors of organized crime activities or other subversive elements that the unit itself has no other information about? What has been done to check out the rumors?

- What developments in major 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 persons on patrol, 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 to 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 should be reviewed at the following meeting to see that action has been taken.

2. Monthly Evaluation of the Intelligence Process. The systematic evaluation of the effectiveness of any function is a normal task of management. But since most functions are made up of more than one task, the first step should be to define the several tasks or elements that go to make up the function.

The approach to definition can be at two levels. The first is to state certain elements in a generic sense, assuming that no matter how small or large the unit, these elements of the function must be present. Two systems of numerical evaluation are suggested.

A second approach is to focus on the specific tasks assigned to personnel in the unit. Once the elements of a function are defined, the person assigned to that element or task can be evaluated in specific terms. The final step in the process is to compare what is accomplished with the assigned objective or goal. It is not enough that tasks are performed efficiently; they must achieve the objectives set or the operation is partially or wholly ineffectual.

3. Monthly User Evaluation of Intelligence Unit Output. It is critical that the intelligence unit commander know specifically and formally how the user and enforcement units view his/her activities. Are they useful and contributory or is little attention paid to them? Often if the question is not asked directly, the answer will be a perfunctory "sure-sure, the intelligence output is great." The commander needs to know which output is great and why and that which is not. A generalized statement is almost worthless. An approach using questionnaires is shown below. One questionnaire is designed for major reports; the other for questioning users of intelligence.

B. Proposed Numeric Evaluation System

The first approach is based on assigning numerical values to the function of the intelligence process. A measure of how well each function is being performed is established by applying an effectiveness value. An overall value for the operation of the unit can be achieved by adding the scores for the functions. This also provides a basis for comparing the operation of one unit at different time periods, or several units in the same time frame.

The suggested approach is based on one or more persons evaluating the intelligence process in terms of questions relating to major elements of the functions. It should be understood that the questions and their suggested values are examples only. A unit commander, after initiating this approach, should review the questions and their relative values in terms of the particular organization and specific tasks as assigned by the chief. If the questions are never changed there is considerable danger that the utility of the evaluation will be reduced as the units focus changes and people become familiar with the questionnaire items.

The numeric values are applied as shown below. On the basis that each function is essential to the process,

the approach is based on an evaluation in which each of the functions is assigned a value of 100, as follows:

- Collection/flow of information 100
- Processing/collation of information files 100
- Analysis 100
- Production/dissemination of reports 100
- Management procedures 100

Each function is then subdivided into elements to which is assigned, on a weighted basis, a portion of the total value of the function. The weighting is based on a judgment of the worth of each element relative to the effective accomplishment of the total function. Those weightings can be manipulated by a unit commander to direct the attention of the staff to critical areas where improvement is desired.

The delineation of elements of functions and the assignment of values is as follows:

1. Collection

- | | |
|---|----|
| A. Intelligence unit receives as part of normal flow of information, copies of all (the bulk of) investigator reports (except in large units where reports relating to known or suspected persons associated with organized crime and major criminal activity would be adequate). | 30 |
| B. Intelligence unit has its own investigators or can task the department's investigative unit to probe areas determined to be important as a result of the intelligence unit's assessment. A procedure exists for the tasking of non-intelligence unit personnel on the basis of agreement between the intelligence and operational unit commanders or orders of the department chief. | 25 |
| C. Department has operating an effective procedure whereby the officer on patrol can report on specified subjects directly to the intelligence unit. | 20 |
| D. Intelligence unit receives (or at least records information contained in) sensitive reports from undercover units, informants, or other specialized sources. | 15 |
| E. Intelligence unit has a plan of action to gain information from other law enforcement agencies—local in area, state, and Federal. | 10 |

TOTAL	100
-------	-----

2. Processing/Collation

- | | |
|---|----|
| A. Information, once filed, can be quickly and correctly retrieved. | 30 |
| B. The information filing system has a capability to focus data received by major crime figures, area/location, type of crime, and other subjects that the analyst finds useful. | 30 |
| C. Unit has an information flow system that causes reports to be reviewed, distributed, and earmarked for filing in a manner that ensures the analyst (or other person responsible for performing analyst function) reads important reports relating to his/her area of responsibility. | 25 |
| D. There is an efficient and effectively operating system for updating biographies (abstracts or biographic forms) of known or suspected major criminals in the area (not necessarily restricted to persons residing within the boundaries of the jurisdiction). | 25 |

E. There is an operational plan for purging the files of outdated and non-pertinent material.	10
TOTAL	<u>100</u>
3. Analysis	
A. The intelligence unit has one or more persons tasked to analyze information received to develop/project/estimate	50
- patterns of organized crime by type of crime,	
- patterns of association among persons believed to be part of organized crime,	
- interrelationships among criminals and types of organized crimes in which they are suspected of being involved.	
B. The intelligence unit has a procedure whereby the person or persons responsible for analysis are available to assist departmental investigators, in person or by phone, by applying information in the intelligence file and his or her own expertise to a current investigation.	50
TOTAL	<u>100</u>
4. Production/Dissemination	
A. The intelligence unit is responsive to requirements of on-going investigations, including having a procedure to keep its members aware of major cases.	40
B. The intelligence unit produces periodically and/or on order reports on major trends in criminal activity in its jurisdiction, emphasizing new or developing types of organized crime activities.	30
C. Intelligence reports are disseminated as widely as possible within limits set by need-to-know and sensitivity of information (the rule should be positive, giving the benefit of dissemination to those who need and can use the information).	30
TOTAL	<u>100</u>
5. Management Procedures	
A. The intelligence unit has a procedure for obtaining the reactions of consumers to its products.	25
B. The intelligence unit has a collection plan to assist it in focusing its efforts on the most important of the crime problems. The plan is periodically updated (monthly) and is coordinated with the chief of investigations and approved by the department head.	20
C. There is an element in the department's training program to prepare personnel for the specialized activities of the intelligence unit, especially analysis and intelligence investigation.	20

D. Security guidelines are in existence and observed, especially in limiting access to the files to analysts and file clerks, distributing intelligence reports only to those with a need-to-know within the organization and only to other law enforcement agencies on the outside with whom there is an agreement for the protection of the intelligence material. 20

E. There is a procedure for evaluation of the effectiveness of the intelligence unit's operation. 15

TOTAL 100

In evaluating performance, each element will be graded in terms of the following scale:

- 1. The element is being implemented effectively. 1 (or full value)
- 2. The unit is organized to accomplish the element but the operation is only partially effective. .80/.70/.60
- 3. The unit is in the process of organizing to accomplish the element but is not yet operational. .50
- 4. The unit has organized to accomplish the element but the operation is ineffective. .30
- 5. The unit has not/does not recognize the requirement to accomplish the element. 0 (lose full value)

As an example of how this system would operate, the following is given as "Unit X is being evaluated, the production/dissemination element is scored as follows:"

- A. The intelligence unit is responsive to investigations including having a procedure to keep its members aware of major cases. (The evaluator found there was no procedure to keep its members aware of major cases. Thus, he gave the unit only 60% of the total value for this item.) 40 x .60 24
- B. The intelligence unit produces periodically and/or on order reports on major trends in criminal activity in its jurisdiction, emphasizing new or developing types of organized crime activities. (The evaluator, after reviewing reports, finds no emphasis on new and developing organized criminal activity. However, the unit SOP calls for such emphasis. Thus, he gives the unit only 30% of this value.) 30 x .30 9
- C. Intelligence reports are disseminated as widely as possible within limits set by need to know and sensitivity of dissemination (the rule should be positive, giving the benefit of dissemination to those who need and can use the information. The evaluator finds unit stresses dissemination, believing useful intelligence information must be made available. Thus, he gives the unit full value.) 30 x 1.00 30

TOTAL 63

The value given to this element by the evaluator is 63 of a possible 100. The evaluator would do the other elements in a similar manner and then come out with a total value for the unit. If this were done periodically, as suggested, weaknesses in the operation would be clearly defined. Corrective actions could be taken and subsequently evaluated also. The overall score could be used to establish a trend line which could be used to compare different intelligence units.

C. Proposed Seven-Value Approach to Evaluation of an Intelligence Unit

This is an alternative to the strictly numerical value system above. The same questions are used for each element. But for some it is difficult to translate a

conclusion about the performance of a function which cannot be defined with precision into a specific numerical statement. What is suggested below is an evaluation which in seven values covers a full range from good to bad, all the way from performing the element of the function properly to not performing it at all. The evaluator only needs to check which space, whether toward effective performance or toward noncompliance, is closest to the operation of the unit as he/she perceives it.

In establishing a total score, the system scorer can number the spaces 1 to 7 using plus 1 to 3 on one side, minus 1 to 3 on the other side, and 0 in the center. Or, in consortium with the unit commander, the scorer can assign weighted values. The evaluator does not have to be concerned with the summing process and needs only to indicate, by a check mark, a rating of the process.

1. Collection

The intelligence unit should receive as part of the normal flow of information copies of all relevant investigator reports. The intelligence unit should have its own investigators or be able to task the department investigative unit for the collection of information in the field according to requirements. Procedures should exist for the tasking of non-intelligence unit personnel based on agreements between intelligence and operational unit commanders, or on the orders of the department chief. The department should have effective procedures whereby patrol officers regularly report on specified subjects directly to the intelligence unit. The intelligence unit should either receive sensitive reports from undercover units, informants, or other specialized sources or be notified of the acquisition of sensitive material. The intelligence unit must be able to receive information from Federal, state, and other local areas through routine procedures.

A. Intelligence unit receives all relevant reports from investigators	- - - - -	Intelligence unit seldom receives investigative reports
B. Investigative support is always available as required	- - - - -	Direct investigative support is not regularly available
C. Reports regularly submitted by patrol personnel	- - - - -	Reports seldom submitted by patrol personnel
D. Unit receives/is notified of all sensitive reports	- - - - -	Unit is not notified of sensitive reports
E. Information from other law enforcement agencies is routinely available	- - - - -	Information from other law enforcement agencies is not routinely available

2. Processing/Collection

Information in the central filing system should be quickly and readily retrievable. The information filing system should be able to categorize data by major crime figures, general area, address, type of crime, type of business, and other subjects as needed by the analyst. The system of information flow should ensure that all analysts are advised of all reports relating to their area of responsibility. There should be a rapid, efficient system for updating biographic or other major files. There should be an operational plan for regularly purging the files of material which is outdated, irrelevant, or seldom used.

A. Information is rapidly retrievable from files	-----	Retrieval of information is cumbersome
B. Files are extensively cross-indexed according to analysts' needs	-----	Files indexed only by name or case; few cross references
C. Incoming reports routed to appropriate analyst for review before filing	-----	Incoming reports filed upon receipt without analyst review
D. Biographic and activity files systematically updated upon receipt of new information	-----	Biographic and activity files neither systematically reviewed nor updated
E. Files regularly and systematically purged	-----	No system for regular purging of files

3. Analysis

The intelligence unit must have one or more persons specifically tasked to analyze information from investigative, patrol, and other sources. Analysts should have no enforcement duties and few, if any, responsibilities for field investigation. The analysis section should be capable of providing strategic assessments and estimates of trends in criminal activity. The section must also be able to provide tactical support to departmental investigators in specific case-related operations.

A. Intelligence unit personnel specifically designated for function as analysts	-----	Intelligence unit has no analysts
B. Analysis section is free of enforcement and field investigator's responsibilities	-----	Analysts are tasked for enforcement and other operational duties
C. Analysis section has resources and expertise to produce strategic intelligence	-----	Analysis section does not produce strategic intelligence
D. Analysts routinely provide tactical assessments to operations personnel	-----	Intelligence unit does not produce tactical assessments
E. Analysts are largely free of clerical responsibilities	-----	Analysts function as file clerks exclusively

4. Production/Dissemination

The intelligence unit should be responsive to the requirements of investigators involved in ongoing cases, producing oral or written reports in support of operations personnel. The intelligence unit should produce, independently or upon request, reports on major trends in criminal activity in its jurisdiction, emphasizing new or developing types of organized crime activities. Reports by the intelligence unit should be disseminated as widely as possible within the limits prescribed by the need-to-know and the sensitivity of the information.

A. Unit is able to provide reports to operations personnel upon request	-----	Unit is not able to respond directly to request by operations personnel
B. Intelligence unit produces strategic reports on trends in organized crime activity	-----	Not capable of producing strategic intelligence reports
C. Unit disseminates reports to all criminal justice agencies concerned	-----	Products of intelligence are largely retained in-house
D. As necessary, unit alerts other jurisdictions of relevant data, findings	-----	Intelligence unit seldom shares intelligence information with other concerned jurisdictions

5. Management Procedures

The intelligence unit should formulate rigorously observed security regulations and guidelines regarding the collection, storage, and dissemination of intelligence information within the unit and to other law enforcement agencies. There should be an intelligence training program directed at developing the specialized skills of intelligence division personnel, particularly intelligence investigators and analysts. The intelligence unit should utilize a collection plan to assist in focusing its efforts on the most important crime problems. The plan should be periodically updated and developed in cooperation with the chief of the investigation division. There should be procedures for evaluating the effectiveness of the intelligence unit, and for determining the reactions of the consumers of intelligence reports.

A. Clear, comprehensive security guidelines are established and observed	-----	No clear cut security guidelines exist
B. Intelligence unit supported by thorough up-to-date training program	-----	Training program for intelligence is ineffective or non-existent
C. Intelligence unit effectively utilizes and periodically updates collection plan	-----	Collection plan not used; collection activities haphazard, ill-defined
D. Intelligence unit conducts regular evaluation of intelligence functions	-----	Evaluation conducted irregularly, using unclear criteria of effective performance

E. Intelligence unit regularly solicits evaluation from intelligence consumers	- - - - -	Unit makes no effort to obtain inputs from intelligence consumers
--	-----------	---

F. Intelligence unit chief effectively monitors activities/performance of analysts and investigators	- - - - -	Intelligence unit chief has only vague idea of analyst, investigator activities
--	-----------	---

6. Guidelines for Intelligence Operations

Each unit should establish clear, up-to-date guidelines regarding the collection and storage of intelligence data which reflect local, state, or Federal privacy and civil liberties legislation. These guidelines must specify conditions under which information will be sought on suspects and rules regarding the retention of information in intelligence files.

A. Current, explicit guidelines exist regarding collection of information	- - - - -	No guidelines exist; guidelines are not systematically updated
---	-----------	--

B. Guidelines exist regarding storage of information	- - - - -	No guidelines exist; guidelines are not systematically updated
--	-----------	--

C. Files are regularly reviewed to purge unproven, unjustified information	- - - - -	Unproven, unjustified information not systematically reviewed or purged
--	-----------	---

D. Evaluation of an Intelligence Unit by Establishing a Value for the Individual Member of the Unit, Relative to Task to Which the Person Is Assigned

A more specific approach to evaluating the operation of an intelligence unit is to focus on the activities of the individual members of the staff. Because the several functions to be performed must mesh if the unit is to be effective, it is essential that the unit commander have some means to find out how well the staff is doing. This can only be done by systematically reviewing each staff member's performance.

If the unit is small, the unit commander will have to perform the whole evaluation. If there is more than one level of supervision, each level will evaluate the activities of its personnel. The lower echelons of supervisors might check their personnel on a monthly basis; the senior supervisors, including the unit commander, might evaluate on a quarterly basis.

While the approach may seem like "overkill," it is important to understand that the intelligence unit stands

or falls on the effectiveness with which it performs each of its functions. Is the investigator focusing his/her efforts or wasting time? Mistakes in filing can subsequently reduce the overall contribution of the unit. The analyst's grasp of the information available must be assessed. Is he/she getting the most out of it? Does he/she see the patterns that are there? Does the analyst know the principal criminals in the area? Is he/she indexing reports properly, especially in terms of criminal activity?

Finally, it is important that the evaluation approach be a two-way street. This gives the person being evaluated a chance to correct errors and to question the procedures, systems, and assignments that make up his/her duties.

The suggested approach is based on the seven-value system. The evaluation is based on the detailed statements of the specific tasks that must be performed to accomplish each major function in the intelligence unit—investigation, analysis, liaison, and filing. These are given in the following figures.

FIGURE 1

DEFINITION OF MAJOR TASKS TO BE PERFORMED BY AN INTELLIGENCE INVESTIGATOR

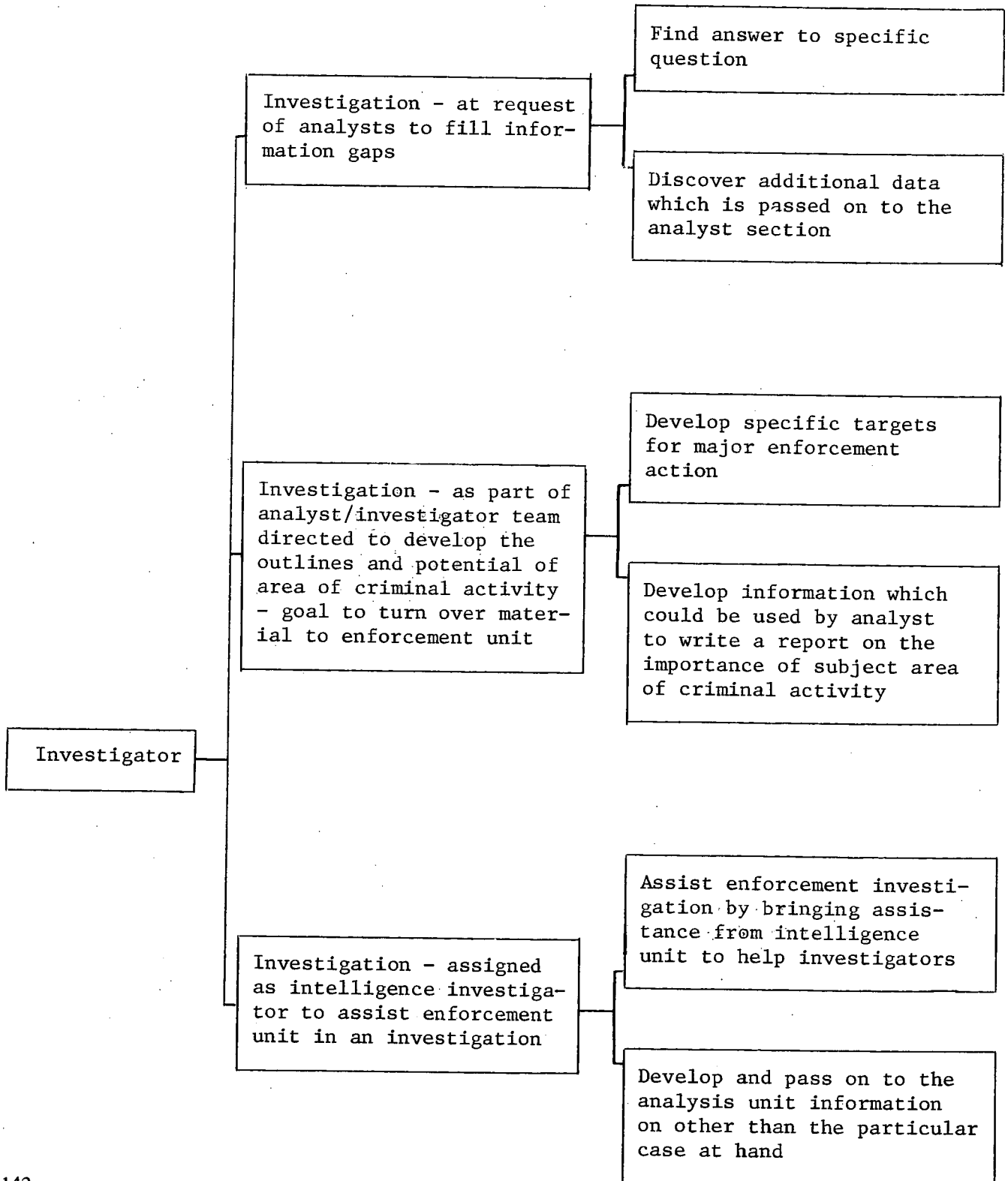


FIGURE 2

DEFINITION OF MAJOR TASKS TO BE PERFORMED BY AN ANALYST

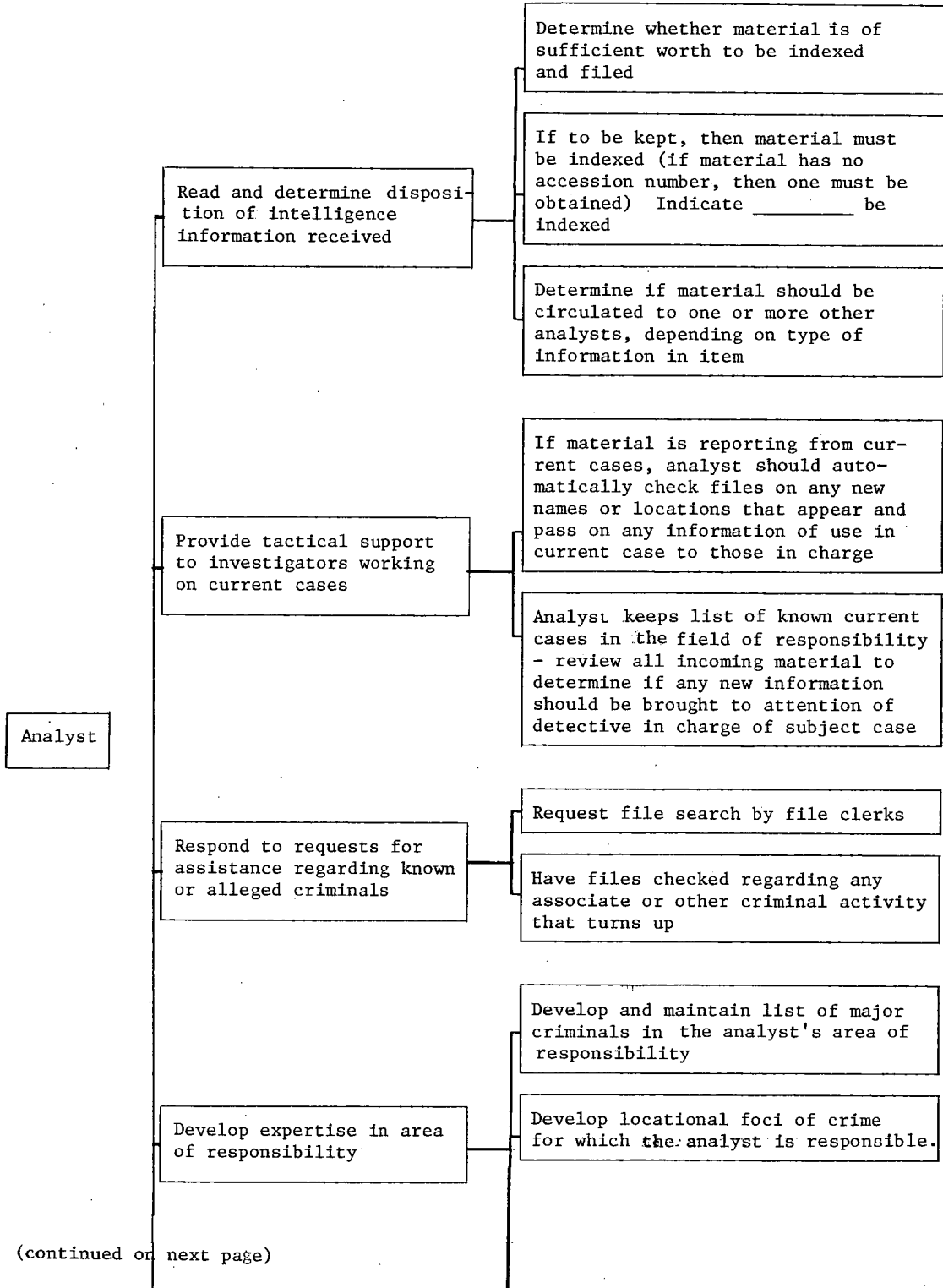


FIGURE 2 (Continued)

DEFINITION OF MAJOR TASKS TO BE PERFORMED BY AN ANALYST

(continued from preceding page)

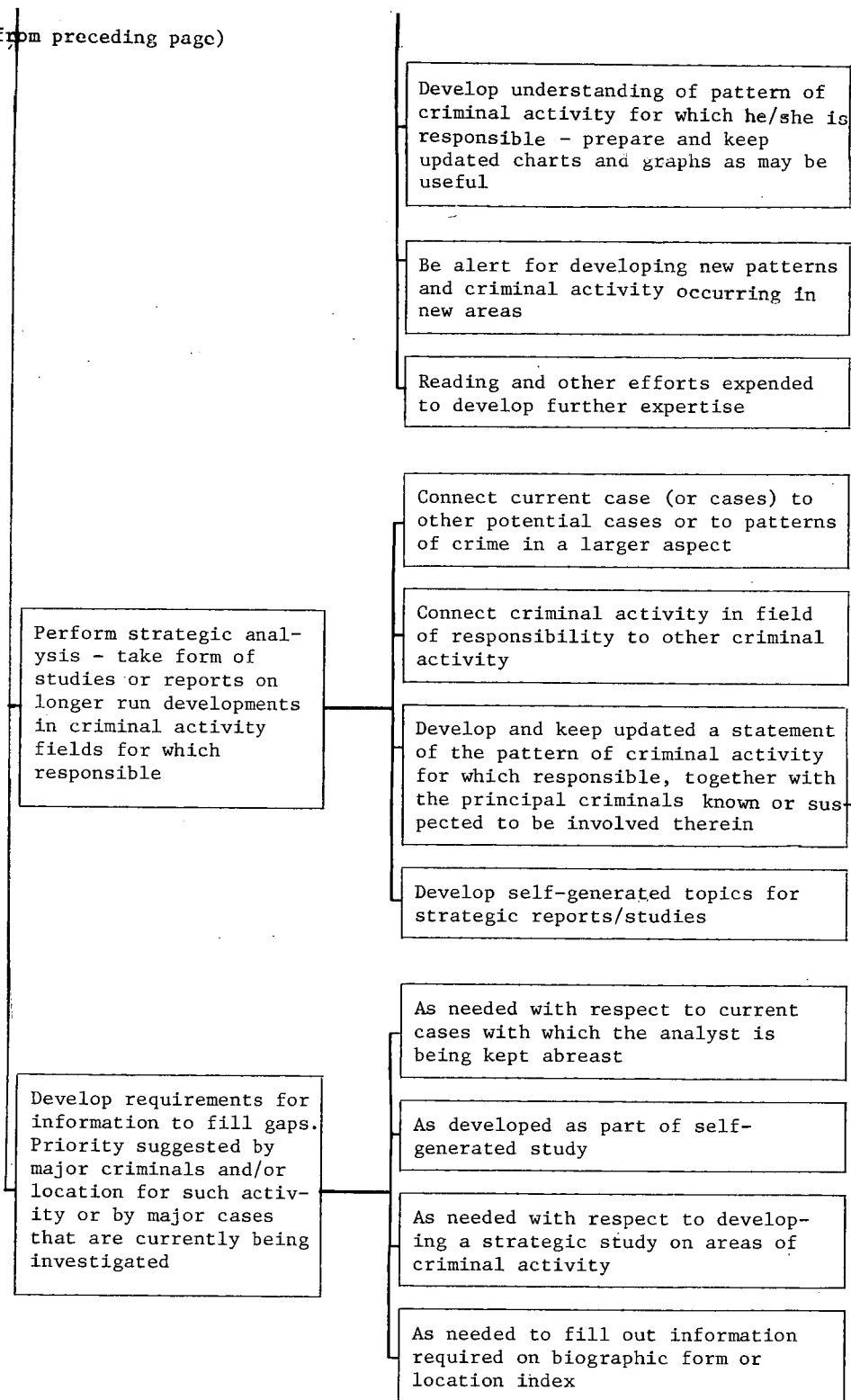


FIGURE 3

DEFINITION OF TASKS
TO BE PERFORMED BY A LIAISON OFFICER

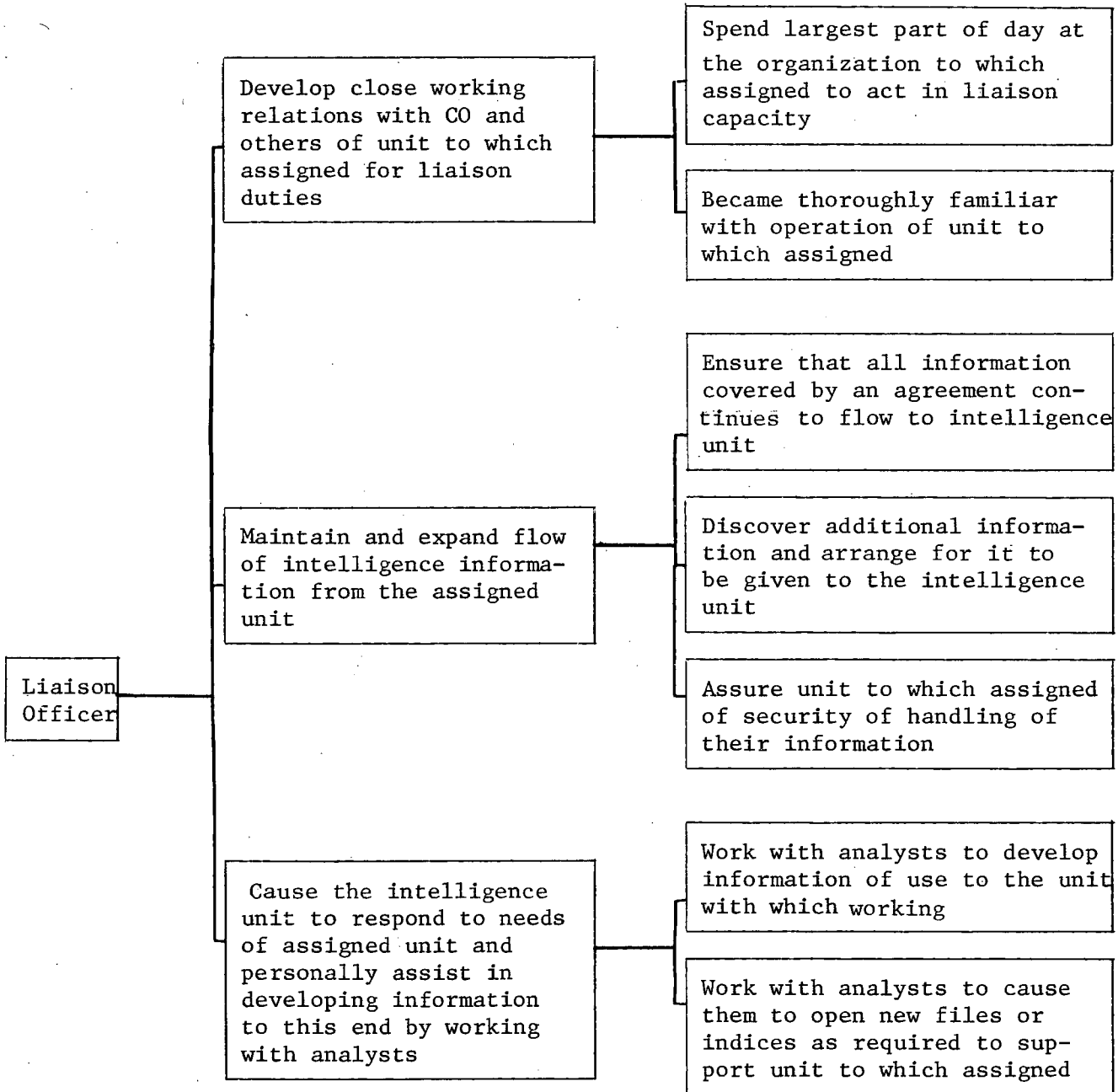
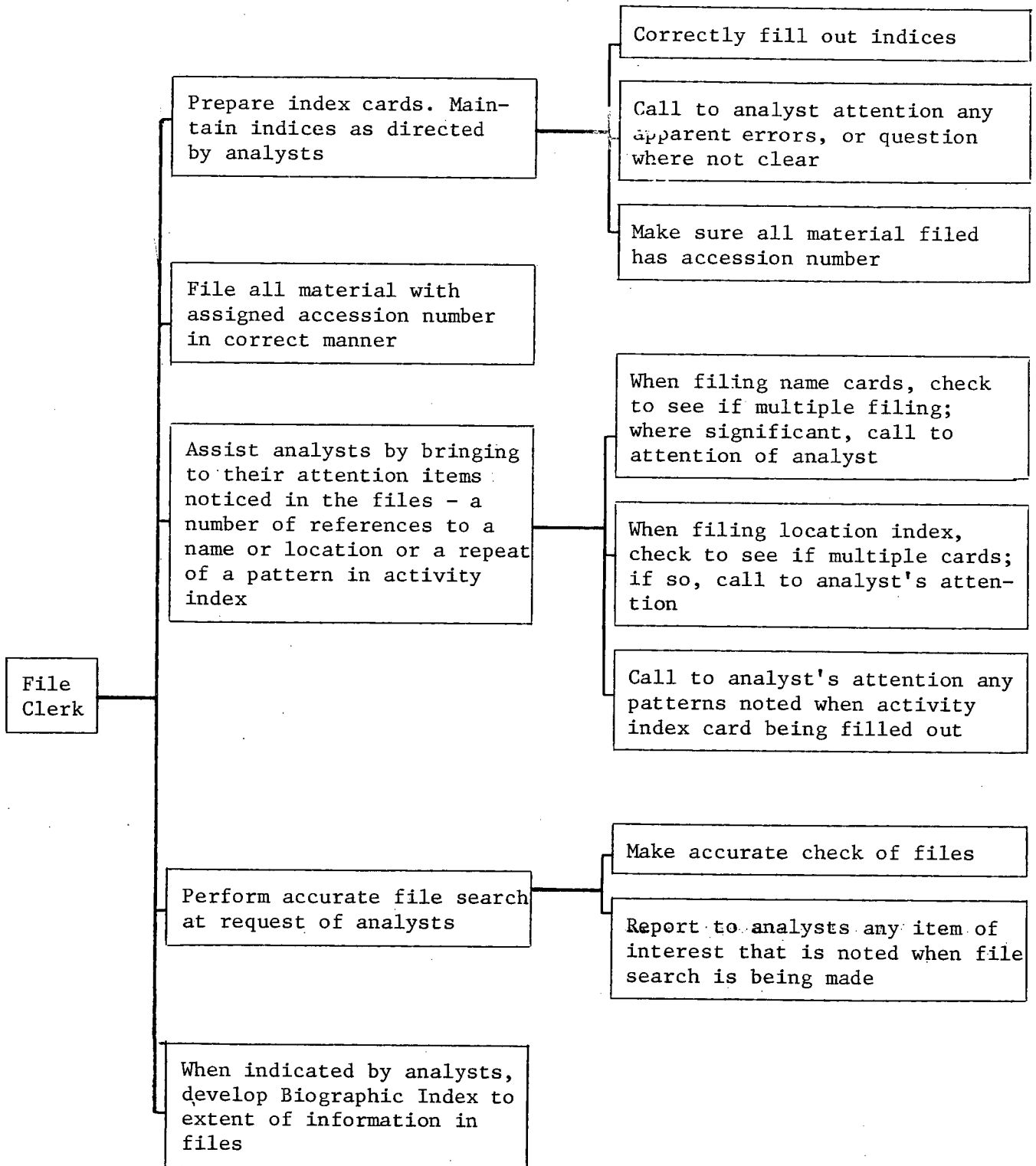


FIGURE 4
DEFINITION OF MAJOR TASKS
TO BE PERFORMED BY A FILE CLERK



As exemplified on the following pages, the principal activities of the analyst and investigator are then subdivided into specific actions. Each of these actions is graded on a seven-value scale of good to bad. A similar

seven-value scale can readily be developed for other functions assigned to an intelligence unit. What is given is an example of an approach to evaluation of personnel.

1. INTELLIGENCE INVESTIGATOR

a. Satisfying Requirements for Intelligence Information

The principal duty of the intelligence investigator is to provide information from field investigations in response to information requirements identified in cooperation with intelligence analysts. The investigator should thoroughly understand the requirements of the analyst and provide accurate, responsive information that answers the questions posed as completely as possible. More generally, the field investigator should understand the differences between enforcement investigation and the intelligence investigation and this understanding should be reflected in the information provided.

A. Information supplied is always responsive to analysts' requests	-----	Information is seldom responsive to analysts' requests
B. Investigator is usually successful in satisfying information requirement	-----	Investigator is seldom successful in satisfying information requirement
C. Works closely with analysts to fully understand requirements	-----	Makes little effort to clarify requirement of analyst
D. Fully understands and follows guidelines for intelligence investigation	-----	Does not understand differences between intelligence and enforcement investigation
E. Always observes departmental guidelines for collection of intelligence information	-----	Consistently violates departmental guidelines for collection of intelligence information

b. Flow of Intelligence Information

The investigator, when not acting to fulfill a specific request for information, should provide a steady flow of information into the intelligence units in response to general requirements identified in the units' collection plan. Whenever possible, field observations should be submitted in writing on the appropriate forms. The investigator is responsible for filing daily reports of his/her activities and observations to further ensure a continual flow of information into the unit. The investigator should encourage patrol personnel to submit field observation reports of unusual activities of interest to the intelligence unit and, when necessary, should debrief patrol personnel in accordance with the specifications of analysts.

A. Provides continual flow of information into intelligence unit	-----	Erratically provides information for intelligence
B. Seeks information in accordance with collection plan	-----	Seeks odd bits of information or none at all unless specifically tasked

C. Always submits written reports in proper format	-----	Submits oral reports, seldom written
D. Maintains close contact with patrol officers, soliciting field observation reports	-----	Does not cultivate patrol officers as sources of intelligence information
E. Seeks out sources for debriefing on own initiative	-----	Conducts debriefing only when directed by analyst
F. In general, strives to exploit all possible sources of information by direction and independently	-----	Exerts only that effort necessary to minimally comply with request
G. Submits detailed daily reports of activities and observations	-----	Inadequately documents daily activities and observations

c. Work Habits and Development of Personal Expertise

The intelligence investigator should keep detailed personal records of his/her investigative activities. These should pay particular attention to current cases, including both productive and unproductive sources of information. Investigative activities in general and field work in particular should be carefully planned and organized. The investigator should be flexible with regard to techniques of investigation and adaptive to the particular requirements of intelligence work. The intelligence investigator must pay particular attention to detail in his/her field work and reporting, to include explicit evaluations of the reliability of his/her information sources and the validity of each piece of information provided. He/she should strive to maintain cooperative relationships with operational and other intelligence investigator analysts, and patrol personnel.

A. Maintains accurate, detailed records of field activities	-----	Records of field activities spotty and inconsistent
B. Always plans field work making most efficient use of time	-----	Seldom plans field activities resulting in inefficient use of time
C. Adaptable to many different investigative situations as required	-----	Bound to rigid investigative techniques which are often inappropriate
D. Makes most effective use of informers as possible	-----	Makes ineffective use of informers, using them too much or too little
E. Conducts careful, meticulous investigations, paying attention to detail	-----	Conducts erratic haphazard investigations of inconsistent quality
F. Accurately estimates reliability and validity of sources and information	-----	Inconsistently evaluates sources and information; evaluations are often in error

G. Maintains effective, cooperative relationship with enforcement and other intelligence personnel

Has difficulty working effectively with others and in maintaining cooperative working relationships

2. INTELLIGENCE ANALYST

a. Reading and Indexing Incoming Reports and Other Materials

The analyst is responsible for reviewing all reports and other materials that are routed to him/her by file room personnel, other analysts, and from sources outside the unit. All potentially useful material is properly marked for indexing by file personnel and routed to other analysts as necessary. If in doubt about the usefulness of information, the analyst should seek the opinions of others in the unit before indexing or discarding a particular item.

A. Exercises excellent judgment in reviewing incoming material for retention

Exercises poor judgment; retaining too much or too little

B. Follows department guidelines in selecting reports for retention

Does not appear to be cognizant of department guidelines

C. Reports are accurately indexed according to current requirements

Indexing is haphazard and not consistent with current guidelines

D. Other analysts are always aware of reports relating to their areas of interest/responsibility

Ignores the requirements and interests of other analysts

E. Seeks advice when in doubt about retention, indexing

Exercises poor judgment; never consults with other analysts

b. Identifying Information Requirements

The analyst is responsible for identifying requirements for further information that will aid the unit as a whole and his/her particular area of responsibility. Priorities should be developed for specific requirements and they should reflect the relative cost of collection as well as the expected utility of the new information. As required, the analyst is expected to participate in the development of a formal collection plan.

A. Actively seeks and requests information related to responsibilities

Never seeks information beyond incoming reports

B. Identifies specific requirements and knows in advance how information will be utilized

Identifies vague categories of information and is unsure how it will be utilized

C. Recognizes the high cost of collection; requests only information which will be useful	- - - - -	Does not consider the cost of collection; requests trivial information, marginally useful
D. Contributes to development of formal unit collection plan	- - - - -	Provides no useful input to development of formal collection plan

c. Tactical Assessment

The analyst is expected to provide tactical support to operations personnel in ongoing cases. Responses to specific requests for information should be timely and they should be specifically directed toward satisfying the particular requirement. Responses to requests for analysis should, to the extent practical, address only the immediate requirements of the investigation. The analyst should keep up-to-date records of the current cases in his/her field of responsibility and periodically review those materials, notifying, on his/her own initiative, the responsible investigators of new information relating to their cases.

A. Provides timely response to requests for assessments	- - - - -	Responses to requests are slow, out-of-date
B. Information provided is completely responsive to requirement	- - - - -	Information provided has little or no relationship to that requested
C. Analysis provided is directly addressed to requirements	- - - - -	Analysis provided is not responsive to requirements
D. Analyst notifies investigators of new information relating to their cases	- - - - -	Analyst does not maintain records on current cases in the area
E. Analyst makes concerted effort to remain aware of investigators' current activities, info requirements	- - - - -	Does not exercise independent effort to ascertain investigators' activities, info requirements
F. In general, produces thorough, high quality tactical assessments	- - - - -	Produces sloppy, inconsistent tactical assessments of little utility

d. Development of Personal Expertise and Knowledge of Analytic Techniques

The analyst should continually seek to improve the performance of his/her assigned duties by becoming familiar with techniques of analysis that have proven useful in police intelligence and by becoming increasingly knowledgeable about criminal activities and investigative techniques relating to his/her area of responsibility. The personal work habits of the analyst should reflect the systematic organization that characterizes research and analytic techniques. The analyst should continually strive to maintain excellent professional working relationships with intelligence and other investigators, liaison personnel, file control personnel, and others whose cooperation and goodwill are required for the successful production of intelligence.

A. Analyst is expert in the use of analytic techniques utilized in police intelligence	-----	Analyst is not familiar with analytic techniques
B. Analyst maintains personal files of criminal activity relating to his/her own area of responsibility	-----	Analyst relies solely on central files for maintaining information in a criminal area
C. Analyst educates self with respect to new techniques and new criminal information	-----	Analyst does not independently seek new information on new techniques or criminal activity
D. Analyst's work is characterized by systematic disciplined inquiry	-----	Analyst has inconsistent haphazard work habits
E. Analyst is up-to-date on reading and indexing responsibilities	-----	Analyst regularly allows reports to accumulate before reading
F. Analyst always follows current departmental and unit procedures	-----	Analyst seldom follows departmental and unit procedures
G. Works to maintain cooperative relationships with intelligence and other personnel	-----	Has difficulty in maintaining cooperative relationships with intelligence and other personnel
H. Always observes departmental guidelines on collection and retention of information	-----	Does not appear to be aware of departmental guidelines on collecting and retention of information

e. Production of Intelligence Reports

Intelligence reports should be written in the format prescribed by the intelligence unit. Characteristics common to all reports are a focused presentation which calls particular attention to the findings and recommendations of the reports and sufficient documentation to enable the reader to evaluate the validity of evidence, assumptions, and conclusions. The analyst must possess good basic writing skills and become accustomed to producing reports that are well-organized and largely free of grammatical errors, colloquialisms, and spelling errors.

A. Analyst consistently produces reports that are generally well-written	-----	Analyst does not write well, and cannot express well in writing
B. Reports are terse, but convey all necessary information	-----	Reports are too wordy or too brief, omitting important information

C. Reports consistently conform to prescribed format

Reports consistently at odds with prescribed format

E. Evaluation of the Intelligence Unit by the User

As discussed above, the intelligence unit must be evaluated from two perspectives in order to achieve a whole view. One aspect covered in Sections B and D is the evaluation of the functions in the intelligence process. This can be in terms of specific elements of each function and of task performance by members of the intelligence staff.

The second aspect is that of the quality of the intelligence unit's output. This can only be judged by users. Unless the intelligence, whether tactical or strategic, assists the user in his/her efforts, the system has failed. In planning for this aspect of evaluation it should

be kept in mind that the "user" is not a single element of the department. It includes the chief, the investigative units, and the planning element. It also includes other departments when assistance has been requested and given.

To perform this phase of evaluation, the intelligence unit must develop some means to go to the user. The request for evaluation must be formal, but at the same time short enough in compass and in simplicity of content so that the burden of the effort will cause the evaluation not to be done. Following are two suggested forms. One should be attached to every longer report done by the unit. The other is a monthly evaluation form that should be sent to all principal user units, both within and outside the department.

EVALUATION OF INTELLIGENCE REPORTS

In order to insure that operational and administrative personnel are provided with useful intelligence products, we are requesting that the primary consumers of the attached report complete this questionnaire and return it to the Intelligence Section. Please answer all questions by placing an "X" next to the appropriate response(s). If none of the responses provided is appropriate, feel free to answer any of the questions in your own words.

- | | |
|---|---|
| <p>1) Was this report requested by you or your unit?
 <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>2) Is this report responsive to your current requirements for intelligence?
 <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>3) The principal value of this report has been its contribution to your understanding of: (Mark one or more)</p> <ul style="list-style-type: none"> <input type="checkbox"/> Activities of a specific criminal or groups of criminals <input type="checkbox"/> Criminal activity associated with a place of business <input type="checkbox"/> Criminal activity in a geographic area <input type="checkbox"/> M.O. of a criminal <input type="checkbox"/> M.O. within a racket <input type="checkbox"/> Relationship among criminals <input type="checkbox"/> Relationships among rackets <input type="checkbox"/> Other _____ <p>_____</p> <p>_____</p> <p>4) What actions have you taken as a result of this report? (Mark one or more)</p> <ul style="list-style-type: none"> <input type="checkbox"/> Adjust priorities <input type="checkbox"/> Investigation initiated/increased <input type="checkbox"/> Warrant/Subpoena <input type="checkbox"/> Arrest <input type="checkbox"/> Case dropped <input type="checkbox"/> Other _____ <p>_____</p> <p>_____</p> <p><input type="checkbox"/> None</p> <p>5) Please estimate your confidence in the <i>factual information</i> presented in this report.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Certainly true <input type="checkbox"/> Probably true <input type="checkbox"/> Probably false <input type="checkbox"/> Certainly false <input type="checkbox"/> Not sure | <p>6) Please estimate your confidence in the validity of this report as a whole.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Certainly true <input type="checkbox"/> Probably true <input type="checkbox"/> Probably false <input type="checkbox"/> Certainly false <input type="checkbox"/> Not sure <p>7) Has this report been useful to you or your unit?</p> <ul style="list-style-type: none"> <input type="checkbox"/> Yes <input type="checkbox"/> No, information not needed <input type="checkbox"/> No, information already known <input type="checkbox"/> No, did not apply to current activities <input type="checkbox"/> No, other reason _____ <p>_____</p> <p>_____</p> <p>8) What are the two greatest deficiencies in this report? Please mark 1 next to the greatest deficiency and 2 next to the second greatest.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Not current <input type="checkbox"/> Too general <input type="checkbox"/> Too specific <input type="checkbox"/> Too speculative <input type="checkbox"/> Utilizes false information <input type="checkbox"/> Trivial, not useful <input type="checkbox"/> Too long, wordy <input type="checkbox"/> Too brief <input type="checkbox"/> Not responsive to requirements <input type="checkbox"/> False conclusions <input type="checkbox"/> Bad judgment <input type="checkbox"/> Other _____ <p>_____</p> <p>_____</p> |
|---|---|

We are interested in any additional comments you may have concerning this report. Please include them either on the back of this form or on a separate sheet. Thank you for your cooperation.

MONTHLY EVALUATION OF THE INTELLIGENCE UNIT

Please answer all questions by placing an "X" next to the appropriate response(s). If none of the responses provided is appropriate, feel free to answer any of the questions in your own words. After you have completed the questionnaire, please return it to the Intelligence Section.

- | | |
|---|--|
| <p>1) Over the past month have you utilized the services of the Intelligence Unit or been exposed to any information provided by intelligence?
 <input type="checkbox"/> Yes (Complete rest of questionnaire)
 <input type="checkbox"/> No (Go no further; return questionnaire to Intelligence Unit)</p> <p>2) Have you specifically requested assistance from the Intelligence Unit?
 <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>3) On the whole, has the intelligence provided been responsive to your requirements?
 <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>4) Over the past month, what has been the contribution of the Intelligence Unit to your understanding of criminal activity? (Answer one or more)
 <input type="checkbox"/> Activity of a specific criminal or group of criminals
 <input type="checkbox"/> Criminal activity associated with a place of business
 <input type="checkbox"/> Criminal activity in a geographic area
 <input type="checkbox"/> M.O. of a criminal
 <input type="checkbox"/> M.O. within a racket
 <input type="checkbox"/> Relationships among criminals
 <input type="checkbox"/> Relationships among rackets
 <input type="checkbox"/> Other _____

 _____</p> | <p>6) Are intelligence reports lacking in information; i.e., are you aware of important facts which should have been analyzed by the Intelligence Unit?
 <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>7) How would you describe the approach of information reported by intelligence?
 <input type="checkbox"/> Certainly true
 <input type="checkbox"/> Probably true
 <input type="checkbox"/> Probably false
 <input type="checkbox"/> Certainly false
 <input type="checkbox"/> Not sure</p> <p>8) In your opinion, what are the two greatest deficiencies in the overall performance of the Intelligence Unit? Please mark 1 next to the greatest deficiency, and 2 next to the second greatest.
 <input type="checkbox"/> Not responsive to requirements
 <input type="checkbox"/> Reports are trivial, not useful
 <input type="checkbox"/> Reports utilize false information
 <input type="checkbox"/> Slow response
 <input type="checkbox"/> Priorities for investigation
 <input type="checkbox"/> Reports are not conclusive
 <input type="checkbox"/> Analyses are in error
 <input type="checkbox"/> Utilize insufficient information
 <input type="checkbox"/> Other _____

 _____</p> |
|---|--|
- 5) What actions have you taken over the last month as a result of assistance provided by intelligence personnel? (Answer one or more)
 Adjust priorities
 Investigations initiated/increased
 Warrant/Subpoena
 Arrest
 Case dropped
 Other _____

 None

We are interested in any additional comments or suggestions you may have concerning the performance of the Intelligence Unit. Please include them on the back of this form or on a separate sheet. Thank you for your cooperation.

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.
- ANDERSON, A. "Organized Crime: The Need for Research." Washington, D.C. LEAA, U.S. Department of Justice, December 1970.
- 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.
- BLUMENTAL, RALPH, and GAGE, NICHOLAS. "Crime 'Families' Taking Control of Pornography," *New York Times*, December 10, 1972, pp. 1, 82.
- BOYDELL, C. L. *Demographic Correlates of Urban Crime Rates*. Ph.D. dissertation, University of Massachusetts, 1970.
- BOYDSTON, H. E. "The Santa Clara Valley Intelligence Unit," *The Police Chief* (November 1973), pp. 26-31.
- "Bull Market in Thievery." *Forbes*, v. 102 (December 15, 1968), pp. 34.
- Chamber of Commerce of 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.
- _____. *White Collar Crime*. Washington, D.C., Chamber of Commerce of the United States, 1974.
- CHARLTON, LINDA. "Crime Thrives on Bootlegged Cigarettes," *New York Times*, December 10, 1972, pp. 1, 42.
- COOK, FRED J. *The Secret Rulers: Criminal Syndicates and How They Control the U.S. Underworld*. New York, Duell, Sloan and Pierce, 1966.
- Chicago Crime Commission. "Spotlight on Legitimate Businesses and the Hood, Part II." In remarks by Charles Harting Percy. *Congressional Record* (Daily edition) v. 114 (June 24, 1968), S7595-S7596.
- COHN, S. I., and McMAHON, W. B., editors. *Law Enforcement Science and Technology III*, IIT Research Institute.
- CRESSEY, DONALD R. *Criminal Organization: Its Elementary Forms*. New York, Harper and Row, 1972.
- _____. *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.
- CRESSWELL, E. (editor). *Proceedings of the Second International Symposium on Criminal Justice Information and Statistics Systems*. San Francisco, SEI, 1974.
- DEMARIS, OVID. *Captive City*. New York, Lyle Stuart, Inc., 1969.
- DIRKS, RAYMOND L. and GROSS, LEONARD. *The Great Wall Street Scandal*. New York, McGraw-Hill, 1974.
- DUCOBNY, AMRAN. *The Billion \$ Swindle: Frauds Against the Elderly*. New York, Fleet Press Co., 1969.
- DUSTER, TROY. *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 Sciences*, v. 374 (November 1967).
- GOURLEY, D. D. "A Final Solution to the Problem of Organized Crime." *Police Chief*, vol. 39, no. 2 (1972), p. 18.
- HILL, ALBERT F. *The North Avenue Irregulars; A Suburb Battles the Mafia*. New York, Cowles Publications, 1968.
- HINDELAGE, 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.
- IANNI, F. A. J. *A Family Business: Kinship and Social Control in Organized Crime*. New York, Russell Sage Foundation, 1972.
- IIT Research Institute. *A Study of Organized Crime in Illinois*. IIT Research Institute, 1971.
- Illinois Crime Investigating Commission. *Justice Racketeers; Report on Criminal Usury in the Chicago Area*. Illinois, Illinois Crime Investigating Commission, June 1970.
- KERSTETTER, WAYNE A., Superintendent and NIXON, LEWIS M., III, Special Agent, Illinois Bureau of Investigation. *Police Intelligence Guidelines: A Response to Legal and Legislative Challenges*, given at the National Organized Crime Conference, Washington, D.C., October 1975.
- 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.
- LEVINE, H. and JORGENSON, J. R. "Organized Crime: A Civil Approach," *Police Chief*, vol. 37, no. 4 (April 1970), pp. 30-41.
- 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.
- MERCHANT, L. *The National Football Lottery*. New York, Holt-Rinehart, 1973.
- MESSICK, HANK, *Lansky*. New York, G. P. Putnam's Sons, 1971.
- _____. *Syndicate in the Sun*. New York, The Macmillan Company, 1968.
- MINTO, M. F. "The Criminal Intelligence Squad," *Police Chief* (February 1975), pp. 40-44.
- MOLLENHOFF, C. R. *Strike Force: Organized Crime and the Government*. Englewood Cliffs, N.J., Prentice-Hall, 1972.
- 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, pp. 3-46.
- New York (State) Commission of Investigation. *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.
- PACE, D. F. and STYLES, J. C. *Handbook on Vice Control*. Englewood Cliff, N.J., Prentice-Hall, Inc., 1972.
- _____. *Organized Crime: Concepts and Controls*. Englewood Cliffs, N.J., Prentice-Hall, 1975.
- 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.
- ROCKFORD, J. MV "Police Intelligence and Organized Crime Enforcement," *The Police Chief* (February 1975), pp. 47-49.
- 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 and TANEPLIN. *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.
- SCHELLING, 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.
- SCHULTZ, D. O. and NORTON, L. A. *Police Operational Intelligence*. Springfield, Illinois, Charles C. Thomas, 1968.
- 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.
- _____. and SALERNO, R. F. "The Use of Strategies in Organized Crime Control," *The Journal of Criminal Law, Criminology and Police Science*, v. 61, no. 1 (1970), pp. 101-111.
- 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, Michigan, 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. PL 90-351. 90th Congress, HR 5037, June 19, 1968, 82 Stat. 197.
- Privacy Act of 1974. PL 93-579. 93d Congress, S.3418, December 31, 1974.
- 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 Subcommittee. *Federal Effort Against Organized Crime: Report of Agency Operations*. Hearings, 90th Congress, 1st and 2nd Sessions, 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 Congress, 2nd Session, August 13, 1970-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 Congress, 1st Session, 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 Congress, 1st Session, 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 Congress, 1st Session, Washington, D.C., Government Printing Office, 1967.
Hearings held March 7-July 12, 1967.
- _____. *Measures Relating to Organized Crime*. Hearings, 91st Congress, 1st Session, March 18, 19, 25, 26 and June 3, 4, 1969. Washington, D.C., Government Printing Office, 1969.
- U.S. Congress. Senate. Subcommittee on Constitutional Rights. Committee on the Judiciary. Hearings in S.254, S.2810, S.2963, and S.2964. *Criminal Justice Data Banks*. 93rd Congress, 2nd Session, Washington, D.C., Government Printing Office, 1964.
- U.S. President, 1969- (Nixon). *Organized Crime* message. . . (91st Congress, 1st Session. House. Document no. 91-105) Washington, D.C., Government Printing Office, 1969.
- U.S. Department of Justice. "Criminal Justice Information Systems," *Federal Registrar*, vol. 40, no. 98 (May 20, 1975), Part III. Washington, D.C.
- "The Urban Poor and Organized Crime." In remarks of Joseph M. McDade. *Congressional Record* (Daily edition) v. 113 (August 29, 1967), H11431-H11435.
- WEISTART, J. C. (editor). *Police Practices*. New York, Oceana Publications, 1974.
- WILENSKY, H. L. *Organizational Intelligence: Knowledge and Policy in Government and Industry*. New York, Basic Books, 1967.
- WORMELI, P. K. "Project Search - System for Electronic Analysis and Retrieval of Criminal Histories," in *Law Enforcement Science and Technology III*, S. I. Cohn and W. B. McMahon editors. IIT Research Institute, 1970.
- YEAGER, MATTHEW G. "The Gangster as White Collar Criminal: Organized Crime and Stolen Securities," *Issues in Criminology*, v. 8 (Spring 1973).

BIBLIOGRAPHY

B. BIBLIOGRAPHY BY CHAPTER

CHAPTER I: Introduction

DULLES, ALLEN. *The Craft of Intelligence*. New York, Harper and Row, 1963.

KENT, SHERMAN. *Strategic Intelligence for American World Policy*. Princeton, N.J., Princeton University Press, 1966.

KILPATRICK, L. B., Jr. *The U.S. Intelligence Community: Foreign Policy and Domestic Activities*. New York, Hill and Wang, 1973.

RANSOM, HARRY H. *The Intelligence Establishment*. Cambridge, Mass., Harvard University Press, 1970.

ROSEFSKY, ROBERT S. *Frauds, Swindles, and Rackets*. Chicago, Follett Publishing Company, 1971.

United Aircrafts, 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.

YEAGER, M. G. "The Gangster as White Collar Criminal: Organized Crime and Stolen Securities," *Issues in Criminology*, v. 8 (Spring 1973), pp. 49-73.

CHAPTER II: Information Flow—Collection

BERS, M. K. *The Penetration of Legitimate Business by Organized Crime - An Analysis*. Washington, D.C. LEAA, U.S. Department of Justice, 1970.

Chamber of Commerce of the United States. *White Collar Crimes*. Washington, D.C., Chamber of Commerce, 1974.

HARNEY, MALACHI L. and CROSS, JOHN C. *The Informer in Law Enforcement*. Springfield, Illinois, Thomas, 1968.

MOORE, JAMES E., SANDERSON, JAMES A., and MEARS, CLARK E. *The Use of State Regulatory Action Against Criminal Infiltration of Legitimate Business*, presented at the National Conference on

Organized Crime, Washington, D.C., October 1, 1975.

The National Association of Attorney Generals Committee in the Office of Attorney General A. F. Summer, Chairman. *Organized Crime Legislation*. January 1975.

O'HARE, CHARLES E. *Fundamentals of Criminal Investigation*. 2nd Edition, Springfield, Illinois, Thomas, 1970.

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. Department of the Treasury. Federal Law Enforcement School.

"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.

CHAPTER III: The File System—Collation

HEWITT, WILLIAM H. *Police Records Administration*. Rochester, N.Y., Aqueduct Books, 1968.

KAHN, GILBERT, YERIAN, THEODORE, and STEWART, JEFFREY R., Jr. *Filing Systems and Records Management*. 2nd Edition. New York, McGraw-Hill Book Company, 1971.

WHISENAND, PAUL M. and TAMARU, TUG T. *Automated Police Information Systems*. New York, John Wiley and Sons, Inc., 1970.

CHAPTER IV: Analysis and Reporting

- BERS, M. K. and DEFRANES, D. J. "Research with Organized Crime Intelligence: The Penetration of Legitimate Business," *Law Enforcement Science and Technology III*. S. I. Cohn and W. B. McMahon (editors). IIT Research Institute, 1970.
- GAMMAGE, ALLEN Z. *Basic Police Report Writing*. Springfield, Illinois, Thomas, 1961.
- GARSON, G. D. *Handbook of Political Science Methods*. Boston, Mass., Holbrook Press, 1971.
- GASPER, L. C. *The Principles of Criminal Economics: An Introduction to the Analysis Measurement and Economic Control of Criminal Activities*. NIIS, 1971.
- SUCHMAN, EDWARD A. *Evaluative Research; Principles and Practices in Public Service and Social Action Programs*. New York, Russell Sage Foundation, 1967.
- TUFTE, E. R. *Data Analysis for Politics and Policy*. Englewood Cliffs, N.J., Prentice-Hall, 1974.

CHAPTER V: Staffing and Training

- American Academy of Political and Social Science. *Gambling*. Philadelphia, v. 269 (May 1950).
- ANASTASI, ANNE. *Psychological Testing*. 3rd Edition. London, The Macmillan Company, 1970.
Useful guide to range of tests available.
- BELLOWS, ROGER M. *Psychology of Personnel in Business and Industry*. 3rd Edition. Englewood Cliffs, N.J., Prentice-Hall, 1961.
- BELLOWS, ROGER M. with the assistance of M. FRANCES ESTEP. *Employment Psychology; The Interview*. New York, Rinehart, 1954.
- BLUM, RICHARD H. *Police Selection*. Springfield, Illinois, Charles C. Thomas, 1964.
Chapters on background investigation and psychological testing.
- BOHARDT, P. H. and RASMUSSEN, H. M. "The Selection and Training of Organized Crime Investigators," *Police Chief*, v. 38, no. 9 (September 1971), pp. 34-35.
- BRERETON, GEORGE H. "The Importance of Training and Education in the Professionalization of Law Enforcement," *Journal of Criminal Law, Criminol-*

ogy and Police Science, v. 52, no. 1 (May-June 1961), pp. 111-121.

- BRISTOW, ALLEN P. *Effective Police Manpower Utilization*. Springfield, Illinois, Thomas, 1969.
- _____. *Police Supervision Readings*. Springfield, Illinois, Thomas, 1971.
- GAMMAGE, ALLEN Z. *Basic Police Report Writing*. Springfield, Illinois, Thomas, 1961.
- GERMANN, A. C. *Police Personnel Management*. Springfield, Illinois, Thomas, 1958.
- _____. "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 1 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.
- PIGORS, PAUL and MYERS, CHARLES A. *Personnel Administration, A Point of View and a Method*. 5th Edition. New York, McGraw Hill Book Company, 1965.
Good basic text though directed at industrial and white-collar management.
- 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.
- 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).
- 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, Suchman, 1969.
- 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.

CHAPTER VI: Management of an Intelligence Unit

BLAKE, ROBERT B. and MOUTON, JANE S. *How to Assess the Strengths and Weaknesses of Personnel Management*. Texas, Scientific Methods, Inc., 1972.

BRISTOW, ALLEN P. *A Preliminary Study of Problems and Techniques in Decision Making for the Police Administrator*. Thesis for Master of Science in Public Administration, Los Angeles, School of Public Administration, University of Southern California, June 1957.

_____. *Police Supervision Readings*. Springfield, Illinois, Thomas, 1971.

_____ and GABARD, E. C. *Decision Making in Police Administration*. Springfield, Illinois, Thomas, 1961.

BROWN, WILLIAM P. *A Police Administration Approach to the Corruption Problem*. Prepared for the Organized Crime Program Division, Law Enforcement Assistance Administration, U.S. Department of Justice. (Available Fall 1971).

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.

HERSEY, PAUL and BLANCHARD, KENNETH H. *Management of Organizational Behavior*. 2nd Edition. New Jersey, Prentice-Hall, Inc., 1972.

Institute on Police Management for Supervisory and Administrative Personnel, Dallas, 1962. *Police Management for Supervisor and Administrative Personnel*. Springfield, Illinois, Thomas, 1963.

WHISENAND, PAUL M. *Police Supervision; Theory and Practice*. Englewood Cliffs, N.J., Prentice-Hall, Inc., 1971.

BIBLIOGRAPHY

C. BIBLIOGRAPHY BY APPENDICES

APPENDIX A: Guidelines for Police Intelligence Units (Part 1)

- American Bar Association. Project on Minimum Standards on Criminal Justice. *Standards Relating to Electronic Surveillance*. Tentative draft. June 1968.
- _____. 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 of computers, especially number 6, "Evidence."
- BLAKEY, G. ROBERT. "Aspect of the Evidence Gathering Process in Organized Crime Cases," Appendix C of *President's 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 Law and Procedure. Hearings, 90th Congress, 1st Session, 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 Record* (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 fact sheet 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.
- REUBHAUSEN, 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 Congress, 1st Session, 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 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.

APPENDIX A: Guidelines for Police Intelligence Units (Part 2)¹

Askin, *Police Dossiers and Emergency Principles of First Amendment Adjudication*, 22 Stan. L. Rev. 196 (January 1970).

Askin, *Surveillance: The Social Science Perspective*, 4 Colum. Hum. Rts. L. Rev. 59 (1972).

Belair & Bock, *Police Use of Remote Camera Systems for Surveillance of Public Streets*, 4 Colum. Hum. Rts. L. Rev. 143 (1972).

Blakey, *Aspects of the Evidence Gathering Process in Organized Crime Cases*, President's Commission on Crime and the Administration of Criminal Justice, Task Force Report: Organized Crime, Appendix C, G.P.O. (1967).

Buchsbaum, *Police Infiltration of Political Groups*, 4 Harv. Civ. Rts. - Civ. Lib. L. Rev. 331 (1969).

Comment, *Chilling Political Expression by Use of Police Intelligence Files: Anderson v. Sils*, 5 Harv. Civ. Rts. - Civ. Lib. L. Rev. 71 (January 1970).

Comment, *Judicial Control of Secret Agents*, 76 Yale L. J. 994 (1967).

Comment, *Police Infiltration of Dissident Groups*, 61 J. Crim. L., C. & P.S. 181 (1970).

Comment, *Police Undercover Agents*, 37 Geo. Wash. L. Rev. 634.

Comment, *Present and Suggested Limitations on the Use of Informers in Law Enforcement*, 41 U. Colo. L. Rev. 261 (1969).

Cowan, et al., *State Secrets: Police Surveillance in America*, Holt, Reinhart and Winston (1974).

Davis, *Police Surveillance of Political Dissidents*, 4 Colum. Hum. Rts. L. Rev. 101 (1972).

Donner, *Political Intelligence: Cameras, Informers and Files*, 1 Civ. Lib. Rev. 8 (1974).

Donner, *The Theory and Practice of American Political Surveillance*, Mono, repr. from N.Y. Times Rev. of Books 27 (April 22, 1971).

¹Part 2 reproduces the bibliography given in Brief Nos. 74-6 and 75-2, *Legal Aspects of Police Intelligence Gathering Activities*, December 1974 and May 1975, Americans For Effective Law Enforcement, Inc., Chicago, Illinois.

Emerson, *Freedom of Association and Freedom of Expression*, 74 Yale L. J. 1 (1964), on infiltration at 22.

Felkenes, *Right of Privacy and Police Surveillance by Aircraft*, 1 J. Pol. Sci. & Ad. 345 (1973).

Felkes, *Some Legal Aspects of Aircraft Usage as an Aid to Law Enforcement*, 3 J. of Cal. L. Enf. 128 (January 1969).

Hentoff, *The Politics of Privacy*, The Village Voice 29 (March 9, 1972), relating to the ORBIS III System.

House Comm. on Intern. Security, *Domestic Intelligence Operations for Intern. Security Purposes* (Hearings before 93rd Congress, 2nd Session, February-June 1974).

Mascolo, *The Role of Functional Observation in the Law of Search and Seizure: A Study in Misconception*, 71 Dick. L. Rev. 379 (1967).

McKay, *The Preference for Freedom*, 34 N.Y.U.L. Rev. 1182 (1959).

Nathanson, *Freedom of Association and the Quest for Internal Security*, 65 Northw. U. L. Rev. 153 (May-June 1970).

Neier, *FBI Files: Modus Inoperandi*, 1 Civ. Lib. Rev. 50 (1974).

Note, *Fourth Amendment Application to Semi-Public Areas: Smayda v. United States*, 17 Hasting L. Rev. 835 (1966).

Note, *Police Surveillance of Public Toilets*, 1966 Wash. & Lee L. Rev. 423.

Note, *Public Toilet - Not an Unreasonable Search*, 1966 Vand. L. Rev. 945.

Note, *Right of Association Extended to Curtail Harassment of Political Associations through Criminal Investigations*, 1969 Utah L. Rev. 383.

Pyle, *Spies Without Masters: The Army Still Watches Civilian Politics*, 1 Civ. Lib. Rev. 38 (1974).

Rifas, *Legal Aspects of Video Tape and Motion Pictures in Law Enforcement*, Northw. University Traffic Inst., Evanston, 19 pp. (1972).

Schad, *Police Liability for Invasion of Privacy*, 16 Cleve.-Mar. L. Rev. 428 (September 1967).

Schlam, *Police Intimidation Through 'Surveillance' May be Enjoined as an Unconstitutional Violation of Right of Assembly and Free Expression*, 3 Clearinghouse Rev. 157 (1969).

Shattuck, *Tilting at the Surveillance Apparatus*, 1 Civ. Lib. Rev. 59 (1974).

Westin, *Privacy and Freedom*, Atheneum Books, N.Y., 487 pp. (1967).

Westin, *Science, Privacy and Freedom*, 66 Colum. L. Rev. 1003 (1966).

ARTICLES

- Baker, Record Privacy as a Marginal Problem: The Limits of Consciousness and Concern, 4 Col. Hum. Rts. L. Rev. 89 (1972).
- Booth, The Expungement Myth, 38 L.A.B. Bull. 161 (1963).
- Comment, Retention and Dissemination of Arrest Records: Judicial Response, 38 U. Chi. L. Rev. 850 (1971).
- Ervin, The First Amendment: A Living Thought for the Computer Age, 4 Col. Hum. Rts. L. Rev. 13 (1972).
- Ervin, Privacy and Government Investigations, 1971 U. Ill. L. Forum 137.
- Freedom: Applications of the Fourth Amendment to National Security Investigations, 17 U.C.L.A. L. Rev. 1205 (1970).
- Fried, Privacy, 77 Yale L. J. 475 (1968).
- Goldwater, Jr., Bipartisan Privacy, 1 Civ. Lib. Rev. 74 (1974).
- Hufstедler, Directions and Misdirections of Constitutional Right of Privacy, 26 Record 546 (1971).
- Karabin, Retention and Dissemination of Arrest Records: Judicial Response, 38 U. Chi. L. Rev. 850 (1971).
- Karst, The Files: Legal Controls Over the Accuracy and Accessibility of Stored Personal Data, 31 Law and Contemp. Prob. 342 (1966).
- Katzenback & Tome, Crime Data Centers: The Use of Computers in Crime Detection and Prevention, 4 Col. Hum. Rts. L. Rev. 49 (1972).
- Kogan and Loughery, Sealing and Expungement of Criminal Records - The Big Lie, 61 Crim. L.C. and P.S. 378 (1970).
- Le Poole, Hassard, Abuse of the Record of Arrest Not Leading to Conviction, 13 Crime and Delinquency, 494 (1967).
- Miller, Computers, Data Banks and Individual Privacy: An Overview, 4 Col. Hum. Rts. L. Rev. 1 (1972).
- Miller, Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information Oriented Society, 67 Mich. L. Rev. 1089 (1969).
- Note, Commercial Information Brokers, 4 Col. Hum. Rts. L. Rev. 203 (1972).
- Note, Data Banks in a Free Society, 4 Col. Hum. Rts. L. Rev. 237 (1972).

BOOKS

- Report of the National Advisory Commission on Civil Disorders.

REGULATIONS

- LEAA Regulations (relating to criminal history information) 40 Federal Register 22114 (May 20, 1975).
- FBI Regulations (relating to dissemination of criminal histories) 28 C.F.R. S0.85 (implementing 28 U.S.C. S543).

APPENDIX E: 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 F: Analyst Manual

- AMOS, J. R., BROWN, F. L., and MINK, O. G. *Statistical Concepts*. New York, Harper and Row, 1965.
A programmed text for self-study, this book offers a very basic and easily understood primer on statistical methods.
- ANDERSON, T. R. and ZELDITCH, M., Jr. *A Basic Course in Statistics*. New York, Rinehart and Winston, 1968.
This is a more traditional text, intended for use in the classroom. It is, however, easily understood and discusses each concept thoroughly. This is an excellent introductory text, but is not suitable as a reference work.

BENSON, O. *Political Science Laboratory*. Columbus, Ohio, Charles E. Merrill Publishing Company, 1969.

Although this is intended as a workbook for use in political science courses on research methods, Chapters 1-3 and 5 offer good introductory material on quantification and measurement and a "cookbook" approach to statistics. Exercises follow each chapter.

BLALOCK, H. M., Jr. *Social Statistics*. 2nd Edition. New York, McGraw-Hill, 1972.

This is one of the most widely utilized statistics texts in introductory graduate courses in the social sciences. Blalock thoroughly discusses the conceptual background and rationale underlying each topic. Intended for classroom use, this is not a reference work and some of the sections may be too advanced for beginning students. However, as a conceptual and practical introduction to descriptive and inferential statistics, this is an excellent book.

FLOUD, R. *An Introduction to Quantitative Methods for Historians*. Princeton, N.J., Princeton University Press, 1973.

This book will be of special interest to intelligence analysts because it deals exclusively with descriptive statistics. There is also good introductory material on preparing data for analysis. This is an excellent introduction to quantitative techniques directed toward a discipline where such methods are largely unfamiliar.

HARPER, W. R. and HARRIS, D. H. "The Application of Link Analysis to Police Intelligence," *Human Factors*, April 1975.

McCOLLOUGH, C. and VAN ATTA, L. *Introduction to*

Descriptive Statistics and Correlation: A Program for Self-Instruction. New York, McGraw-Hill, 1965.

This is a programmed text intended for self-instruction. Dealing entirely with descriptive statistics, it is a good introduction to the basic concepts of greatest interest to the intelligence analyst.

ROSCOE, J. T. *Fundamental Research Statistics for the Behavioral Sciences*. New York, Holt, Rinehart and Winston, 1969.

Intended for use in the classroom, this text offers less detailed explanations of concepts. For this reason, and because the book covers a great deal of material, it serves better as a reference work than a first introduction to the field.

SIMON, J. L. *Basic Research Methods in Social Science*. New York, Random House, 1969.

Preparation and analysis of data are covered in Chapters 20-22. An unusual approach to inductive statistics is presented in Chapters 23-24. Much of this book is concerned with the research process in general and particular research and data collection methods.

YEOMANS, K. A. *Statistics for the Social Scientist I: Introducing Statistics*. Middlesex, England, Penguin Books, Ltd., 1968.

A good basic introduction, this book is concerned only with descriptive statistics. The book begins with a review of the basic mathematical operations and notations which are required to follow the substantive chapters. Directed toward the non-mathematician, this is a good first book on statistics which may also be useful as a supplementary volume to a larger text.