Joint Task Force on Intelligence and Law Enforcement

Report to the Attorney General and Director of Central Intelligence

May 1995

Executive Summary

Background

In the early 1990s, the BNL and BCCI prosecutions gave rise to public, press, and congressional perceptions of shortcomings in the Intelligence Community/Law Enforcement relationship. Many of those perceptions were articulated in three studies of the relationship: by the staff of the Senate Select Committee on Intelligence (SSCI); by the CIA Inspector General (IG); and by Judge Frederick Lacey, who was appointed as a special counsel by former Attorney General Barr. In March 1993, Director of Central Intelligence (DCI) R. James Woolsey and then-Acting Attorney General Stuart Gerson directed a joint study of the relationship by members of the two communities. This report is the result of that study.

The study was conducted by a joint Task Force. The members of the Task Force chaired parallel working groups, four for each of the two communities. Each community's four working groups focused, respectively, on legal policy, operations, information management, and judicial support. A small secretariat comprised of members from both communities was responsible for collating the studies of the working groups and drafting this report.

Although the Task Force and working groups initially looked at the perceived intercommunity difficulties identified in the SSCI, IG, and Lacey reports, they quickly realized that other issues pertaining to the relationship between the communities and its future development also merited careful attention.[1] Consequently, while this report addresses issues raised in those earlier documents, it goes beyond them to explore other important aspects of the evolving Intelligence Community/Law Enforcement relationship.

The study produced a total of 23 conclusions and recommendations regarding the relationship, which are set forth in abbreviated form below. For convenience's sake, they are divided into seven groupings.

Intelligence Community/Law Enforcement Relations at the Investigative Stage

In exploring the issues raised by BNL, BCCI, and other cases, the Task Force realized that the two communities had sufficient legislative and regulatory authorities to cooperate effectively and that such cooperation, if properly structured, may be pursued in a manner that maintains full protection for intelligence sources and methods. The Task Force also concluded, however, that law enforcement currently does not take advantage of the collection and

[1] Some agencies operate with elements in both communities, such as the FBI. For these agencies, the different legal frameworks controlling the separate activities are particularly important

information resources of the Intelligence Community (IC) to the full extent permitted by law and by considerations relating to the protection of sources and methods. The Task Force therefore concluded:

1. The legal authorities governing the activities of each community should be maintained without change. However, executive branch procedures should be further developed in specific areas of joint law enforcement/intelligence interest to facilitate the use of intelligence collection and information resources in assisting domestic law enforcement agencies, to the extent authorized.

2. Law Enforcement should make more disciplined use of the US intelligence requirements system to ensure that its needs for strategic intelligence are considered and, where appropriate, met. Law Enforcement should develop an enhanced capability to use information collected for foreign intelligence purposes to shape policies and directions for appropriate aspects of law enforcement.

3. Although cooperation between Law Enforcement and the Intelligence Community on specific investigations can present certain risks, those risks can be minimized if such cooperation is properly structured. For example, a Law Enforcement agency may provide an IC agency with target-specific lead information that the IC agency could properly exploit for foreign intelligence purposes. The IC agency, if it collects information from that target, may then disseminate the collected information to the Law Enforcement agency that had supplied the target-specific information.

4. As Law Enforcement increasingly collects information on international issues valuable to the Intelligence Community, the timely flow of information from Law Enforcement to the Intelligence Community, where allowable by law and to the extent consistent with the protection of both prosecutive and intelligence equities, must be encouraged and systematized.

Information Management

A principal concern of the SSCI and Lacey reports was the apparent inability by Main Justice to locate, or make use of, intelligence reporting relevant to the BNL matter. The Task Force recognized that information management improvements were imperative and recommended the following:

5. Both communities must improve their information management capabilities, particularly to ensure necessary retrievability.

   - Law Enforcement should appoint a working group to determine a satisfactory automated message handling system for Main Justice.

- Law Enforcement should, under Justice leadership, form a standing Information Management Committee of Law Enforcement agencies that use foreign intelligence information. This Committee would periodically review information management needs within the Law Enforcement Community.

6. The Intelligence Community should continue reviewing dissemination guidelines in order to make its information accessible and usable by Law Enforcement to the maximum extent possible.

Structural Reform and Training

The Task Force realized that improved communication could solve most problems between the two communities. In addition, each community currently operates with only a limited amount of knowledge about the other. Internal training initiatives and cross-community training should be improved to alleviate this situation. To address these problems, which may only increase as the Intelligence Community/Law Enforcement relationship evolves, the Task Force recommended:

7. Each agency within the communities should establish focal point systems to serve as points of entry and to interface with agencies in the other community. These systems are not intended to restrict the normal daily interaction between members of the two communities.

8. The two communities should form a Joint Standing Committee to review matters of overlapping interest in pending investigations and prosecutions and to conduct postmortem reviews of cases of mutual concern.

9. The communities should form a Joint Standing Committee for Training to identify subjects to be covered; recipients for the training; resources to be committed to training; and an implementation plan.

Searches of Intelligence Community Files

Litigation-related searches of Intelligence Community files burden the information management systems of intelligence agencies and may unnecessarily place intelligence sources and methods at risk:

10. The communities should form a small committee to:

    - Develop guidelines and procedures for conducting such searches.

    - Identify factors that may be considered in determining whether overly broad defense discovery demands should be resisted on the grounds that

the intelligence agency was not "aligned" with the prosecution on the specific case at issue.

11. When a Law Enforcement agency refers to a prosecutor a matter for prosecution, that agency should advise the prosecutor of the contacts its investigators have had with Intelligence Community components. Prosecutors apprised of such contacts should begin immediate coordination of search and discovery issues through the US Attorney's Office designated national security/international affairs referent.

12. To ensure Washington-level awareness of sensitive cases, the Department of Justice should clarify its guidance to prosecutors regarding investigations that require preindictment notice to the Criminal Division.

13. The Department of Justice should inform US Attorneys' Offices that Intelligence Community attorneys are a resource to help explain intelligence-related issues to courts, especially in pretrial Classified Information Procedures Act (CIPA) proceedings.

14. Procedures should be devised for noncriminal enforcement actions, such as INS exclusion proceedings, to permit the use of classified information while fully protecting sources and methods. The Department of Justice should determine whether legislation is needed in this area.

15. The two communities should consider whether CIPA-like procedures should be sought for Federal civil cases and state court criminal proceedings and explore seeking Federal removal jurisdiction over classified information issues in state court criminal proceedings.

16 *The United States Attorneys' Manual* should make clear to prosecutors that Rule 6(e)(3) authorizes them to disclose grand jury information to Intelligence Community personnel to assist them in responding to search requests.

17. *The United States Attorneys' Manual* should state that classified information may not be used before grand juries unless the prosecutor first complies with Section 9-90.200 of the *Manual*.

18. Both communities agree on the fundamental importance of protecting from public disclosure the true identities of intelligence officers testifying in court; they recognize that absolute protection may not always be possible or appropriate. The two communities could not agree on the procedures to be followed in determining when the intelligence officer's identity will not be fully protected. The Attorney General and DCI should establish the procedure for deciding when intelligence officers must testify in true name.

Crimes Reporting Obligations

The current procedures under which the Intelligence Community must report certain Federal crimes to the Criminal Division are outdated because: (1) they were promulgated before the Intelligence Community began disseminating regularly and directly to Law Enforcement agencies intelligence information indicating potential criminal activity; and (2) they do not specifically require the reporting of certain Federal crimes that are now of significant national interest but do require the reporting of too many crimes that are of *de minimis* interest.

19. The existing Memoranda of Understanding concerning crimes reporting should be revised and updated. (This recommendation is not intended to reflect or affect any existing responsibilities exercised by Intelligence Community Inspectors General in the crimes reporting area).

Intelligence Community/Law Enforcement Relations With Congress

The Intelligence Community and Congress should be sensitive to the impact that the public revelation of information concerning ongoing criminal investigations will have on those investigations. The need for confidentiality will have to be carefully protected consistent with Congress's oversight responsibilities.

20. Intelligence Community agencies must coordinate with the Department of Justice before reporting to the intelligence oversight committees intelligence matters related to ongoing criminal investigations.

21. Intelligence Community agencies should not be compelled to provide classified information related to criminal investigations to nonoversight committees. The Intelligence Community should seek the assistance of the oversight committees in brokering negotiations with other committees over demands for such information.

22. The Attorney General and DCI should consider an NSC review of the "Gates Procedures," which were established at the beginning of 1993 to regulate the dissemination of foreign intelligence that identifies Congressional members or staff. The NSC review would determine whether or not the procedures should be continued, amended, or abolished. Congress should be consulted in this process.

Center

The Task Force considered the concept of a single, centralized mechanism, such as a joint "center," to focus most or portions of the interaction between the two communities at the prosecution phase. The center could assist in reviewing, clarifying, and prioritizing search requests, and mediate problems between prosecutors and intelligence agencies.

23. The Attorney General and DCI should appoint a senior group of representatives to study the concept of a joint center and issue a report recommending whether a center should be established and, if so, in which community it should be located and what should be the scope of its responsibilities.

Contents

Introduction

The scandals involving the intelligence and law enforcement communities in the early 1970s marked a traumatic juncture in their relationship. As documented by the Watergate, Rockefeller, Church, and Pike investigations, the exposure of activities of the intelligence agencies in the sphere of domestic security were so unsettling that both communities reflexively withdrew for more than a decade from substantive, cooperative dealings. This reluctance to cooperate, while understandable, was counterproductive and not driven by any requirement of law.

Beginning with President Ford's Executive Order 11905 and culminating with President Reagan's Executive Order 12333, the Intelligence Community received clarified direction on the circumstances and procedures under which it could clandestinely collect information on US persons, as well as provide expertise and specialized equipment to the US Law Enforcement Community. These Executive Orders were particularly significant in that they specifically authorized as valid targets for intelligence collection information—including information on US persons—concerning international terrorist activities and international narcotics activities.[2] These substantive areas, of course, commanded at the same time the increased attention of US law enforcement agencies in the 1980s as foreign-based terrorist networks and drug cartels threatened the American people both domestically and abroad.

Thus, the intelligence and law enforcement communities found that their resources were beginning to be devoted to an increasing number of common subjects. At the same time, the two communities continued to share and remember the mutually painful experience of the investigations of the early 1970s when elements of intelligence and law enforcement clearly engaged in inappropriate conduct. Beginning in the mid-1980s, however, there were signs that the two communities were developing ways to enhance their cooperation without crossing legal boundaries.

First, the Director of Central Intelligence created "centers" where the operational, technological, and analytical expertise in the Intelligence Community was brought to bear on a given subject of worldwide scope. The first was the Counterterrorist Center in 1986, followed by centers for counternarcotics, counterintelligence, and nonproliferation. Each center has representatives from appropriate law enforcement agencies on detail to contribute their perspective and input. Second, as exemplified by the creation of the centers and involvement of law enforcement in them, both communities began to recognize that key national security issues confronting the United States in the post–Cold War world—terrorism, narcotics trafficking, proliferation of weapons of mass destruction, economic crimes—have both foreign intelligence and law enforcement components. Finally, another critical factor breaking down these institutional barriers was the utilization of the Classified Information Procedures Act (CIPA) 18 USC. App. III, which established a reliable mechanism for dealing with classified information issues in criminal litigation.

Since the late 1980s, however, a number of high-profile criminal cases (for example, Noriega, BCCI, and BNL) in which intelligence information and equities have either played a key role or were the subject of controversy have caused a reexamination of the relationship between the two communities. In varying degrees, these cases have been characterized by conflict, miscommunication, and a perception on the part of some in the Congress, the press, and the public at large that the intelligence and law enforcement communities remain either unwilling or unable to work together effectively. The Justice Department's 1992 investigation and prosecution of officials of BNL/Atlanta, and the process of securing CIA information in the course of

[2] It should be noted that NSA is not authorized to collect on US persons involved in international narcotics activities unless it has probable cause that those persons are agents of a foreign power as defined in the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. §§ 1801 et seq.).

that prosecution, represents a notable and controversial instance of apparent weaknesses in the relationship between intelligence and law enforcement.

As a result of the BNL case, the interaction between the two communities was scrutinized in three separate investigations in late 1992: one by Judge Frederick Lacey, appointed as a special counsel by then-Attorney General Barr; one by the CIA Office of Inspector General (OIG); and one by the staff of the Senate Select Committee on Intelligence (SSCI). None of these investigations found evidence of official misconduct. All of them, however, concluded that there was a need to improve communication between intelligence and law enforcement. Both the OIG and SSCI Reports specifically called for a comprehensive study of the fundamental relationship between the law enforcement and intelligence communities. In response, the Acting Attorney General and the Director of Central Intelligence established in March 1993 parallel but interrelated task forces to examine all aspects of the relationship and to propose ways to make it stronger and more effective. Those task forces were later merged into this Joint Task Force. This paper represents the results of that effort by the Joint Task Force.

Each of the three BNL investigative reports also proposed changes in the communities' operating procedures and information management systems to reflect increasingly overlapping areas of interest. Accordingly, the Task Force considered all of the major Lacey, OIG, and SSCI recommendations, concurring with many and disagreeing with a few. They will be more specifically addressed throughout this report.

The Task Force functioned through a small staff and operated through eight substantive working groups, four in each community, that focused on the following areas: legal policy, operations, information management, and judicial support. Each of the parallel working groups in the two communities carried out a comprehensive review in which all issues were open for discussion:

- The ***Legal Policy Groups*** addressed issues such as discovery obligations in criminal prosecutions; the appropriateness of information collection by the Intelligence Community in assisting a law enforcement investigation; providing Congress with intelligence information pertaining to ongoing prosecutions; and whether there is a need for new legislation, executive orders, or memoranda of understanding to articulate the desired relationship between these two communities.

- The ***Operations Groups*** examined such issues as identifying domestic and foreign situations that require contact between the two communities; the need for focal points for contacts; procedural issues related to information searches of Intelligence Community files; dissemination of information found during such searches; and training.

- The ***Information Management Groups*** studied each community's management of its own files, as well as the handling of information received from the other community.

- The ***Judicial Support Groups*** examined the problems posed by intelligence information for judicial proceedings, including, *inter alia*, CIPA, with particular attention to the need for procedures to protect classified information pertinent to matters in noncriminal enforcement proceedings and crimes reporting procedures.

The objective of the Task Force was not to reexamine conclusions reached in the Lacey, OIG, and SSCI investigations of the BNL matter; rather, it was to review the communities' relationship as it now exists and to focus on areas where problems do exist and where changes can and should be made to improve the overall relationship. In this report, we have broken the relationship into five phases, which are addressed in turn: routine dissemination of intelligence to law enforcement; investigation before the assignment of a prosecutor; investigation after the assignment of a prosecutor; court

proceedings; and several crosscutting issues including the Intelligence Community's relations with Congress, the need for intracommunity and intercommunity training, and a proposal for a detailed study of the advisability of establishing a Joint Intercommunity "Center."

Although this report will identify some issues about which the intelligence and law enforcement communities disagree, there was widespread consensus about those matters involving fundamental aspects of the relationship that must be improved. For instance, both sides recognize that significant effort and resources will be needed in each community to upgrade what are currently antiquated and too often unreliable information management systems. At the same time, there was unanimous resistance to overly broad changes in other key areas. For example, there was no support for relaxing the existing legal prohibitions on direct involvement by intelligence agencies in domestic law enforcement activities.

From the outset, the Task Force recognized that, given the self-imposed deadline for this report, it would be impossible to examine exhaustively all aspects of the multifaceted relationship between intelligence and law enforcement or to prescribe definitive, mutually agreed solutions to all problems. Accordingly, the report will identify several specific areas and potential new initiatives that merit further consideration at the policy level.

Finally, in reading this report, one must bear in mind that the Task Force has evolved substantially since it was commissioned by the DCI and Acting Attorney General. Over the ensuing months, it became increasingly clear that the task was far too complex and the problems far too subtle to address comprehensively in a short time given: the traditional views about the interrelationship between the communities, dramatic changes that have taken place in the way both do their business, and the ongoing evolution of the relationships. Also, it became clear that few of the issues are "black and white"; to the contrary, the relationship is dynamic as it moves through various phases. We concluded that in those areas where the two communities have overlapping concerns, significant institutional changes and detailed guidelines may be needed. Even so, these changes will only succeed if the relationship is based on trust, cooperation, and mutual understanding between the two communities. In the final analysis, the success of the relationship depends on modern institutional structures coupled with the willingness of both sides to work together on a day-by-day, case-by-case basis.

Conclusions and Recommendations

The Joint Task Force concluded that the basic legal authorities delineating the separation of responsibilities and duties of the two communities are sufficiently sound and flexible to permit the Intelligence Community (IC) to provide assistance to Law Enforcement Agencies (LEAs) as suggested by Judge Lacey and the Senate Select Committee on Intelligence in their BNL reports. What is required is not new legislation radically altering the relationship, but rather a different approach to the existing relationship—one that is more interactive on a number of fronts, yet maintains the important distinctions between these two communities based on law, culture, and mission.

The Task Force's recommendations relate either to improving interaction between the Intelligence Community and Law Enforcement Agencies or changing procedures where significant differences of interpretation have led to problems in the past. The recommendations have been applied to specific areas of overlap between the Law Enforcement and Intelligence Communities: legal authorities (including intelligence tasking); information management; structural reform for better coordination of interaction; training; searches of IC files; the interrelationship of the communities during court proceedings; the crimes reporting obligation; and Congressional oversight. The final recommendation suggests a detailed study on the advisability of establishing a joint office or center to enhance and formalize coordination in the contentious areas of interaction, especially during prosecutions affecting intelligence sources or methods.

Absent sweeping recommendations for legislative reform, the recommendations and discussion of issues below may appear overly cautious to some. However, a review of past patterns of interaction indicates that implementing the recommendations described below will require a major commitment to, and outspoken support from, each community's principals. A detailed discussion of these recommendations follows.

I. Legal Authorities

The Task Force believes the Intelligence Community has adequate legal authority to provide appropriate assistance to LEA's. Further, expansion of the IC's role into the investigatory and enforcement realms is not advisable and in many cases is not within the scope of the IC's authority. Such action not only could jeopardize the protection of sources and methods but also would present serious Fourth Amendment problems, at least with respect to electronic surveillance and other forms of intelligence gathering that would constitute searches or seizures if done for a law enforcement purpose. The Task Force believes that if the Law Enforcement Community takes steps to suggest broad topics for intelligence gathering in a more orderly and coordinated fashion than it currently does, the IC can better provide appropriate assistance to LEA's. Nevertheless, while the limitations on using Intelligence Community resources to perform law enforcement searches and seizures are relatively clear and while no change in the legislation governing the relationship of the two communities is necessary, better definition of this relationship and its underlying legal authorities are needed.

Recommendation #1

The principal legal authorities governing the activities of each community, as well as those governing assistance by the Intelligence Community to the Law Enforcement Community, should be maintained as currently written. However, in those areas where the activities and interests of the two communities overlap and where the IC can lawfully provide assistance to Law Enforcement without compromising sources and methods, procedures and limits regarding the extent to which IC resources may be brought to bear should be drafted and disseminated within both communities within 180 days from the date of this report.

II. Intelligence Tasking/Information Sharing

The IC traditionally has disseminated its intelligence product to a broad range of government agencies, including the law enforcement and regulatory agencies, using a well-defined structure that prioritizes the information required by policy agencies ("users") against the capabilities of the intelligence gathering agencies. By and large, the Law Enforcement Community has sporadically participated in the process of setting foreign, strategic intelligence collection requirements, but not in a sufficiently orderly and coordinated manner. There are a number of reasons: lack of knowledge about the requirements process, reluctance to participate in setting foreign intelligence collection requirements because of concerns regarding the legal authorities to do so, and a decentralized approach to setting law enforcement priorities that has tended to focus on specific cases rather than on strategic trends. Records management issues also played a role. The LEAs have much to gain from using strategic foreign intelligence to identify and illuminate areas of law enforcement concern.

As Law Enforcement increasingly collects information on international matters relevant to the foreign policy and/or national security responsibilities of members of the Intelligence Community, the transfer of this information to the Intelligence Community is pivotal to improved cooperation. Such information sharing is essential to enable members of the Intelligence Community to comply with their statutory requirements and carry out their normal responsibilities. Law Enforcement information relevant to intelligence topics not only serves to improve the Intelligence Community's analytic capabilities but also increases the Intelligence Community's ability (consistent with governing legal authorities and the protection of sources and methods) to collect and analyze additional information useful to Law Enforcement. Certain restrictions on Law Enforcement, such as Grand Jury secrecy, pretrial discovery, and wiretap limitations, will limit what information can be shared outside of the Law Enforcement Community. Nevertheless, when such restrictions are not applicable, efforts should be taken to facilitate the full exchange of information.

Recommendation #2

Law Enforcement, in general, and the Department of Justice, in particular, should develop an improved capability to use foreign intelligence and other strategic information to help shape policies and overall directions for law enforcement. Moreover, Law Enforcement should, in a more orderly and coordinated fashion, suggest broad topics for foreign intelligence gathering and provide advice during the evaluation and prioritization of such topics on the basis of their foreign intelligence and national security significance. Recommendations for creating such strategic and analytical capabilities in those law enforcement agencies, where they do not exist currently, should be prepared for the heads of individual law enforcement agencies within 180 days from the date of this report.

Although Law Enforcement may (and does) suggest broad topics for intelligence gathering, more difficult issues are presented by cooperation between Law Enforcement and the Intelligence Community on specific investigations. For example, the Intelligence Community performing searches and seizures (including electronic surveillances) or using intelligence collection resources to gather case-specific information, poses risks to intelligence sources and methods. One way to minimize those risks and ensure that case-specific collection is undertaken in a manner consistent with pertinent legal authorities is for Law Enforcement to provide target-specific lead information to IC agencies, which would then determine whether exploiting the target would produce foreign intelligence information. If collection against the target is then undertaken, the IC agency in all likelihood would disseminate the information collected to the interested intelligence consumers, including the LEA that provided the target-specific information. For its part, Law Enforcement can increase its flow

of information to the Intelligence Community in appropriate instances.

Recommendation #3
A committee composed of representatives of both communities should be established to develop standards and procedures regarding law enforcement's ability to propose subjects of interest for intelligence collection. Those standards and procedures should be presented to the Attorney General and the DCI for their approval within 180 days from the date of this report.

Recommendation # 4
Policies and procedures should be put into place to ensure that the Law Enforcement Community, where allowable by law and to the extent consistent with the protection of prosecutive equities, shares in a timely manner with the Intelligence Community information it obtains on international issues relevant to the responsibilities of the Intelligence Community.[3]

III. Information Management

At present, even when foreign intelligence relevant to law enforcement interests is identified and disseminated, the Law Enforcement Community often cannot effectively exploit it for want of adequate information management structures. Based on exhaustive reviews/critiques of its information management system prepared by the CIA's Inspector General and the SSCI in its BNL report, the CIA's Directorate of Operations (DO) has undertaken a comprehensive upgrading of its information management system. This work should be continued and be mirrored in the Law Enforcement Community.

[3]State Department objects to the phrase "to the extent consistent with the protection of prosecutive equities ..." and believes it should be deleted. In State's view, this phrase is open ended and subject to unilateral interpretation by the Law Enforcement Community that in effect would formalize a one-way flow of information between the two communities.

Recommendation #5
The Intelligence Community should continue its comprehensive effort to overhaul its information management systems. The Law Enforcement Community must concurrently upgrade significantly its information management capabilities. Each community must be able to securely and efficiently transmit, receive, store, and retrieve information provided by the other.

A. *The Law Enforcement Community should establish an Information Management Task Force to define within 180 days of this report the requirements for an automated message handling system for use within Main Justice. The Task Force should include representatives from the Executive Office for United States Attorneys, Department of Justice (DOJ) litigating components, and Justice Department and Treasury Department components that regularly receive or transmit information critical to investigations and ongoing litigation within DOJ.*

B. *A Standing Information Management Committee should be established immediately, chaired by the Justice Department and including representatives from the law enforcement agencies that routinely receive or require foreign intelligence information. The objective of the Information Management Committee should be to review periodically information management needs within the Law Enforcement Community.*

Recommendation #6
The Intelligence Community should continue its comprehensive review of dissemination restrictions with an eye toward making its information more readily usable by law enforcement, while still protecting sources and methods.

IV. Structural Reform for Better Coordination: Focal Points, Centers, or Other Coordinating Structures

Improved communication could solve many problems between the two communities by

facilitating the identification, discussion, and resolution of underlying issues. The existing DCI centers (counterterrorist, counterintelligence, counternarcotics, and nonproliferation) are examples of structures that have improved coordination and information sharing by fostering close and highly effective cooperation. There was agreement in the Task Force that a structured process is needed to resolve issues in the day-to-day exchange between the communities as they deal with investigations and prosecutions of overlapping interest.

Recommendation #7
Within 180 days of this report, each agency should establish focal point systems, or designate one or more specific offices, to serve as a point of entry and an interface[4] with the other community on matters of mutual interest to the two communities. These focal point systems should not limit the normal, routine, daily contact between personnel in the two communities.

Recommendation #8
A standing committee should be created within 30 days of this report to review matters of overlapping LEA and IC interest in pending investigations and prosecutions. This standing committee shall be tasked to conduct postmortem reviews of cases of mutual concern in order to identify weaknesses in the relationship and to recommend corrective measures. The committee should meet periodically, but not less than quarterly.

V. Training

There currently is an insufficient amount of knowledge within each community about the other. Both communities are now reviewing their internal training needs in the area of IC-LEA interaction and are pursuing creative modifications to their programs to alleviate this situation. These internal training initiatives need to be complemented by a collaborative effort designed to foster an across-the-board appreciation for each other's basic legal authorities and limitations, missions, cultures, and modus operandi. This program of cross-community training and education should reach all levels of both communities, to include entry level, middle, and senior management levels, as well as prosecutors and judges.

Recommendation #9
Both communities must invest significantly in training and education—both internally and cross-community. Accordingly, a Joint Standing Committee for Training should be formed within 30 days of this report to identify appropriate subjects to be covered; individuals and groups that should receive such training; what level of resources needs to be committed; and how such training should be prioritized and implemented. This committee should prepare a report for the DCI and the Attorney General within 180 days of this report.

VI. Searches of IC Files

Even in those specific areas where the Intelligence Community and Law Enforcement agencies work together well on a day-to-day basis (for example, terrorism and narcotics), there is a lack of consistent policies and procedures when cases with intelligence equities approach prosecution. Due to this and the increasing tendency for prosecutors and defendants to make ever broader search requests, the Task Force concluded that the policies that trigger Intelligence Community participation in criminal litigation must be coherently defined and regularized. In particular, the issue of what constitutes "alignment" of an Executive Branch agency with the prosecution so as to require searches of that agency's files for purposes defined in law (for example, *Brady* and the Jencks Act) needs to be clarified.

In addition, there is now an increasing number of prosecutors' requests for "prudential searches" of intelligence agency records as a precautionary measure in anticipation of a defendant raising classified or other intelligence related matters. This creates onerous burdens on the Intelligence

[4] "Point of entry" and "interface" are vague terms that were selected deliberately in order to permit the greatest room for flexibility in debating and defining a focal point mechanism

Community records systems. It is clear that consistent policies addressing these and related issues of concern to both communities are required rather than merely continuing the current *ad hoc* approach.

Recommendation #10
A committee, comprising representatives of both communities, should be created and charged with:

A. *Developing within 180 days guidelines for determining when and how to conduct searches of Intelligence Community records in response to requests emanating from law enforcement investigations and prosecutions. These guidelines should cover searches sought by defendants for discovery purposes as well as searches sought by prosecutors and investigators for their own purposes. The guidelines should provide precise definitions for the various levels of searches of Intelligence Community records and identify factors that might warrant each level of search.*

B. *The committee also should identify factors that may be considered in determining whether "alignment" exists between the prosecution and a component of the Intelligence Community in a particular case and what significance alignment or lack of alignment should have on whether an intelligence agency's records should be searched for either "defensive" or "prudential" purposes.*

Recommendation #11
Law enforcement agencies should inform prosecutors at the time of prosecutive referral if the investigators engaged in any significant or ongoing cooperation with a component of the Intelligence Community. Where there has been such significant or ongoing, case-specific cooperation, prosecutors should contact the relevant component of the Intelligence Community as soon as possible to begin any necessary coordination. This coordination should be effected through the US Attorney's Office's designated national security/international affairs coordinator.

Recommendation #12
To ensure Washington-level awareness of prosecutions in which there may be Intelligence Community involvement, within 180 days the Department of Justice should clarify its guidance to US Attorneys regarding investigations that require notification to the Criminal Division before indictment.

VII. Relationship Between IC and Courts

While the prosecuting attorney must retain overall management and tactical control of the prosecutions, Intelligence Community lawyers are a valuable resource and can, with the consent of the prosecutor, assist the court by explaining intelligence-related issues and responding to any questions from the bench during Classified Information Procedures Act (CIPA) proceedings. Prosecutors should be encouraged to use this resource in CIPA cases.

In recognition of the beneficial effect CIPA has had in criminal cases involving classified information, there was a strong minority view within both communities in favor of extending the CIPA procedures to Federal civil cases, state prosecutions, and noncriminal proceedings such as INS deportation hearings. This view is based on the fact that since CIPA does not now apply to these proceedings, there is generally no means of protecting classified information other than asserting a state secrets privilege effectively forcing dismissal of the case. Short of seeking new legislation, the proposed solution is to attempt to craft administrative procedures so that proceedings now outside CIPA purview can proceed while sensitive intelligence information remains protected.

Further, the special rules that govern use of Federal grand juries raise two concerns for the Intelligence Community. First, grand jury secrecy limits dissemination of grand jury material to "an attorney

for the government for use in the performance of such attorney's duty" and to such other government personnel who assist that attorney in his or her duty to enforce federal criminal law. Rule 6(e)(3)(A), Fed. R. Crim. P. Where searches of Intelligence Community files are necessary for a criminal investigation, Intelligence Community personnel will often need access to that grand jury information in order to design and execute these searches. Prosecutors should be clearly advised that where intelligence personnel are conducting searches to assist Federal law enforcement, the law allows necessary disclosure of grand jury information to them. At the same time, intelligence personnel who receive such disclosures must agree that they may use the information only for the limited purpose of assisting law enforcement, and not for other purposes. Rule 6(e)(3)(B), *id.*

Second, grand jurors are not security cleared. Presenting classified information to a grand jury, therefore, may present a security risk. Federal prosecutorial practice provides a general procedure for securing advance permission from the appropriate IC agency before prosecutors disclose classified information to third parties. This procedure should apply to disclosure before a grand jury as well.

Recommendation #13

While the Federal prosecutor must remai responsible for the overall management and tactical prosecution of a case, the Department of Justice should encourage prosecutors to make greater use of Intelligence Community lawyers, when appropriate, such as to brief the court before trial on intelligence-related issues, including sources and methods. This potential use of Intelligence Community lawyers needs to be clearly articulated in The United States Attorneys' Manual and in prosecutor training.

Recommendation #14

In noncriminal enforcement actions, for example, INS proceedings, there is an urgent need to devise procedures, pursuant either to statute or regulation, that permit the Government to make appropriate use of classified information or unclassified substitutes but with full protection for sources and methods and other national security equities. Within 90 days of this report, the Department of Justice, in consultation with the Intelligence Community, should determine whether this issue can be dealt with via administrative regulation or whether legislation is necessary.

Recommendation #15

Consideration should be given to whether procedures to create a functional analog of the Classified Information Procedures Act (CIPA) is needed to provide for the protection of classified information implicated in Federal civil litigation and state criminal proceedings.

A. *Within 30 days of this report, a committee should be established, composed of representatives of the Department of Justice (including the Civil Division), intelligence agencies, and any other relevant parties, to devise regulations setting forth procedures for use in civil litigation similar to those provided by the CIPA. This committee should prepare recommended regulations for circulation to the Attorney General and other appropriate government officials within 180 days of this report.*

B. *Similar consideration should be given to creating limited Federal removal jurisdiction when classified information becomes relevant to state court criminal prosecutions. The Department of Justice, in coordination with the Intelligence Community, should propose legislative or procedural solutions to this issue within 180 days of this report.*

Recommendation #16

Within 90 days of this report, The United States Attorneys' Manual should be revised to make clear to prosecutors that Rule 6(e)(3) of the Federal Rules of Criminal procedure authorizes them to disclose grand jury information to Intelligence Community personnel to help those personnel focus and conduct search requests received from prosecutors;

provided, of course, that all recipients of such disclosure comply with legal requirements for the handling of such grand jury information.

Recommendation #17
Within 90 days of this report, DOJ should amend The United States Attorneys' Manual to provide that classified information may not be used before grand juries without complying with Section 9-90.200 of the Manual regarding the handling of classified material.

Finally, while the Task Force agreed on the fundamental importance of protecting classified information whenever it becomes relevant to Federal criminal litigation, one topic raised sharp disagreement and requires a policy-level resolution. On occasion, there is a legitimate need for a covert intelligence officer to appear in Federal court as a witness; the issue is whether the officer must be publicly identified in true name.

Recommendation #18

A. *Intelligence Community Position: As a general policy, the officer's true name is classified information that must be protected from public disclosure. In appropriate cases, true name may be made available under seal, and in secure circumstances to the judge, prosecutor, defense attorney, defendant, and jury. The provisions of CIPA should be rigorously applied in such cases and both the Attorney General and the DCI must approve in advance all exceptions to this policy. The policy should be published in The United States Attorneys' Manual.*

B. *Law Enforcement Position: Individual prosecutors should review each case calling for the appearance of an Intelligence Community witness to assess the government's need to protect the officer's identity versus the effect on the trial proceedings of employing protective measures. Requests to have covert officers appear in true name must be approved by the Assistant Attorney General/Criminal Division.*

VIII. Crimes Reporting Obligations

Both communities for the most part believe that the current working procedures governing the Intelligence Community's "crimes reporting obligations" are outdated, unreasonable, and unnecessarily burdensome on DOJ and on the Intelligence Community. A substantial majority of the Task Force believes that crimes reporting procedures should encompass only an intelligence agency's duty to report suspected significant criminal misconduct by officers, employees, contractors, or agents and it should not include information involving possible violations of law involving third parties acquired during foreign intelligence collection; routine intelligence dissemination to the relevant law enforcement investigative agency should be all that is necessary in the latter category. For its part, FBI concurs that the procedures should be reviewed and updated but disagrees with the formulation outlined in the previous sentence.

Recommendation #19
The existing Memoranda of Understanding between IC and LE agencies on crimes reporting should be revised, taking into account the increased routine dissemination of intelligence information to law enforcement agencies relevant to criminal activity. The new memoranda should provide clearer definition regarding the crimes to be reported to the Law Enforcement Community.

IX. IC and Law Enforcement Relations With Congress

Congress and the Intelligence Community need to be constantly mindful of the impact that public revelation stemming from Congressional briefings and hearings may have on ongoing criminal investigations and prosecutions. With respect to dealing with intelligence oversight committees, the need to preserve separation of powers and the confidentiality of such cases must be carefully weighed against with Congressional oversight responsibilities. When responding to nonoversight

committees' requests for classified information regarding pending prosecutions, the Executive branch must continue to preserve the separation of powers and to protect national security information as well as information involved in a prosecution. In any case, in light of the effect Congressional hearings may have on a pending prosecution, any response to a Congressional request must be thoroughly coordinated between the intelligence and law enforcement communities.

Recommendation #20
Before providing its Congressional oversight committees with information related to ongoing criminal investigations or prosecutions, the Intelligence Community must coordinate with DOJ and other involved law enforcement agencies to avoid developments that might adversely affect the investigations or prosecutions.

Recommendation #21
The Intelligence Community should not provide information related to ongoing criminal investigations to nonoversight committees of Congress except in special circumstances. In any such case, there must be coordination with DOJ. The intelligence oversight committees should be asked to assist the Intelligence Community in brokering negotiations with the nonoversight committees of Congress and in making arrangements for transfer of classified information when deemed appropriate in a particular case.

On 31 December 1992, then-DCI Robert Gates sent a memorandum to all members of the National Foreign Intelligence Board (NFIB) establishing procedures for disseminating foreign intelligence that identifies Congressional members or staff. These procedures, which were coordinated with the National Security Council (NSC) staff and IC, provide for an initial review by the collecting agency to determine whether the information may be properly retained and disseminated under that agency's procedures. As is typically the case with US persons, the Congressional identities are removed before any dissemination. Except for the President, Vice President, Secretaries of State and Defense, and the National Security Adviser, any recipient of disseminated information must submit a written request for the Congressional identities to the DCI.

Recommendation #22
The Attorney General and DCI should consider seeking an NSC review of the procedures governing dissemination of foreign intelligence regarding members or staff of Congress established on 31 December 1992 by then-DCI Robert Gates. This review should determine whether they should remain, be amended, or be abolished. The views of Congress should be solicited in this process.

X. Center

In the view of many Task Force participants, many of the issues identified in the report could be resolved through creation of a single, centralized mechanism (that is, a joint "center"), which is limited in scope, but given clear authorities within its area of responsibility. Although some participants believe that a center could cover most or all of the interaction between the communities, the majority concluded that it should be limited to the prosecution phase, with its focus on handling search requests of IC records. The majority argued that any attempt to encompass all of the interaction between the two groups would limit, over-bureaucratize, and confuse the healthy exchange already taking place at the investigative level. Center functions could include framing the scope of search requests, prioritizing the incoming requests, ensuring that requests are not duplicative, mediating conflicts between individual prosecutors and IC agencies over prosecution-related issues, providing personnel to appear in court as witnesses to answer questions related to file searches, and designing and implementing training for members of both communities in this area. It is not intended that a center would replace or limit the direct contact between individual prosecutors and the IC agencies after search results have been made available.

Recommendation #23

The Attorney General and DCI should establish a senior group of representatives from both communities to prepare a report within 180 days regarding the formation and implementation of a joint "center" to serve as a clearinghouse for the day-to-day interaction between the communities concerning ongoing criminal prosecutions. The group's report should incorporate recommendations on scope of authority, staffing, resources required, and location.

Discussion

The Law Enforcement and Intelligence Communities today face a fundamental question: Can they work together cooperatively to the benefit of both, without doing violence to the very different principles that govern each? The "relationship" between law enforcement and intelligence was until relatively recently an oxymoron, largely because during the last half century the two communities have existed in largely separate spheres. They were two communities separated by law, mission, culture, scope of activity, and language.

The Task Force's original, more modest objective was to identify and correct flaws and inefficiencies of the existing law enforcement/intelligence relationship. Nonetheless, as the work of the Task Force progressed, it became increasingly clear that a more comprehensive review was needed and that a thorough examination of the two communities "from the ground up" was required before recommending fundamental changes. Both sides recognized that a better relationship would require a host of changes, large and small. The starting point for change is a thorough understanding of the authorities, structures, and behavior of these two communities.

The Task Force organized its efforts around four pairs of working groups, one group in each pair essentially comprised of Intelligence Community representatives and one group essentially comprised of law enforcement representatives, though each had some representation from the other community. Each pair was assigned to consider one of four broad subject matter areas (law and policy, operations, information management, and judicial support).

The respective roles of the Law Enforcement and Intelligence Communities on a given subject change over time. Subjects of mutual interest (for example, counternarcotics and counterterrorism) often evolve from topics of general intelligence study and analysis to actual "cases" involving a specific law enforcement objective. We found that this evolutionary pattern could be divided into four phases:

Phase One
Routine dissemination of intelligence information and analysis to law enforcement agencies for general strategic, policy, and "crimes reporting" purposes.

Phase Two
Collection of specific intelligence information relevant to individual ongoing investigations.

Phase Three
Prosecution searches of intelligence information and analysis (preindictment).

Phase Four
Use and protection of intelligence information and analysis (postindictment).

In this paper, the four subject matter areas examined by the working groups will be discussed as they arise in the four phases of the relationship between the Intelligence and Law Enforcement Communities. Several common issues are more fully discussed in the final section of miscellaneous issues.

Phase One

Routine dissemination of intelligence and analysis to law enforcement agencies for general strategic, policy, and "crimes reporting" purposes.

A. The Nature of the Problem

During Task Force discussions, several problems were identified about Phase One of the relationship:

- Foreign intelligence information has become increasingly relevant to law enforcement in a global environment where domestic law violations often have international aspects.

- Although Law Enforcement Community officials participate in the foreign intelligence collection requirements process, they do not participate in a sufficiently orderly and coordinated manner and, in general, make limited use of the analytic capabilities of the Intelligence Community; further, they must develop an increased understanding of the more problematic issue of tasking intelligence agencies to investigate specific instances of criminal activity.

- Serious legal issues, as well as risks to sources and methods are presented by cooperation between Law Enforcement and the Intelligence Community on specific investigations.

- Law Enforcement information management systems remain inadequate to handle growing amounts of intelligence information, even without considering the greater amount of such information that might be disseminated to Law Enforcement as a result of improved Law Enforcement participation in the foreign intelligence collection requirements process.

- The current procedures for "crimes reporting" may be obsolete: relevant criminal conduct has expanded as a category and the Intelligence Community is often not equipped—and probably should not be expected—to determine what information reflects evidence of possible criminal activity.

These are the problems in Phase One. What solutions are possible?

B. Law Enforcement's Role as an Intelligence "Consumer"

Law enforcement agencies differ from traditional intelligence consumers in at least three respects:

- Their lack of historical experience with foreign intelligence.

- The particular topics of interest to them may not otherwise be priority targets from a foreign intelligence standpoint.

- The highly public potential use (that is, in prosecutions) of the intelligence information which they receive.

These differences raise several questions:

- Does the Law Enforcement Community know how to make the most effective use of the foreign intelligence collection requirements system?

- What determines whether a subject of interest to the Law Enforcement Community is also a proper matter for foreign intelligence collection?

- How may the Law Enforcement Community submit its strategic foreign intelligence information needs to the Intelligence Community in the most cogent way and have its proposals effectively prioritized against the more traditional foreign intelligence requirements?

- Should the Intelligence Community seek statutory or regulatory amendments that will permit it to target and collect law enforcement information that is now legally "off-limits" because a

sufficient foreign intelligence or counterintelligence nexus is missing?

- Does the Law Enforcement Community effectively use even that intelligence information it now receives?

C.(1) Question Raised: Does Law Enforcement Know How To Make the Most Effective Use of the Foreign Intelligence Collection Requirements Process?

The Task Force found that although the Law Enforcement Community is familiar with the Intelligence Community process for establishing strategic foreign intelligence collection requirements, it does not use it as effectively as it might. The process itself is highly complex and resource-intensive, demanding both strategic vision and tactical flexibility. The Intelligence Community devotes significant resources to developing technical and human collection assets that can address known long-term strategic foreign intelligence needs while retaining enough flexibility either to concentrate on critical near-term targets or to shift focus onto unforeseen issues.

In essence, the process involves agencies in the national security community—including intelligence components of law enforcement agencies—that need strategic foreign intelligence information identifying to the Intelligence Community subjects of interest. These needs are called "requirements." Long-term collection needs (for example, Eastern Europe in the post–Cold War era) are known as "standing requirements." Time-sensitive, near-term collection needs and modifications to standing requirements are dealt with through a variety of "ad hoc requirements."[5]

[5] Beyond this general description, each individual intelligence collection discipline (for example, human intelligence, signals intelligence, imagery intelligence, and so forth) has its own separate approach to compiling, verifying, prioritizing, and tasking collection requirements. Each of these disciplines independently sets priorities for the intelligence collection requirements it receives. Therefore, a requirement that is a high priority for imagery intelligence, for example, may be a low priority, or no requirement at all, for human intelligence.

The process was established to meet US military and diplomatic needs. Over time, it has evolved to include participation by the intelligence components of LEA's such as Treasury, FBI and DEA, which propose broad topics of interest to them. Those topics are then validated and prioritized in accordance with whether and to what extent they call for the collection of information of *bona fide* foreign intelligence value.

Because there are many more collection needs than the Intelligence Community has resources to accommodate, prioritization of requirements is essential. In consequence, subjects of law enforcement interest with little strategic foreign intelligence value might easily receive lower priority than intelligence topics of greater foreign intelligence value and, thus, receive only limited, if any, attention. Like all suggested collection topics, strategic foreign intelligence collection requirements proposed by LEA's must compete with the universe of all other strategic foreign intelligence collection requirements.

C.(2) Question Raised: Can Law Enforcement Use Intelligence Resources and Information More Effectively?

Greater cooperation between law enforcement and intelligence, and better-focused participation by LEA's in proposing intelligence requirements, will lead to better use of existing resources. For its part, law enforcement should:

- Continue to identify and urge collection on foreign intelligence subjects which also are of law enforcement interest, but do so in a more orderly and coordinated fashion.

- Work with intelligence agencies to analyze relevant foreign intelligence information that it does obtain.

- Make optimum use of this information by improving its information management structures.

At present, however, the Law Enforcement Community lacks the organizational structures, analytic expertise and information management systems to implement these steps in the most effective manner possible. This state of affairs exists in large part because no single centralized authority in the Law Enforcement Community serves as an advocate for the foreign intelligence needs of the community as a whole. As noted above, some law enforcement agencies (for example, Treasury, FBI, and DEA) have intelligence components that participate in the "requirements" process. Others, however, particularly the Department of Justice, are largely absent from the process.

Law Enforcement's involvement in the requirements process could be improved by any number of bureaucratic "fixes." For instance, the Law Enforcement Community could establish an Issue Manager or Focal Point to gather or prioritize strategic law enforcement foreign intelligence needs before submitting them to the Intelligence Community for validation and, if appropriate, prioritization in the strategic foreign intelligence collection requirements process.

Nonetheless, Issue Managers or Focal Points are not a panacea. Law enforcement agencies must also change the way they analyze the foreign intelligence information they receive. At its core, intelligence is a mosaic. Broad pictures can be painted and long-term trends identified, but frequently only by putting bits of information together over time. In contrast, law enforcement is action-oriented, inherently reactive, and focused on specific facts, rather than long-term analysis. As a result, law enforcement agencies at times lack the analytic capability or resources to integrate what may be thousands of disparate pieces of foreign intelligence collected over time on a given subject.

Compounding this problem is the fact that the Department of Justice now has very little capability to store, track, and retrieve the extensive amount of foreign intelligence information it presently receives. Foreign intelligence information that does not relate to a matter of immediate interest is often destroyed shortly after receipt in order to avoid problems of classified information storage. Thus, an item of foreign intelligence that Justice receives today is likely to be unretrievable if and when it becomes significant later in an investigation.

There are no easy solutions. At a minimum, however, a strategy must be designed to make better use of the respective interests, expertise, and analytic approaches of the two communities in subject matter areas of overlapping interest.

C.(3) Question Raised: Should Crimes Reporting Procedures Be Revised?

The Intelligence Community's crimes reporting obligations are set out in 28 USC. 535, Executive Order 12333 and several implementing MOUs between the Attorney General and the DCI, Secretary of Defense, and Director of NSA.[6] Taken together, these laws and implementing procedures require Intelligence Community agencies to report to the Justice Department all information tending to show: (1) possible violations of Federal criminal law by Intelligence Community employees, and (2) possible violations of certain selected Federal criminal laws by nonemployees.

A substantial majority of the Task Force has concluded that the existing crimes reporting procedures should be modified to:

- Eliminate reporting on *de minimis* violations of law.

[6] Intelligence Community Inspectors General, especially so-called "statutory" IGs, have separate defined responsibilities to investigate and report to Justice as well as Congress regarding possible crimes by IC personnel and others. The Task Force considered these discrete IG responsibilities as outside the mandate of the Task Force. Accordingly, none of the findings, conclusions, or recommendations contained in this section are intended to reflect or apply to crimes reporting responsibilities of these Inspectors General.

- Cut down on duplicative or redundant reporting.
- Ease the onerous administrative burden imposed on both communities by the current system.

The current crimes reporting obligations originated at a time when the Intelligence Community disseminated far less information to Law Enforcement agencies than is the case today. Further, the Intelligence Community sought to deliver reports of possible crimes directly and exclusively to the Criminal Division of the Department of Justice because intelligence officials lacked confidence in Law Enforcement's overall ability to safeguard intelligence sources and methods. In recent years, the volume of these crimes reports, particularly from CIA to Justice, has increased exponentially; at the same time, the seriousness of the crimes reported has declined. In the majority of cases, these crimes have been discovered during initial security processing of applicants for employment or in routine security reinvestigations of current employees and, in many instances, relate to *de minimis* instances of personal misconduct in the distant past. Such reports often fall below the guidelines for Federal investigation and prosecution and are thus not pursued. Nonetheless, the current procedures compel reporting of even such trivial, outdated information about employees, contractors, and applicants, notwithstanding the fact that the statute of limitations may have run or that prosecution is otherwise a practical impossibility. In short, significant time and resources are wasted by both sides under the current system.

Meanwhile, the volume of foreign intelligence reporting disseminated to Law Enforcement agencies has increased dramatically. This reporting has covered a wide variety of topics and activities from terrorism to economic crimes. Possible violations of Federal laws by nongovernmental persons that are the subject of crimes reports to Justice have often already been covered in the intelligence reports now routinely sent to US investigative or regulatory agencies. Thus, whatever concerns the Intelligence Community may have harbored in the past about law enforcement agencies' capability to protect sources and methods seem to have dissipated, taking with them a major reason for maintaining a separate and formal crimes reporting channel to the Criminal Division. This changed environment requires a fresh look at a number of issues:

- Is the routine dissemination of intelligence to law enforcement entities adequate, or must a formal "crimes report" be made to Justice as well?
- What crimes must be reported?
- What amount of information is sufficient to require a crimes report?
- Is the Intelligence Community adequately trained always to recognize an expanding list of criminal activities of concern to US law enforcement?
- Must intelligence officials be able to recognize information of interest to law enforcement as well as determine when a crime has actually occurred?

In short, the original circumstances and rationale behind the Intelligence Community's crimes reporting obligation and procedures have changed; modification is necessary and overdue.

Several approaches were considered by the Task Force. At a minimum, if a formal crimes report program continues, the Task Force concluded that new MOUs with updated reporting standards are needed. With the exception of the FBI, the Task Force believes that the best overall approach would be to limit an intelligence agency's crimes reporting obligation to Justice to the following:

- All possible significant violations of law by officers, employees, contractors, or agents within the Intelligence Community.[7] Such a standard

[7] DOD has for some time taken the position that the special reporting requirements contained in the DOD/DOJ Memorandum of Agreement should only apply when the employee, contractor, or agent is engaged in an intelligence activity when the offense is committed. Other reporting requirements already compel reports by DOD to DOJ on certain types of Federal employee criminal activity, regardless of whether the employee is a member of the Intelligence Community. DOD questions the value in adding to the preexisting requirements a requirement to report crimes committed by Intelligence Community personnel that are not linked to intelligence activities.

would have to be established consistent with 28 U.S.C. 535, which sets criteria and limitations regarding the reporting of federal crimes involving Government officers and employees.[8]

- Information on possible specific, significant, enumerated violations of Federal law by third parties acquired in the course of foreign intelligence collection activity or personnel security processing when such information does not meet requisite criteria for dissemination (for example, reliability, specificity, and policymaker interest) as an intelligence report.

Deciding what to report can cause a bit of a dilemma to an IC officer in the field. These officers, who are performing intelligence-gathering functions and are, further, prohibited by law from performing law enforcement functions, cannot be expected to focus on every possible violation of a federal statute that may possibly have been committed by third parties. On the other hand, some information is of obvious crimes reporting value—such as terrorist activity affecting US persons or interests. Also, under current guidelines, many of the current crimes reporting requirements are (and will continue to be) foreign intelligence requirements and will be reported through intelligence disseminations. For the other relatively small category of crimes which fall outside of formal intelligence dissemination, the relevant MOUs should be revised to reflect a short, precise list of significant reportable crimes. Under this approach, all other information relevant to the Law Enforcement Community, whether reflecting actual criminal activity or not, becomes part of the normal intelligence dissemination process.[9]

[8] A variation to this solution favored by some involved continuing the dissemination now in place but doing so through a focal point or center combining representatives of both communities. In this way, information of possible relevance to Law Enforcement agencies could be disseminated and reviewed, drawing upon the legal expertise of Law Enforcement agencies and the analytic capability of the Intelligence Community.

C.(4) Question Raised: What Is the State of Information Management Capabilities in the Law Enforcement Community?

Serious flaws in the Law Enforcement Community's information management systems were studied by the Information Management Group of the Law Enforcement side of the Task Force. This group analyzed the volume and nature of Intelligence Community cable traffic routinely received by the Law Enforcement agencies as well as the divisions of the Department of Justice.

Initiatives to improve the flow of intelligence information to law enforcement are dependent on adequate information management systems in both communities. Intelligence information must be transferred in a secure and timely fashion. Law Enforcement agencies, after initial review, must have information management systems that retain and account for the data to permit review and evaluation as investigations develop.

The Departments of Justice and Treasury together receive over 79,000 cables a month through 10 primary entry points covering a wide array of subjects. Cable recipients say that a significant portion of this traffic is of minimal current relevance to law enforcement and thus is put to little use. In large part, this is attributable to the fact that

[9] The larger investigative roles played in recent years by Intelligence Community Inspectors General lend further justification to a change in the crimes reporting threshold. Currently, the relevant MOUs require the Intelligence Community to report any allegations that "are clearly not frivolous or false." In light of the thorough and rigorous investigative activities conducted by Intelligence Community/IGs, this threshold is too low. With respect to possible crimes in connection with Intelligence Community employees, programs, or activities, the standard could be properly changed to that under which the CIA Inspector General now operates, that is, "a reasonable basis to believe that a Federal crime has been committed." In addition, the reporting threshold for possible crimes that do not go through the IG should be based on DOJ prosecutorial guidelines so the Intelligence Community agencies do not report possible offenses that have no realistic chance of being prosecuted. There should be sufficient information on which the DOJ can either act directly or conduct an independent investigation. Fragmentary information alone is of little value

once information on a subject has been requested by a law enforcement representative, the representative (or his successor) may be reluctant to turn off the flow months or even years later even if there no longer is any need for it.

The ability of Justice, Treasury, and their components to account for the flow of this traffic varies widely. FBI, DEA, and the US Customs Service use automated message handling systems. In contrast, cable traffic received electronically at the Telecommunication Services Center in Justice is printed in hard copy, manually logged by a Center employee, and disseminated through the internal mail process or by courier. No standard cable delivery approach exists: some cables go to named addressees; others are delayed while employees make judgments about the appropriate recipient. An individual receiving the report frequently has no idea why it has been provided or what should be done with it. Logs in the Telecommunications Center are routinely destroyed after 90 days, and there is no storage capability. As a result, some individual components of Justice have created *ad hoc* systems for review and storage of cable traffic to meet their own specific requirements.

The Task Force concluded that the Law Enforcement Community, particularly Justice, must establish a more effective method of handling and evaluating cable traffic to ensure the proper consideration and routing of information transmitted from the Intelligence Community and particularly to ensure that those Law Enforcement components that need the cables actually receive them. Full automation of the process of receiving, storing, and retrieving cable traffic would be the most cost-effective approach to this problem. Meanwhile, even before an automated system is put in place, the present cable traffic should be periodically "pruned" to eliminate the flow of cables no longer relevant to law enforcement needs.

Phase Two

Collection of Specific Intelligence Information Relevant to Ongoing Investigations

A. How Can Law Enforcement Obtain Information From the Intelligence Community Relevant to Ongoing Investigations?

As indicated in the discussion of "Phase One" issues, there is widespread consensus within both communities that Law Enforcement should continue to participate in the strategic foreign intelligence collection requirements process, and that the quality of that participation should be enhanced. More complex, however, are the issues surrounding Law Enforcement's ability to obtain information collected by the Intelligence Community that relates to ongoing law enforcement investigations. Bound up with this subject is the question whether Law Enforcement may direct intelligence agencies to collect "case-specific" information.

Such "tasking"—where a law enforcement agency asks an intelligence agency to focus its collection on a specific law enforcement target—raises serious legal and practical concerns. The first subsection of this Part explains those concerns, and the second subsection suggests an alternate framework for satisfying the information needs of law enforcement consistent with applicable law.

A.(1) Concerns Presented by Law Enforcement Tasking of Intelligence Community Resources

A. (1) (a) Legal Concerns

There are statutory and constitutional restrictions on whether and to what extent intelligence agencies may collect information for law enforcement purposes. Many types of intelligence collection techniques—electronic surveillance, unconsented physical searches, and mail surveillance, for example—would constitute a "search" or "seizure" within the meaning of the Fourth Amendment if done for law enforcement purposes. The courts have

consistently ruled that if the Government wishes to exploit such a technique against a US person, or within the United States, for the sole or primary purpose of law enforcement, it must first obtain a warrant based on a showing of probable cause of, *inter alia*, actual or imminent criminal activity.[10] That is not, however, true with respect to searches or seizures of the property of non-US persons outside the United States.[11]

With respect to electronic surveillance, the issue is complicated by the strictures of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, 18 USC. §2510 *et. seq.* That statute makes electronic surveillance a Federal felony offense, save under specified conditions, of which the most notable is conducting such surveillance pursuant to an order from a US District Court. Section 2511(2)(f) of Title 18 specifically exempts from Title III, however, " . . . the acquisition by the United States Government of foreign intelligence information from international or foreign communications . . ." Thus, intelligence agencies require no court order for overseas electronic surveillance, *provided they are engaged in such activities for foreign intelligence purposes*, but would have to be concerned about Title III if they were to conduct electronic surveillance primarily for nonforeign intelligence purposes. With respect to other kinds of "search and seizure" activities, the basic rule continues to be that Fourth Amendment protections apply to US persons and to activities within the United States but not to activities affecting non-US persons outside the United States.

Outside the context of searches and seizures, the legal risks of utilizing foreign intelligence collection resources for law enforcement purposes are less clear, though by no means negligible. CIA, for example, is forbidden by the National Security Act of 1947 from exercising any "police, subpoena or law enforcement powers, or internal security functions." 50 USC § 403-3(d)(3). Nevertheless, it may be that CIA is permitted under certain circumstances to collect intelligence for the primary purpose of law enforcement, as long as there is some valid foreign intelligence or counterintelligence purpose for the collection.[12] Similarly, DOD agencies other than NSA might be able to collect case-specific information to assist Law Enforcement under certain circumstances without running afoul of the Posse Comitatus Act, 18 USC. § 1385 (which prohibits use of the armed forces to execute the criminal laws within the territory of the United States). In sum, outside the area of searches and seizures (primarily electronic surveillance) and their attendant Fourth Amendment restrictions, the "primary purpose" test may not apply, suggesting greater (but not unlimited) flexibility from a legal standpoint in using foreign intelligence collection resources to gather case-specific information.

A. (1) (b) Concerns Relating to Sources and Methods

Apart from legal concerns, tactical collection tasking by Law Enforcement of the Intelligence Community raises serious questions about the protection of sources and methods. At present, when an intelligence agency provides information to an LEA, it typically does so in accordance with a "lead purposes only" principle: the LEA may use the information to develop leads in an investigation, but not in any other way (for example, not as a basis for obtaining a search warrant and not as part of the Government's case in chief). Thus far, this restriction has been important to the protection of intelligence sources and methods in at least two

[10] See, for example, United States v. Truong, 629 F.2d 908, 915 (4th Cir. 1980) (warrantless electronic surveillance is permissible under the Fourth Amendment only if the surveillance is conducted "'primarily' for foreign intelligence purposes"); United States v. Butenko, 494 F.2d 593, 606 (3d Cir.) (en banc), cert. denied, 419 U.S. 960 (1974) (same)

[11] United States v. Verdugo-Urquidez, 110 S.Ct. 1056 (1990).

[12] DOD believes that the concept of authorizing an intelligence agency to collect intelligence for the primary purpose of law enforcement, as long as there is some valid foreign intelligence or counterintelligence purpose, notwithstanding the legal caveats, poses substantial dangers arising from the perception of the intelligence agency as an agent for law enforcement. This may jeopardize intelligence sources and methods. In DOD's view, the concept would shift the whole purpose of the collection from that of foreign intelligence collection in the interests of national security, to that of law enforcement, and would eliminate the "incidental" law enforcement aspect when collection is done solely for the purposes of foreign intelligence in the national security interest

respects. First, it puts everyone on notice that sensitive sources and methods are involved and that none of the information should be used as part of the case in chief. And second, it allows the Intelligence Community to keep some distance from investigators and prosecutors, helping to convince the judge that the defendant has not been disadvantaged by being denied access to information made available to the prosecution.

But if the information in question was provided to an LEA as the result of direct collection tasking of the intelligence agency by Law Enforcement, it will probably be impossible to enforce the "lead purposes only" restriction. For reasons elaborated in greater detail in the discussion of Phase 3 below, if an intelligence agency were to accept tactical collection tasking from Law Enforcement and then hand over to Law Enforcement the product of that collection, a court would be more likely to find that (a) the intelligence agency had acted outside the scope of its authority and/or (b) the defendant was entitled to discovery of the intelligence agency's records. Although CIPA provides safeguards in that contingency, sources and methods will, nevertheless, be placed at some level of risk, a risk that could have been avoided had the tactical collection tasking been avoided.

A.(2) Law Enforcement Supplying Target-Specific Information to the Intelligence Community: A Constructive Alternative to Tactical Collection Tasking

There is, however, a way Law Enforcement can derive the benefits that would result from "tactical tasking" without the associated legal and practical costs. Instead of asking or directing an intelligence agency to collect information on a particular target, Law Enforcement can supply an intelligence agency with specific lead information—such as a telephone or telex number, a name, or an address—which will enable the intelligence agency to gather information on that target. The intelligence agency, on receiving the target-specific information, can determine whether exploiting that information will lead to the collection of foreign intelligence or counterintelligence information covered by one or more intelligence collection requirements. (For "search and seizure" collections, the intelligence agency can determine whether the primary purpose of the collection will be the collection of foreign intelligence or counterintelligence information.) If the intelligence agency determines that the target-specific information can be used that way (for example, because it will help the agency collect information about terrorism, arms proliferation, or the foreign aspects of international narcotics trafficking), the intelligence agency may then use the information and supply the resulting intelligence to all consumers who ordinarily receive intelligence information collected on the subject at issue, including, in all likelihood, the LEA that supplied the target-specific information.

This process allows the intelligence agency to determine whether the target-specific information will be exploited to serve a foreign intelligence or counterintelligence purpose, which foreign intelligence requirement the collection serves, and which consumers will receive any information collected. These distinctions ought to reduce the legal and practical concerns presented by direct tactical tasking because it keeps Law Enforcement at an appropriate distance from the analysis and decision about whether to gather specific intelligence. So long as that analysis and decision is made by an intelligence agency using appropriate criteria, it is less likely a court will find Fourth Amendment or other legal problems. Similarly, if the collection decision is undertaken in this manner and the information collected is distributed to a variety of intelligence consumers, not just the LEA that supplied the target-specific lead information, a court will be less likely to view the intelligence agency as part of the law enforcement investigation. This, in turn, will reduce the chances that the intelligence agency will be subject to discovery by a defendant charged as a result of the investigation.

The legal and practical problems surrounding Law Enforcement–Intelligence Community cooperation

in the area of collection are complex. As a result, there has been a great deal of caution and uncertainty within each community about how to cooperate. The Task Force has concluded that the legitimate, lawful needs of Law Enforcement for intelligence information relating to ongoing investigations may be served without imposing the costs presented by tactical collection tasking. We recommend that a committee be established, composed of members of both communities, to develop standards and procedures to regularize and discipline interaction between the two communities at the tactical collection level. By making clear that LEAs are free to supply target-specific information to intelligence agencies, which will then make the collection and dissemination determinations, this committee can encourage and enhance lawful cooperation in this area while assuring that sources and methods are adequately protected.[13]

Phase Three

Preindictment Prosecution Requests for Information

Once a prosecution becomes a probability, even before return of an indictment, the third phase begins. From this point on, it is fair to say that the primary driving force for any intelligence collection or provision of information respecting the specifics of the case is likely to be law enforcement, notwithstanding any continuing foreign intelligence interest.

Here the communities must carefully consider, *first*, whether intelligence agencies can and should be used to engage in additional affirmative evidentiary collection, and *second*, the extent and appropriateness of responding to law enforcement requests to search *existing* intelligence databases for information bearing on the case. Moreover, for the first time, they must deal with the prosecutor, who is unlikely to have had much prior experience with the Intelligence Community.

A. An Overview

Once prosecution becomes likely, the wisdom and legality of further foreign intelligence collection must be judged in light of the probable impact of a later public trial.

Two threshold questions arise. *First*, does the Intelligence Community have the authority to continue further intelligence collection, and, if so, how will the method of collection satisfy the Constitutional and statutory requirements normally imposed upon criminal investigations? If the primary purpose for further information collection is law enforcement with its attendant procedural restrictions, the best course may be to cede all further collection to law enforcement agencies notwithstanding the presence of a legitimate foreign intelligence interest.[14]

Second, are intelligence sources and methods endangered if collection continues and a prosecution results? Here again, wisdom may counsel turning erstwhile intelligence resources and assets over to law enforcement. This may be easier said than done, since intelligence agencies understandably are

[13] Of course, apart from disseminating information, the Intelligence Community can and does assist Law Enforcement by, inter alia, (1) participating in counterespionage, counterterrorist and counternarcotics activities unless otherwise precluded by law; (2) detailing expert personnel and lending equipment; and (3) rendering any other assistance and cooperation to law enforcement authorities not precluded by applicable law. See E.O. 12333, Part 2.6(a), (c), and (d); see also the Economy Act, 31 U.S.C. §§ 1535-1536 (authorizing the head of an agency to order goods and services from another agency under specified circumstances and procedures)

[14] The FBI believes that, in circumstances in which a counterintelligence investigation may result in a criminal prosecution, as, for example, when a US person is investigated for conducting espionage on behalf of a foreign power, utilizing a mechanical "primary purpose" test may not be appropriate or helpful. FBI believes, rather, that if substantial counterintelligence interests and needs warrant continued collection, then a counterintelligence investigation can and probably should continue, notwithstanding that a criminal prosecution is virtually certain. In the FBI's view, there will be circumstances in which an FBI counterintelligence investigation has established that a US person is violating the espionage statutes, but additional information regarding the activities of the foreign power at whose behest he is doing so will be acquired through continued use of intelligence collection methods and authorities

reluctant to cede control of their own assets, and the intelligence agencies may have continuing foreign intelligence reporting responsibilities regarding related matters that preclude their withdrawal from collection and analysis.

There is an additional factor to consider in this area. Often, intelligence agencies find that they have already collected information of significant value to prosecutors when asked to look for evidence in support of a prosecution. Prosecutions focused on foreign narcotics trafficking or international terrorism are the most obvious examples. This preexisting intelligence information may be valuable because it can direct law enforcement to a particular human or documentary source of material evidence; because it may suggest further lines of inquiry; or because it reflects increased or diminished culpability of subjects of the investigation. For these reasons, whenever it is likely that intelligence information relevant to a matter nearing prosecution has already been collected, law enforcement must consider whether to request a review of Intelligence Community data bases. Because these data bases are compartmented and are designed and maintained for operational security—not for assisting prosecutions—the "file search" issue has been at the center of several fractious episodes involving the Intelligence and Law Enforcement Communities in recent years.

B. Question Raised: How Can File Searches Be Improved? Some General Principles and Practical Implications of File Searches

Unfocused or unnecessary excursions into the Intelligence Community files can have potentially devastating effects on the operations of the requested agencies, as well as on the actual legal case, for several reasons:

- Searches of Intelligence Community files, if not adequately narrowed, can tie up information retrieval capabilities for huge periods of time.
- If requests are not framed to take into account the agency's information retrieval criteria, searches may not yield all relevant information.
- Massive prosecutorial acquisition of Intelligence Community information may unnecessarily put sources and methods at risk because such information will normally be subject to defense discovery demands. Such information is thus likely to spawn time-consuming discovery battles.
- In seeking information from files, prosecutors must recognize that some categories or particular pieces of information potentially supportive of a criminal prosecution or exculpatory to the defense cannot under any circumstances be introduced as evidence at trial because of the risk posed to sensitive intelligence sources and methods by public disclosure. If such intelligence information includes sensitive sources or methods that cannot be revealed at trial without serious harm, the prosecution must be prepared to block introduction of the information, even if that means the prosecution must be dropped. If a prosecution must be aborted on these grounds, the Classified Information Procedures Act requires a report to the Congress.

From the foregoing, it is clear that a prosecutor should not request a search of Intelligence Community files without first understanding how a search must be structured and conducted, what it could potentially yield, and the resource burden it poses. Also, the prosecutor, in making his request, must articulate to the intelligence agency with specificity the nature of the information being sought—precise names, dates, places, and events—as well as the reasons for the search. For example, the prosecutor should make clear at the outset whether the search is to gather information supporting the prosecution or to anticipate discovery rights of a possible defendant. In short, each search raises different issues.

C. The Role of the Justice Department and the US Attorneys in Review of Intelligence Files

Occasionally, a US Attorney's Office and/or the Department of Justice learns that an Intelligence Community agency has potentially relevant information in its files regarding an imminent prosecution. The prosecutor needs to review such information to ensure a complete investigation and a fair opportunity for defense discovery, as well as to avoid duplicative requests to Intelligence Community agencies.

Two issues arise:

- How can the Department of Justice ensure timely coordination between US Attorneys and Intelligence Community agencies?

- Can the Department of Justice require notification of individual prosecutions by responsible US Attorneys' Offices to help ensure Washington-level awareness of investigations about which relevant intelligence may exist?

Effective, reliable, and secure information resources management inside the Justice Department is an essential component of the first issue. As noted earlier, however, Justice needs dramatic improvement in its capability to track, retrieve, and appropriately disseminate case-relevant information from Intelligence Community agencies. Only with such capability in hand can relevant components and affected US Attorneys' offices be promptly made aware of such case-relevant intelligence information. Nonetheless, no matter how sophisticated and well-coordinated, no law enforcement system of information management will be foolproof. To ensure that prosecutors are not surprised by relevant intelligence information, Intelligence Community agencies must also improve their tracking and retrieving of relevant data, even if it means creating redundant systems to identify information that has been previously provided to the Law Enforcement Community.

The second issue—notifying Main Justice of significant investigations in US Attorneys' Offices—involves more than information management systems. Traditionally, US Attorneys enjoy and insist on substantial independence; they investigate, present, and prosecute most cases without Main Justice prior approval or control. Even so, some categories of cases involving Intelligence Community information (for example, espionage or terrorism) already require preindictment coordination with the Criminal Division. Thus, there is precedent for requiring Department level coordination of specific categories of prosecutions.

D. "Prudential" Searches by Prosecutors

In recent years, another kind of search request has become common. The "prudential search" seeks information relevant to the prosecution not only *prior to* indictment, but also without any indicia of an intelligence connection to the case. Properly used, the prudential search helps to identify and manage potential classified information problems *before* indictment and trial. It allows prosecutors to tailor indictments to reduce or eliminate the relevance of the classified information. In some cases, the search may uncover intelligence information which will persuade the prosecutor not to seek the indictment at all.

The growth in overlapping interests of the Intelligence Community and Law Enforcement has contributed to the dramatic increase in prudential searches. This increase results from several recent "high profile" cases in which a prosecutor was surprised to find classified information apparently at the center of a prosecution in a way that had not been anticipated. Excessive caution by prosecutors has been the response, accompanied by an overuse of prudential searches. Traditionally sought only when the prosecutor had a reasonable basis to conclude that the Intelligence Community agency was involved in the case and therefore might have pertinent information, prudential search requests are now being made in cases in which there has been no prior Intelligence Community participation and with

no indication that an intelligence agency may have relevant information. Moreover, some prosecutors, unfamiliar with the Intelligence Community, seek to avoid the possibility of BNL-like controversies suddenly arising late in their prosecutions and have resorted to "fishing expedition" queries to the Intelligence Community as a form of preindictment insurance.

These requests have spawned serious problems. The requests themselves are often vague or overbroad and either cause an unacceptable drain on Intelligence Community resources or cannot be fulfilled at all. Intelligence Community agencies have a finite capacity to search their records systems, and the technology and software in place is designed to satisfy intelligence demands, not those of prosecutors under the case law of *Brady*, Rule 16, or Jencks.[15] Moreover, pursuant to 18 USC. § 3504, the US Government must search records for any evidence of "unlawful" electronic surveillance of a defendant.[16] Some recent records searches required by prosecutors have been so massive that they have interfered with the intelligence agencies' ability to handle data for intelligence functions. This state of affairs cannot continue. While the Intelligence Community recognizes the authority of a court to enforce the defendant's discovery rights, the Community should not be required to conduct record searches based on little more than a hunch or whim.

[15] *Brady v. Maryland*, 373 U.S. 83 (1963), and its progeny, require the prosecution to produce to a criminal defendant evidence in the possession of the government that is favorable to the defendant on the issue of guilt or punishment, or that impeaches the credibility of a government witness.

Rule 16 of the Federal Rules of Criminal Procedure requires the prosecution to produce to a criminal defendant the following types of information that is within the possession, custody, or control of the government: (1) statements of the defendant that are relevant; (2) a copy of the defendant's prior criminal record; (3) documents and other tangible objects that are material to the preparation of the defendant's defense; and (4) the results or reports of physical, mental, or other tests that are material to the preparation of the defendant's defense.

The Jencks Act, 18 U.S.C. § 3500, requires the prosecution to provide to a defendant statements of a government witness that relate to the subject matter of the witnesses testimony.

[16] But such searches are normally limited to seven specified Federal law enforcement agencies

The Task Force concluded unanimously that far greater discipline is required before broad "prudential" searches are demanded of Intelligence Community records. What type or level of search is "reasonable" provoked considerable discussion, however. Most members of the Task Force believe that policies in this area must be developed in a "case-by-case" fashion, creating something akin to a common law of intelligence search obligations. Others, arguing that generally applicable standards can be established, favor adoption of the so-called "alignment principle"—a judicial doctrine that limits a prosecutor's duty to search for information only to those agencies that "aligned" themselves with the prosecution by participating either in the criminal investigation of the defendant or in the post-indictment prosecution effort.

Use of the "alignment principle" as the basis for determining whether files of any given Intelligence Community agency must be searched was the subject of sufficient attention and debate within the Task Force to merit its discussion here.

E. The "Alignment" Principle

A prosecutor must provide to the defendant information "in the possession of the government" that is exculpatory, as well as the statements of the defendant or a government witness, and certain other information of direct relevance to the defense case under, *inter alia*, *18 USC. 3504*; *Brady v. Maryland*; Rule 16, Federal Rules of Criminal Procedure; and the Jencks Act. A number of courts have held, however, that the Government's Brady, Rule 16, and Jencks Act obligations extend only to the files of a government agency that has been an investigative arm of the prosecution, or has otherwise participated in that particular case, (for example, by providing a prosecution witness). These cases stand for the proposition that such an agency is "aligned" with the prosecution and, therefore, subject to the same obligations that would

apply directly to the prosecution and investigating agencies.[17]

Consequently, some Intelligence Community members of the Task Force argue that, if an Intelligence Community agency has not previously provided prosecutors or their investigators with information or otherwise participated in the investigation or prosecution of the particular case, the prosecutor is under no obligation and correspondingly should not be permitted to search Intelligence Community files even for information that, if found, would otherwise have to be disclosed under *Brady*, Rule 16, or Jencks. Moreover, even where an intelligence agency has had some involvement with the case, the argument is further made that the prosecutor should first determine whether the scope of involvement is enough to have "aligned" the agency with the prosecution. Only then, the argument goes, is the prosecutor under a legal or constitutional duty to require a search of the agency's files. Where there is no such duty, the prosecutor should not request a search.

The Justice Department has serious reservations about adopting the "alignment" principle as the dispositive criterion to determine whether a "prudential" search of Intelligence Community files should be undertaken. First, Justice contends that it is not clear what type or level of Intelligence Community involvement will constitute "alignment" in a given case. Intelligence Community involvement, after all, can range from supplying the prosecution with foreign intelligence information that directly bears on the guilt or innocence of the defendant to providing the prosecutors with only a general background briefing on political conditions in a foreign country. (The former probably constitutes alignment, and the latter probably does not.) Thus, while Justice endorses the need to ease the burden on Intelligence Community agencies by limiting, so far as possible, the scope of prudential searches, it does not believe the alignment doctrine can be applied as a litmus test to determine whether a prudential search of Intelligence Community files is warranted in any given case.

Accordingly, Justice is not prepared to accept the "alignment" principle as the dispositive criterion for determining the propriety of all prudential search requests. In the view of Justice, the better approach is careful case-by-case scrutiny in which the alignment principle is considered along with other factors and more vigorous resistance to excessive gratuitous searches of Intelligence Community agency files—not only with respect to prudential searches by prosecutors, but also in the defense discovery arena as well.

For its part, DOD suggests that adequate criteria could be developed to allow reasonable application of an "alignment" theory. DOD believes that criteria could be adopted similar to that developed under the Posse Comitatus Act lines, where the armed forces cannot participate directly in law enforcement activities (for example, arrest, search and seizure). DOD envisages a "bright line" test, whereby any *direct support* provided to LEAs by IC agencies would trigger the search and other consequences of "alignment;" any direct participation in the criminal investigation, prosecutoral preparation, and prosecution of the case would be sufficiently clear to establish the required "bright line."

The Task Force has concluded that a small committee should be created to develop guidelines for determining whether and how intelligence agency records should be searched in particular cases. The committee should be charged with identifying the factors to be considered in making these case-by-case determinations, identifying the factors that should be considered in determining whether alignment exists in a particular case, and determining the significance that should be attributed to the lack of alignment in a particular case.

[17] See, for example *United States v. Brooks*, 966 F.2d 1500 (D.C. Cir 1992).

F. The Need for Both Sides To Work Together

Finally, both communities agree that, regardless of the standard used for permitting prudential searches, the searches themselves must be conducted with maximum focus and coordination. At the outset, prosecutors must define their search requests carefully and in writing to avoid misunderstandings and misdirected searches. The ability of an intelligence agency to conduct a timely and thorough search will be affected by the specificity with which the request is framed and the "leadtime" provided to fulfill it. Because an Intelligence Community agency cannot be expected to retrieve immediately every conceivably responsive piece of information in its files, the prosecution must be as specific as possible about the nature, dates, and locations of the charged offenses, and provide biographical data on the relevant persons. More generally, a coordination mechanism may be required to enforce discipline and achieve a standard approach among prosecutors around the country.

To this end, the Task Force is convinced that centralized, intercommunity focal points must be established to facilitate enhanced communication and cooperation in the search of Intelligence Community files for litigation purposes and the use of classified information in litigation.

Although focal point missions and structures will require further definition, the Task Force reached consensus on four points:

- *First*, prosecutors' search requests should be reviewed early on by focal points to ensure they are clear, specific, and practicable; whenever possible, requests should be in writing.

- *Second*, focal points should prioritize multiple requests so that they are addressed in proper order to safeguard limited Intelligence Community resources and balance the needs of different prosecutions.

- *Third*, focal points should identify overlapping or duplicate requests from prosecutors pursuing similar intelligence issues (for example, export control violations concerning Iraq) with the goal of permitting a single, consolidated search.

- *Fourth*, after the focal points have properly prioritized and formulated a search request, US Attorneys' Offices and Intelligence Community agencies must work directly with one another up to and during the trial.

Phase Four

Postindictment Use and Protection of Intelligence Information During Prosecution

Each community's equities face the greatest risk after an indictment has been returned. For Law Enforcement, a prosecution may have to be abandoned if relevant sensitive intelligence information is ordered disclosed at trial; for the Intelligence Community, sensitive sources and methods may be exposed, and thus compromised, if they become central to a prosecution. One Task Force working group looked specifically at existing practices that can assist prosecutions implicating intelligence interests. The Task Force then reviewed these practices to determine whether any should be updated or discarded altogether in favor of new approaches designed to protect Intelligence Community information. The key issues were the expansion of the provisions of the Classified Information Procedures Act (CIPA), an expanded role for Intelligence Community lawyers in court, and the use of covert intelligence officers as witnesses.

A. Should CIPA Be Expanded?

The Task Force focused on whether CIPA should be amended or replicated to apply in other fora, such as Federal civil litigation; state court criminal trials and Immigration and Naturalization Service (INS) deportation proceedings.

CIPA was enacted to provide a procedural mechanism for use in Federal criminal trials involving classified information. The statute requires that the relevance of such classified information to a prosecution be resolved through the use of pretrial procedures in a nonpublic forum. While the statute does not eliminate the tension that arises whenever classified information becomes relevant to a criminal prosecution, it does lend rigor and predictability to the use of classified information in a prosecution. Under CIPA, the government can be assured that no classified information will suddenly surface during the proceedings, by preserving the option of proceeding with a prosecution or, if necessary, abandoning part or all of the indictment in order to protect classified information.

CIPA offers a step-by-step procedure by which the government may litigate, first, the discovery, and then the use at trial, of classified information. This step-by-step approach allows the government to reassess the potential risk of exposure of classified information at trial as matters develop. CIPA also provides protective mechanisms (for example, redactions, substitutions, and stipulations) to protect classified information in trial while yet allowing the introduction of necessary facts. Thus, the government can avoid the "disclose-or-dismiss" dilemma. If necessary, interlocutory appellate court rulings on discovery and evidentiary matters are available. The essence of CIPA is that the government retains complete control over the disclosure of classified information at all times by requiring the court, to the extent possible, to make pretrial rulings on relevance and on the permissibility of using an unclassified substitute or stipulation at trial in lieu of classified information.

After more than a decade of use, CIPA was judged to be an unqualified success by the Task Force. There was support in both communities for an extension of CIPA protections into other proceedings. For instance, although CIPA does not expressly cover pleas and sentencing hearings in Federal courts, the government to date has successfully argued on several occasions that it applies during those phases of the criminal trial.

In other contexts completely removed from the Federal criminal process, no procedures comparable to CIPA exist. Leaving aside mutual agreement, the only formal legal means to protect classified information is an assertion of the state secrets privilege, and both communities recognize that the privilege should be invoked sparingly as a last resort. Some Task Force participants, accordingly, suggested creation of procedures similar to CIPA for use in Federal civil litigation. However, such a "civil CIPA" remedy has provoked considerable opposition in the past. The Intelligence Community and the Justice Department's Civil Division historically have opposed extending CIPA to civil cases as unnecessary, burdensome, unworkable, and arguably an approach which would erode the viability of the state secrets privilege.

Specifically, those opposed to a civil statute analogous to CIPA point out that the Civil Division is already well-positioned to forge compromises with civil litigants whose discovery requests call for the production of classified information. For example, such a litigant often can be persuaded to narrow the scope of a discovery request so that the request does not encompass classified information but still provides the information he needs. The possibility that the government will invoke the state secrets privilege provides the litigant with a powerful incentive to reach such compromises. The opponents argue that if a civil version of CIPA were in place, the litigant might instead be inclined to take a tougher stance, invoke civil CIPA (which could be viewed as creating new discovery rights), and put the government to the effort of creating substitutions and summaries. Ironically, of course,

this might ultimately result in a more frequent assertion of the state secrets privilege because it would make it harder to reach mutually agreeable resolutions of disputes over classified information.

Those opposed to a civil CIPA also believe the benefits of such a statute are more difficult to discern than the likely costs. The Civil Division and private litigants are presently free, without civil CIPA, to agree to mechanisms incorporating CIPA-like features, which the district court can adopt in the form of protective orders. Moreover, critics of a civil CIPA believe it is unlikely such a statute would be workable, because the incentive impelling the government to prepare CIPA's substitutions and summaries are unique to criminal cases, where the government could be forced to abandon a prosecution if adequate substitutions and summaries are not submitted. That incentive is not present in a civil case, where the government may not even be a party or may be a defendant with no interest in keeping the case alive.

A second area of concern involves state criminal proceedings. In the few instances to date in which a state prosecution has implicated classified information, the Federal Government has relied on the discretion of the state courts to fashion judicial protective orders to guard the information. If a state court were to refuse to adopt appropriate procedures to protect the information, the Federal Government's only alternative would be to withhold the information altogether, placing the state prosecution at risk of dismissal.

Moreover, although the Federal Government can intervene in the proceeding to appeal a state court refusal to protect classified information, no statutory provision allows removal to the Federal courts. Thus, consideration was given in the Task Force to creating a CIPA removal procedure, like that which exists under the Foreign Intelligence Surveillance Act (FISA), at 50 USC. §§ 1806(f). This procedure would allow the Federal Government to remove to Federal court issues concerning the discovery and use of classified information implicated in state criminal proceedings in order to permit CIPA hearings and to protect the Federal Government's appellate rights. Again, however, there was considerable debate inside the Task Force about whether or not such a procedure would be either feasible or wise.

Although consensus was not reached, the two communities agreed that the expansion of CIPA in these areas merits further study. Finally, it also has become increasingly clear based on a few actual cases in recent months that study should be devoted to how to handle classified information relevant to INS removal hearings. This particular issue has already drawn the attention of Congress.[18]

B. Classified Information at Trial: The Use of Undercover Intelligence Officers as Witnesses

Greater overlap between the two communities has increased the likelihood that information obtained by intelligence officers may be relevant to a prosecution and that the testimony of those officers may be desired. The possibility of calling undercover intelligence officers as witnesses proved to be a difficult and highly charged issue inside the Task Force. The widely divergent views held by the Intelligence Community and the Law Enforcement agencies require explanation.

B. (1) Background

Undercover intelligence officers trained in the collection of intelligence from human sources represent substantial assets of the US Government. The cost of their training and support is substantial, and they must be able to work undercover (that is, without acknowledging their true names and/or intelligence affiliation), if they are to be effective. Such a capability should not be lightly compromised. Testimony in a public trial without

[18] Section 5110 of the House Crime Bill (H.R. 3355), as amended and passed by the Senate, would address this problem by establishing FISA-like procedures, to permit the use, but limit the discovery, of classified and other information, albeit only in removal proceedings involving suspected terrorists.

benefit of cover diminishes and often may end one's effectiveness as an intelligence officer. The value of these officers, even while assigned in the United States, is inexorably linked to their ability to maintain their cover. They live their lives undercover and often work in facilities that themselves have no overt connection to the Intelligence Community. Without this cover, an officer's utility for clandestinely collecting intelligence is greatly reduced; indeed both the officer's life and those of persons who cooperate with him, now or in the past, may be endangered. The Intelligence Community believes strongly that to put such an investment at risk routinely is a wrongheaded use of government resources, particularly since alternatives are often available. Moreover, the Intelligence Community considers the officer's true identity as an Intelligence Community employee to be a classified "fact" and thus must be afforded the same CIPA protections as would any other classified information.

For its part, the Justice Department has taken the position that, if these officers are required to testify in a criminal trial, the need to protect their true identities from public disclosure may clash with the constitutional rights of the criminal defendant both to confrontation of the witnesses against him and to a public trial. Further, Justice contends that having a witness testify under conditions that protect his identity may insert into the criminal proceeding an aura of secrecy that could easily influence or distract the jury.

B.(2) Intelligence Community Position

Because of the interests at stake when an undercover intelligence officer is called to testify, the Intelligence Community has urged that CIPA be strictly applied, arguing that the Department of Justice should adopt a policy that provides in every case the maximum protection possible under CIPA for that officer's identity.

The Intelligence Community considers this issue as going to the heart of its ability to perform its duties and to protect intelligence sources and methods. Indeed, Congress recognized the importance of protecting intelligence officers by directing the DCI to ensure that the risks to those involved in the collection of national intelligence through human sources are minimized (50 USC. § 403-3(d)(2)) and by enacting the Intelligence Identities Protection Act (50 USC. §§ 421-426). The Intelligence Community acknowledges the occasional need to have case officers testify in court but does not agree that such case officers must, therefore, appear before the public in true name and in unaltered or public appearance. In the Intelligence Community's view, so long as the judge, prosecutor, defense attorney, defendant, and jury are provided the case officer's true name, the defendant's right to confront his accusers is satisfied, and the case can be adequately tried without the case officer's true identity and appearance being made available to the public at large. In limited circumstances, courts have permitted witnesses to testify with protections for their true identity. For example, in *US v. George*, 1992 US Dist. LEXIS 11043 (D.D.C. July 29, 1992)(Memorandum and Order # 29), the trial judge granted the government's motion to employ certain measures to protect the true identities and/or features of intelligence officers who testified, based on statements in an affidavit from the Deputy Director of Central Intelligence that disclosure of the identities or features of these officers could: (1) jeopardize the safety and lives of the officers, their colleagues, officials of foreign governments, and foreign nationals who have been involved in intelligence activities; (2) jeopardize the security of current and past intelligence operations; and (3) diminish the effectiveness of current or future operations.[19]

Therefore, the Intelligence Community seeks a policy, perhaps published in *The US Attorneys' Manual*, that (1) prosecutors must seek to protect from public disclosure the true identity of covert officers of the US Government who must testify as witnesses in a criminal trial; and (2) such officers must testify without measures to protect their

[19] See also, *United States v. Lemetree*, 35 MJ 396 (CMA 1992), in which a general court-martial conviction was upheld even though the true identity of a government witness was not disclosed to the defense on national security grounds.

identities only with the prior approval of the Attorney General and the Director of Central Intelligence.

The Department of Defense supports the position that the Attorney General and the Director of Central Intelligence (or the Secretary of Defense, as appropriate) are the proper officials for deciding questions on the revelation of true identities of IC agents.

B. (3) Department of Justice Position

In contrast, the Justice Department remains concerned with the constitutional principles that are implicated in determining whether to protect from public disclosure the identities of government agents who testify at a Federal criminal trial. It further believes that a blanket policy is unworkable because of the nuances of individual criminal cases, including the strength of the prosecution case.

The Justice Department believes that the better approach is to review each officer-witness on a case-by-case basis in order to assess the magnitude of the government's need to protect the officer's identity and the effect on the trial proceedings of employing protective measures in a given case. The Justice Department proposes that the approval level for requests to have covert officers testify in true name in court should be that of the Assistant Attorney General, Criminal Division.

C. The Role of Intelligence Community Lawyers in Court

The SSCI Staff BNL Report placed considerable emphasis on the need for closer cooperation between the Law Enforcement and Intelligence Communities in connection with criminal prosecutions. In light of this SSCI concern, the Task Force reviewed whether Intelligence Community lawyers should play a more active role in court during pretrial litigation of matters affecting the discovery or use of classified information in criminal prosecutions. The Task Force reached a general consensus that: (1) Intelligence Community lawyers currently do play a role in criminal proceedings that involve classified information, but the significance of that role is dependent on the personalities involved in a given case; and (2) prosecutors must remain responsible for the overall management and tactical prosecution of a case but also should be encouraged to make greater use of Intelligence Community lawyers.

There was general agreement that the Intelligence Community lawyer has an important role to play in prosecutions involving classified information and that more can be done to enhance the effectiveness of that role. Coordination and clarification of search requests, preparation of materials related to CIPA proceedings, and informing prosecutors about the implications of disclosing information on intelligence sources and methods are all important functions for Community lawyers. Moreover, recent experience underscores the value of using Intelligence Community lawyers to educate prosecutors, and even the judiciary, on the activities, procedures, and functions of the Intelligence Community.

The Task Force concluded that the basic objective should be to structure the day-to-day working relationship between intelligence and law enforcement so that all concerns are effectively addressed. One useful model is that currently played by Intelligence Community lawyers in the BNL prosecutions. With the full consent of the prosecuting AUSAs, Intelligence Community lawyers provided the court with several briefings to explain CIA records systems, how CIA has conducted searches, and the results of those searches. Agency lawyers also briefed the court directly on intelligence sources and methods. However, the Intelligence Community lawyers did not argue relevancy of information or CIPA issues. Those matters remained the province of the prosecutors.

Miscellaneous Issues

Communications With Congress, Training, and Coordination

While the body of this Report has discussed the relationship between the communities in the context of specific phases, there are two issues that affect all phases of the relationship and have been cited often throughout this Report: training and education and information management. This final section discusses these issues. First, however, there should be some discussion as to whether a closer Law Enforcement/Intelligence Community relationship will affect the Intelligence Community's current relationship with Congress.

A. Communications Between the Intelligence Community and Congress Regarding Ongoing Criminal Investigations

A.(1)Background

Sections 501 and 502 of the National Security Act of 1947, as amended, require the President and the DCI to keep the House Permanent Select Committee on Intelligence (HPSCI) and the Senate Select Committee on Intelligence (SSCI) "fully and currently informed of all intelligence activities . . . including any significant anticipated intelligence activity." This provision covers a potentially wide range of human and technical intelligence activities. Section 501 also directs the President to report illegal intelligence activities and corrective action to the oversight committees, while section 502 requires the DCI to report any "significant intelligence failure." Again, the terms "illegal intelligence activity" and "significant intelligence failure" are subject to broad interpretation.

There are no formal regulations defining the circumstances under which the Intelligence Community will discuss ongoing criminal investigations with its oversight committees. Neither NSA nor DIA has faced this issue in the past. For its part, CIA generally informs the committees of certain categories of cases: counterintelligence cases involving Agency employees; criminal prosecutions against Agency officers (for example, Iran/Contra); criminal prosecutions where allegations of improper CIA behavior arise (for example, BNL and BCCI); investigations with a covert action component; highly topical items of intense media interest (for example, Noriega); and joint operations/ investigations involving substantial commitment of Agency resources (for example, Pan Am 103). In addition, CIA may alert the committees to cases where the media are likely to accuse the Agency of dilatory conduct (for example, BNL and BCCI). In each instance, the guiding principle is that the case involves an issue within the parameters of the National Security Act as outlined above and/or the traditional oversight responsibilities of the intelligence committees.

As a general rule, CIA does not provide operational information or raw intelligence to nonoversight committees but will provide finished intelligence products and analytic (as opposed to operational) briefings. Similarly, CIA does not normally brief nonoversight committees on the status of or its involvement in ongoing criminal investigations or prosecutions. On occasion, a committee (such as the House Banking Committee with respect to the BNL case) will seek access to Agency documents through the issuance of a subpoena. In such instances, CIA will consult with the White House and the Department of Justice to make an appropriate response.

A.(2)Findings/Conclusions

The Task Force determined that a number of fundamental considerations and precepts apply to the intelligence/law enforcement relationship as it involves Congress:

- The relevant statutory oversight provisions make it extremely problematic, from a legal and practical standpoint, for the Intelligence Community (especially CIA) to deny the

committees access to information, including relevant documents, about ongoing criminal investigations with significant intelligence implications, such as BNL and BCCI.

- The IC's production of information to Congress pertaining to law enforcement investigations ought to be conducted in a spirit of comity. In deciding how to respond to a Congressional request for information, executive branch agencies must balance the Congressional need to know (in order to perform its function) against the executive branch's need to protect information (in order to perform its function). No absolute rule can or should be applied to every case; each request may raise different issues and require careful negotiations with Congress to achieve a mutually satisfactory resolution. It is essential, however, for an IC agency to coordinate with the responsible law enforcement agency prior to producing to Congress information pertaining to that law enforcement agency's investigation.

- The IC (notably CIA) must improve its coordination within the Executive branch whenever it communicates with its oversight committees concerning ongoing criminal investigations or intends to provide documents originated by other agencies. With respect to committee hearings or letters sent to oversight (or nonoversight) committees pertaining to ongoing investigations, the IC will inform appropriate law enforcement agencies in advance. If a law enforcement agency objects to an IC agency communicating with its oversight committees on a particular investigative matter and the IC agency disagrees with that position, the case should be resolved by higher authorities (for example, DOJ or the White House). With respect to documents originated by other agencies, the IC must follow the "third agency" rule.

- The IC should apply substantially stricter standards before providing nonoversight committees with information on ongoing criminal investigations with significant intelligence implications. The IC's statutory obligation to inform Congress of all intelligence activities, including those with law enforcement aspects, applies only to its oversight committees. Accordingly, the IC can and should resist to the maximum extent possible attempts by other committees to make excessive and undue inquiries for information relating to ongoing investigations with significant intelligence implications. To this end, an effort should be made to encourage HPSCI/SSCI to assist CIA and the rest of the IC in responding to requests from other committees for law enforcement-related information. The SSCI has provided assistance to CIA by making their secure office space available for briefing Senators not on the Committee and by doing the briefing under S. Res. 400, which provides for the protection of classified information provided to the Committee. No similar arrangement has been made with the HPSCI since its rules do not permit HPSCI to pass along classified information received from the Executive branch to a member not on the committee unless a vote is taken by HPSCI specifically authorizing such action. Accordingly, HPSCI should be encouraged to alter these rules so as to allow briefings to be conducted in their secure office space and under rules that will ensure confidentiality of the information provided. In the absence of assistance by oversight committees in "brokering" negotiations between the IC and nonoversight committees, the IC and law enforcement sides should consider other options, including the invocation of Executive Privilege, when circumstances so warrant.[20]

[20] The NSC Staff does not agree with any suggestion that an itnelligence oversight committee can compel the IC to provide classified informaton related to a criminal investigation and that a nonintelligence oversight committee cannot. In either case, the NSC Staff believes that the issue turns on the jurisdiction of the requesting committee, its need for the information, and the President's executive privilege.

B. The "Gates Procedures"

B.(1)Background

On December 31, 1992, then DCI Robert Gates sent a memorandum to all members of the National Foreign Intelligence Board (NFIB) establishing procedures, which were coordinated with the NSC and the IC, for disseminating clandestinely collected foreign intelligence that identifies Congressional members or staff. Normally, the identities of such individuals, because they are US citizens, are removed before dissemination. Under the Gates procedures, any recipient of disseminated information (except for the President, Vice President, Secretaries of State and Defense, and the National Security Adviser), who wants to know the actual identity of a Congressional member or staffer must make a request, in writing, to the DCI, not to the originating agency. The DCI makes the decision on dissemination and, in those cases in which dissemination is approved, also notifies specified members of Congress.

B.(2)Justice Department, Including FBI, Objections

The Justice Department's concerns about these procedures are based primarily on Mr. Gates' 31 December 1992 letter that transmitted the procedures to the leadership of the House and Senate. The letter specified the circumstances under which the DCI would inform the Congressional leadership of the dissemination of intelligence information that identifies members or staff. Among the factors listed that would support dissemination was whether "the information indicates that a member of Congress or staffer has engaged in activity that is potentially criminal, unethical, or of a counterintelligence concern, *unless* the Department of Justice interposes an objection." (emphasis added).

The Justice concern is that the mechanism and criteria for Congressional notification as described in the Gates letter violate the "third agency" rule established by Executive Order 12356, pose a threat of interfering in the criminal investigative responsibilities of law enforcement agencies, and could be inconsistent with internal guidelines of the FBI.

B.(3)CIA Position

CIA disagrees with Justice for the following reasons. Section 103(a) of the National Security Act, as recently amended, specifies that the DCI shall be responsible for providing national intelligence to the President, the heads of departments and agencies of the executive branch, the Chairman of the Joint Chiefs of Staff, and where appropriate, the Senate and House of Representatives. Similarly, subsections 1.5(k), (l), and (s) of executive Order 12333 provide that the DCI shall:

- Have full responsibilities for the production and dissemination of national foreign intelligence.
- Ensure the timely exploitation and dissemination of data gathered by national foreign intelligence collection means.
- Facilitate the use of national intelligence products by Congress in a secure manner.

Despite this broad grant of authority to the DCI, CIA notes that the procedures provide that the DCI consider the concerns of other Intelligence Community agencies before disseminating their information to the Congressional leadership. CIA thus believes there is ample opportunity under the procedures for these agencies to bring their concerns to the attention of the Director before any dissemination of this information is made to the Congress.

The second concern raised by the Department of Justice involves the potential for interfering with ongoing criminal investigations or prosecutions. CIA points out that whenever this type of information is at issue, the DCI or the CIA General Counsel would first seek the permission of the Department of Justice before briefing the Congressional leadership, and, if this permission

were denied, the DCI would not undertake such a briefing. Accordingly, CIA contends that it is not possible for briefings conducted under these procedures to interfere with ongoing criminal investigations or prosecutions.

Finally, the Department of Justice expressed concern that the procedures may be inconsistent with FBI internal guidelines for briefing Congress. These guidelines require that the Attorney General or her designee approve the provision to Congress of "foreign intelligence, counterintelligence, or criminal information" by the Bureau. Again, CIA notes that the DCI would seek the permission of appropriate officials of the Department of Justice before briefing the Congressional leadership on intelligence information that indicates a member or staffer is engaged in activities of a criminal or counterintelligence concern. Thus, in these circumstances, CIA views the procedures as consistent with the FBI guidelines. To the extent there is any other "disconnect" with the guidelines, CIA suggests that the guidelines can be clarified or modified as necessary.

In short, CIA believes that the DCI, in his role as head of the Intelligence Community, has the legal authority to disseminate to the Congressional leadership intelligence information, which originated in other agencies of the Community and which identifies Congressional members or staffers, without first obtaining the permission of the originating agency. NSA does not dispute the DCI's legal authority in this area, but from a policy standpoint questions the wisdom of the IC providing this kind of politically sensitive information about one member of Congress to other members of Congress, particularly those in the opposite party. For its part, Justice (including FBI) considers the Gates procedures to be ill-advised and contrary to other existing legal guidelines. Accordingly, Justice believes they should be abolished.

B.(4) Need for a Policy Review of the Procedures

Given the separate concerns expressed by the Justice Department (including FBI) and NSA, the Task Force believes it would be appropriate for the DCI, in consultation with the Attorney General, to consider whether or not the Gates procedures should be reviewed and either abolished or amended by the NSC. For instance, the procedures could be limit reporting to Congress to only when the Congressional identity has some foreign intelligence (as opposed to domestic law enforcement or counterintelligence) value, and then only to the oversight committees.

It is important to recognize that these procedures were the product of months of painstaking coordination inside the Intelligence Community. For obvious reasons, they are a matter of great interest and sensitivity in Congress. In large part, they were established in response to a perceived concern in Congress that the Intelligence Community did not have clear and comprehensive standards in this area. Nonetheless, they also embody *significant policy judgments* arrived at by senior officials in the Bush administration, including the DCI and Attorney General. As noted above, and especially in light of the Justice Department's and NSA's concerns, the Task Force concluded that DCI Woolsey and Attorney General Reno should consider whether or not the procedures (including the accompanying Gates' letter) should remain in effect or be subjected to a policy review by the NSC. The views of the oversight committees should be solicited as part of this process.

C. Training and Cross Training

C. (1) Existing Programs: A Consensus To Expand

The Task Force believes that both the types and availability of training within the Communities about each other's responsibilities, authorities, and restrictions are inadequate. For example, only a limited number of investigators, attorneys, and paralegals within the Law Enforcement Community receive training on handling classified information under the Classified Information Procedures Act (CIPA). Commensurately, intelligence officers

receive little training on how to recognize and avoid intelligence collection activities that may unnecessarily make the officers witnesses in future prosecutions.

Within the Law Enforcement Community advanced training on the implications and use of intelligence information in criminal matters generally has been limited to FBI agents. Recently, however, this type of formal instruction for prosecutors was incorporated into courses in Narcotics Prosecutions and Complex Crimes Litigation. The Justice Department's Office of Legal Education also trains CIA attorneys on trial techniques, FOIA, and other civil litigation issues.

The basic training provided to agents and prosecutors contains little or no information on CIPA and nothing on legal or operational issues that might arise from contact with the Intelligence Community on criminal matters.[21] For many investigators and prosecutors, the learning process takes place as the need arises through their caseloads. Judges also are trained on an "as needed" basis in the application of CIPA by the Security and Emergency Planning Staff of the Justice Management Division. Although the need for training may arise unpredictably in some cases, the communities have no joint mechanism in place to assess specific needs and deliver appropriate training. The present system of informal "on the job" training is no longer adequate to meet the increasingly complex and frequent interactions of both communities.

An important first step in expanding training for prosecutors was the DOJ decision to identify one Assistant US Attorney in each office to act as liaison on national security and international matters. In September 1993, these Assistants began to receive extensive training in Washington and will serve as the resident specialists on CIPA and other Intelligence Community issues in their respective offices. Although the complete training agenda is not final, these AUSAs will be exposed to speakers from DOJ, the Intelligence Community, and the Departments of State and Defense. Training topics are expected to include such areas as how the Intelligence Community stores and retrieves its records and the use of specialized terminology.

In addition to the limited availability of training, there is a broad consensus within the Task Force that the quality of current training is deficient to the extent that it is based on outdated views of the needs of both communities and is too narrowly focused. The task of redefining training needs, therefore, will require answers to the following questions:

1. In those areas in which law enforcement and intelligence organizations share responsibilities or interact, what problems have been identified (or can be reasonably anticipated) that could be addressed by improved training?

2. Who should receive what types of training?

3. What types of training methods are best suited to the needs and circumstances of the target groups?

4. What type of mechanism (new committee and existing group) should have responsibility for assessing training needs, evaluating the various training options, and ensuring the adequate preparation and delivery of training?

5. What are the resource implications of specific training options?

C.(2) Training Issues and Alternatives

In addition to investigators and prosecutors, Task Force participants believe that judges, intelligence officers, defense attorneys, Congressional staffers, and possibly some of the media would also benefit from education programs. All training should be updated to include any new requirements or procedures developed as a result of approved Task Force recommendations. Given the diverse groups being considered for training, separate training

[21] *The United States Attorneys' Manual* (USAM) does offer some written guidance to prosecutors on certain required policies and procedures (USAM 9-90.000 et. seq). For example, the USAM specifies that the Internal Security Section of the Criminal Division should coordinate the implementation of CIPA (USAM 9-3, 400D).

packages should be developed. For members of the communities, there should be a Core Package for all recipients and Specialized Packages tailored to specific needs. The Core Package, for example, might include essential information on CIPA and basic requirements for handling classified information that would be helpful to all target groups.

Specialized training for members of both communities could include such topics as Federal rules and procedures regarding discovery; guidelines on the types of contact with the Intelligence Community that expose information to discovery; the law of evidence; the Constitutional requirement to provide the defendant with exculpatory evidence; how to focus an investigation to minimize the exposure of sources, methods, or national security information; and how to request help from the Intelligence Community in a way that is clear and not unduly burdensome. Intelligence officers specifically need some training in identifying situations in which intelligence collection opportunities should be referred to Law Enforcement agencies in order to protect the intelligence officer from becoming a necessary witness.

The Task Force participants identified education for judges as particularly important. A possible package for judges could include the creation of a videotape, perhaps in cooperation with the Federal Judicial Center, that would be tailored to their needs. Other options include providing training at various judicial conferences and requesting the help of former FISA judges to educate their colleagues. A videotape Core Package and a manual might also be developed for broad use among the other categories of recipients.

C. (3) Implementation Options

Given the consensus that training and cross training should be expanded in terms of both material covered and target audiences, one option is to create a standing Joint Law Enforcement/Intelligence Community Training Committee, consisting of both law enforcement and Intelligence Community members. This Joint Training Committee would assess training needs by group, evaluate the options for providing training, and ensure the adequate preparation and delivery of training. It would prepare specific training recommendations for review and approval by the Attorney General and DCI or their designees. A second option would be to identify and task an existing entity (such as DOJ's LEI) with some or all of these responsibilities. The second option may not be as practicable, primarily because of a lack of appropriate experience with these matters and a lack of intercommunity groups.

C. (4) Resource Implications

Some training expenses could be relatively high. For example, to host 93 AUSAs in Washington for three days will cost approximately $70,000. The Joint Training Committee or its equivalent should explore measures to minimize costs, such as manuals, other written materials, and videotapes. Written materials and manuals are the least expensive medium. A videotape may be produced inexpensively at the Office of Legal Education's Video facility or, more expensively, by an outside contractor. To the extent that conferences are planned, travel and related costs should be considered.

D. The Adequacy of Current Information Management Capabilities

Both communities need to make information resource management changes to improve IC agencies' abilities to respond to LE search requests and to ensure that LEA's can identify and properly route information received from IC agencies.

The Task Force believes that a committee inside the Law Enforcement community should be formed to examine the requirements associated with implementing an automated message handling system within Main Justice. The committee should include representatives of those components of the Departments of Justice and Treasury that regularly receive or transmit information critical to investigations and ongoing litigation handled by litigating Divisions of the Department of Justice or the US Attorneys. The Executive Office for United

States Attorneys and representatives of appropriate Department of Justice litigating divisions should be represented. Its members should be a mixture of management, legal, and technical personnel, and it should be chaired by the Assistant Attorney General for Administration.

The focus of the committee should include the following:

- A detailed analysis of the needs of the litigating components of the Department of Justice for cable traffic from the intelligence and law enforcement communities.
- The identification and evaluation of commercially available automated message handling systems, with an assessment of options.
- An estimate of costs to acquire, install and maintain an automated system.
- Proposals for funding.

Several alternative options should be developed. Each option should consider various factors, including: feasibility; costs and method of funding; the level of automation; compatibility with existing systems used by one or more of the Federal law enforcement components; security features; and the availability of contractual vehicles for implementation. On completion, the committee should submit a report to the Attorney General and the Secretary of the Treasury for final approval and implementation.

Appendix

The principal legal authorities relevant to an understanding of the relationship between the Intelligence Community and Law Enforcement are found in Executive Order (EO) 12333 (the charter for the Intelligence Community), the National Security Act of 1947, as amended (establishing the DCI and CIA), and, for Intelligence Community components within the Department of Defense, the Posse Comitatus Act, 18 USC § 1385 (limiting the use of the Army and Air Force to enforce civil laws), as well as Chapter 18 of Title 10, United States Code, 10 USC. § 371-380 ("Military Support for Civilian Law Enforcement Agencies" and 10 USC. § 124).

These authorities generally reflect the belief that national foreign intelligence and law enforcement functions should not be combined in a single entity. The modern origins of this view are found in the 1947 National Security Act. The National Security Act established CIA as a foreign intelligence agency with the kind of broad authority and great secrecy powers necessary to conduct foreign intelligence activities and protect US national security interests. Perhaps because of the appalling precedents provided by secret police agencies such as the Gestapo and NKVD, Congress provided that CIA would not function as a law enforcement entity. It specifically included a law enforcement "proviso" in the National Security Act, which provided "that the Agency shall have no police, subpoena, law enforcement powers, or internal security functions." 50 USCA. § 403-3(d)(1). This so-called law enforcement proviso has gained strength in the period intervening since passage of the National Security Act; it has also been applied to other national foreign intelligence agencies by a succession of Executive Orders.

EO 12333 provides the basic charter for the Intelligence Community and its various member agencies.[22] Specifically, it authorizes the Intelligence Community to "conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States"[23]; it does not authorize any of the Intelligence Community agencies to engage directly in law enforcement activities. Rather, the Order authorizes each agency to provide assistance to law enforcement and only in specifically defined circumstances and pursuant to explicit approval procedures.[24] Within this legal framework, each of the Intelligence Community agencies has its own specific regulations and limitations, summarized below.

The Central Intelligence Agency

For the CIA, the National Security Act serves as a basic organic charter and provides additional statutory authority. As noted above, the Act's law

[22] This Executive Order, issued in 1981 by President Ronald Reagan, is the third in a series of superseding executive orders that govern the Intelligence Community. These orders were issued as a result of the investigations into the activities of the Intelligence Community in the middle 1970s. In order in part to address Congressional and public criticism of unfettered Intelligence Community activities in support of domestic security and law enforcement activities in the 1970s, each Order has carefully spelled out the Intelligence Community's collection authority as well as its ability to support Law Enforcement.

[23] EO 12333 § 1.4. The Order specifically defines "international terrorist and international narcotics activities" as subjects appropriate for foreign intelligence collection. *Id.*, at § 1.4(c).

[24] Pursuant to Section 2.6 of E.O. 12333, each agency within the Intelligence Community may provide only the following types of assistance to law enforcement:

- Cooperate with appropriate law enforcement agencies for the purpose of protecting the employees, information, property and facilities of any agency within the Intelligence Community.
- Unless otherwise precluded by law or this Order, participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers, or international terrorist or narcotics activities.
- Provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any department or agency, or, when lives are endangered, to support local law enforcement agencies. Provision of assistance by expert personnel shall be approved in each case by the General Counsel of the providing agency.
- Render any other assistance and cooperation to law enforcement authorities not precluded by applicable law.

enforcement proviso restricts the CIA from exercising law enforcement powers or internal security functions.[25] This provision has been interpreted by the CIA Office of General Counsel, in consultation with the Department of Justice, to prohibit CIA personnel from participating directly in a US law enforcement operation, such as the arrest of an international terrorist or the interdiction of a narcotics shipment. If there is a legitimate foreign intelligence interest, however, CIA is authorized to provide a variety of assistance to Law Enforcement under certain circumstances pursuant to specific procedural direction.

CIA can and does disseminate to Law Enforcement agencies information incidentally collected during an authorized foreign intelligence or counterintelligence activity—if the information is relevant to matters within the investigative or prosecutive jurisdiction of those agencies.[26]

Thus, the application of the law enforcement prohibition to the collection of information relies upon a distinction between providing Law Enforcement with information incidentally obtained during the course of legitimate foreign intelligence collection activities as opposed to specifically collecting information of interest to Law Enforcement in the absence of a sufficient foreign intelligence interest. The prohibition precludes only the latter, not the former.[27]

[25] The prohibition is codified at 50 U.S.C. § 403-3(d)(1). Of particular note was the fact that the February 1993 report prepared by the staff of the SSCI on the Intelligence Community's involvement in the BNL affair disagrees that this statute bars CIA from engaging in law enforcement activities.

[26] Such collection and dissemination are conducted pursuant to Attorney General-approved procedures.

[27] The law enforcement prohibition does not preclude CIA from providing operational assistance to Law Enforcement agencies, but the assisting activity must support foreign intelligence or counterintelligence collection or in some other way be in support of the Agency's mission. If a Law Enforcement agency requests assistance that falls outside of CIA's authorities—and thus would be barred by the law enforcement prohibition—CIA may assist only by a formal detail of appropriate personnel to the requesting agency, or by a transfer of equipment under the Economy Act. Executive Order 12333, §2.6(c). Detailed employees act as officials of the Law Enforcement agency, not of CIA, and are permitted to provide assistance pursuant to the authorities of the requesting agency. Correspondingly, they are also subject to the limitations of the requesting agency.

Department of Defense Intelligence Agencies

In addition to the limits of EO 12333, those members of the Intelligence Community within the Department of Defense[28] must ensure their activities do not violate the Posse Comitatus Act.[29] That Act, coupled with 10 USC. § 375, prohibits the use of uniformed personnel of the Army, Navy, Air Force, and Marine Corps to participate directly in a search, seizure, arrest, or other similar law enforcement activity unless otherwise authorized by law. Therefore, intelligence agencies such as the National Security Agency and Defense Intelligence Agency must ensure that none of their uniformed personnel, including those detailed to a law enforcement agency, participate directly in such a law enforcement activity. In addition, these agencies may not provide support to law enforcement agencies if such support would adversely affect the military preparedness of the United States. So far as consistent with national security, these agencies are required to share intelligence information relevant to civilian law enforcement matters. They also may provide training and advice; as well as supply, maintain, and operate equipment.

The National Security Agency

Additional legal and policy constraints limit NSA's ability to collect information when not for the sole or primary purpose of foreign intelligence. NSA's intelligence gathering activities fall under the broad category of "electronic surveillance." When done for a law enforcement purpose, such activity constitutes a search for purposes of the Fourth

[28] These members are:
- Defense Intelligence Agency.
- National Security Agency.
- Offices for the collection of specialized intelligence through reconnaissance programs.
- The intelligence elements of the Army, Navy, Air Force, and Marine Corps.

Executive Order 12333, § 3.4(f).

[29] While the Posse Comitatus Act technically applies only to the Army and Air Force, the Department of Defense, as a matter of policy, applies its restrictions to the Navy and Marine Corps. However, the Department of Justice, Office of Legal Counsel, has opined that the Act does not apply outside of U.S. territory.

Amendment to the US Constitution. As such, these collection activities are strictly regulated by both the Constitution and statutes.[30] *In contrast, when such collection techniques are employed in support of foreign intelligence and are not directed at those whose constitutionally guaranteed rights might be affected, both the Courts and Congress have recognized that applying the requirements of individualized warrants and probable cause that arise in a criminal setting are unnecessary and unworkable. Indeed, if such requirements were employed to foreign intelligence collection activities, they would cripple national intelligence collection capabilities. As a result, both the Courts and Congress have devised a different approach to wiretaps and electronic surveillance when they are performed for a foreign intelligence purpose.*[31]

Foreign intelligence agencies actually benefit from the prohibition on law enforcement activities; they are not subject to the intense regulation of law enforcement designed to effect the Constitutional protections for criminal defendants and the subjects of criminal investigations. Over time these detailed authorities and the rationale for them was lost to many. Instead, two simple principles took their place for the day-to-day needs of intelligence officials: avoid collecting on law enforcement subjects or US persons absent a compelling foreign intelligence justification.[32] To understand why, we must consider how the purpose of foreign intelligence and law enforcement differ.Foreign intelligence collection is a strategic exercise which normally does not involve the individual rights and liberties of US citizens. Intelligence agencies identify trends, predict intentions, and assess policy level matters not related to specific cases or individual rights and liberties. The goal of foreign intelligence is to inform national policymakers about broad strategic issues of concern to the United States. With the exception of military intelligence, it is a long-term, continuing collection effort, not designed to end with the accomplishment of a specific overt act, such as an arrest or prosecution. In contrast, the legal restrictions imposed on Law Enforcement agencies as they collect information are due largely to the fact that this collection is tactical in nature: it is directed at specific cases and specific individuals. Its goal is the arrest, prosecution, conviction, and punishment of those suspected of committing criminal offenses.

As a practical matter, intelligence agencies also engage in tactical intelligence collection. They may, for example, attempt to identify the perpetrators of an international terrorist event or provide information on military targets during hostilities. Such information can be extremely valuable to law enforcement when it involves actual or potential violations of Federal criminal law.

These contrasting purposes permit slightly different standards under the unreasonable search and seizure test of the Fourth Amendment to the US Constitution. The collection technique used may be the same, but the "reasonableness" standard under the Fourth Amendment has been interpreted more broadly where collection focuses on a foreign policy issue not the constitutional protections of a US citizen. Fewer procedural hurdles have been required of intelligence agencies, even when the technique employed would be aggressively regulated when used by a Law Enforcement agency. This greater operational freedom enjoyed by the Intelligence Community creates an undeniable, if superficial, appeal to the idea of making the resources of the Intelligence Community available for direct tasking by Law Enforcement agencies. It is argued that the broad and flexible capabilities of the intelligence agencies, if used for Law Enforcement, would boost Law Enforcement

[30] Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, 18 U.S.C. § 2510 *et seq*.

[31] See, for example, 18 U.S.C. § 2511(f) (recognizing a foreign intelligence exception to the warrant requirements of Title III of the Omnibus Crime Control and Safe Streets Act of 1968); and *United States v. Truong*, 629 F.2d 908 (4th Cir. 1980) (Government may be excused from warrant requirement in conducting electronic surveillance only where surveillance is conducted primarily for foreign intelligence purpose).

[32] An intelligence interest, in itself, is not a sufficient basis for NSA to collect intelligence on a U.S. citizen. The use of electronic surveillance to collect information on U.S. persons is regulated by the Foreign Intelligence Surveillance Act, 50 U.S.C. 1801-1811, and Executive Order 12333.

agencies struggling in foreign realms. Yet to do so would bring many valuable intelligence collection methods under the severe constitutional and statutory restraints that already apply to law enforcement. Here the classic example is wiretaps. They are governed under two statutory regimes (Title III and FISA), depending on the specific circumstances.

For example, directing NSA to conduct electronic surveillance for the sole or primary purpose of law enforcement missions abroad would quickly bring the agency's operations under the strict limits of Title III. Upon subsequent court review, such a loss of flexibility would greatly reduce NSA's usefulness in assisting law enforcement agencies; it could also seriously jeopardize the Government's ability to utilize NSA for its intended foreign intelligence purpose. Generally speaking, NSA collects intelligence not by targeting a particular individual but by conducting electronic surveillance on a particular topic or particular part of the world. Although NSA is capable of ensuring that the privacy rights of US citizens are not violated as a result of NSA's collection activities (for example, by assuring that any incidentally acquired names of US persons are not included in NSA product reports), requiring NSA to determine in advance whose communications it is intercepting would impose a crippling burden on the agency.