LAW ENFORCEMENT INFRASTRUCTURE CHALLENGES

Report to the
President's Commission
on Critical Infrastructure Protection

1997

This report was prepared for the President's Commission on Critical Infrastructure Protection, and informed its deliberations and recommendations. The report represents the opinions and conclusions solely of its contributors.

Page

Acknowledgments

The assistance of the following in preparation of this paper is gratefully acknowledged:

Mr. David V. Keyes, Commissioner, President's Commission on Critical Infrastructure Protection;

Ms. Ann Beauchesne, National Governors' Association;

Mr. Joseph P. Bonino, Commanding Officer, Records and Identification Division, Los Angeles Police Department;

Ms. Laura Carter, National Law Enforcement Telecommunications Systems, Inc.;

Mr. William M. Casey, Commander, Information Technologies Division, Boston Police Department;

Major Jim Martin, South Carolina, State Law Enforcement Division;

Mr. Harlin R. McEwen, Deputy Assistant Director, Criminal Justice Information Services Division, Federal Bureau of Investigation;

Mr. Brian A. Reaves, United States Department of Justice, Bureau of Justice Statistics; and

Ms. Patricia Burt and Ms. Julie Consilvio of the PCCIP for their editing support.

Note: For purposes of this paper, law enforcement responsibilities pertaining to special jurisdictions, such as Military Police, law enforcement officers of the Bureau of Indian Affairs, Transit or Port Police, or other similar special cases have not been included.

Executive Summary

Law enforcement in the United States is neither centrally directed nor homogenous. As such, it does not readily fit the definition of infrastructure set out in the report of the Critical Infrastructure Working Group. Local, State and Federal law enforcement agencies have their own (and sometimes unique) geographic and statutory jurisdictions, as well as operating procedures that may or may not overlap or coincide. The Attorney General is the chief Federal law enforcement officer and has authority to oversee the activities of Federal law enforcement agencies and Federal efforts to provide assistance to local law enforcement authorities. However, no Federal authority exists to oversee the activities of non-Federal law enforcement agencies. Because of the diversity and redundancy of the U.S. law enforcement structure, there appears to be almost no realistic vulnerability or group of vulnerabilities that could debilitate the entire law enforcement system through physical attack. This said, there are four areas examined in this paper which may prove to be information, electronic and/or cyber issues for the Commission to highlight. These are:

1. Radio frequency allocation by the Federal government, which has sold or is selling to the private sector certain radio frequencies traditionally used by law enforcement and other emergency services;

2. Training for local officials in terrorism matters, including sharing of threat and vulnerability information;

3. The need for local law enforcement officials to share information concerning cyber attacks and intrusions with the Federal government; and,

4. The security and assurance of common criminal justice information support systems presently in existence or in an advanced stage of development. Representative examples include the National Crime Information Center computer system, the National Law Enforcement Telecommunications Systems and the Integrated Automated Fingerprint Identification System.

Law Enforcement

In a December 1995, response to a Presidential Decision Directive regarding terrorist threats to the United States, the Attorney General and Deputy Attorney General convened a small group of knowledgeable senior government managers as a Critical Infrastructure Working Group (CIWG). Under the personal direction of the Deputy Attorney General, the group was charged with examining two categories of threats to, and vulnerabilities of, critical national infrastructures. The categories of threats include physical threats to tangible property (physical threats), and threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures (cyber threats). This paper uses the definition of infrastructure established by the CIWG:

> "Infrastructure is the framework of interdependent networks and systems comprising identifiable industries, institutions, and distribution capabilities that provide a continual flow of goods and services essential to the defense and economic security of the United States, the smooth functioning of governments at all levels, and society as a whole.[1]"

Executive Order 13010 charges the Presidential Commission on Critical Infrastructure Protection (PCCIP) with examining, among others, the "infrastructure" of Emergency Services, which includes police, fire, rescue and emergency medical services. Law enforcement does not readily meet the criteria established by the above definition. Unlike some European countries that have either a national police or an Interior Ministry with policy oversight of a country's many police agencies, there is no centralized policy oversight or command and control over the nation's law enforcement agencies. As a result, the characterization of the law enforcement infrastructure in the United States can be done only in general terms. While this characterization is admittedly limited, it represents a starting point for further examination.

How Big is the Law Enforcement Community?

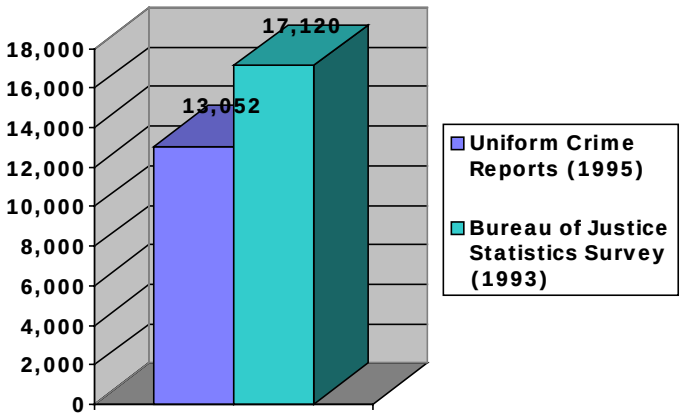
So decentralized are the nation's law enforcement agencies, that it is not entirely clear exactly how many exist. Section VI of the publication Crime in the United States 1995 Uniform Crime Reports, states that, for the 1995 report, the FBI received crime statistics from 13,052 city, county

[1] Undated report of the Critical Infrastructure Working Group (CIWG) circulated to various Cabinet Secretaries in March, 1996.

and State police agencies.[2] However, because the crime reporting process is voluntary, the number of Uniform Crime Report (UCR) participants is thought to be lower than the actual number of law enforcement agencies. The 13,052 agencies that did participate in the 1995 UCR reported that they employ 586,756 sworn officers and 226,780 civilians.

A more accurate law enforcement census may be found in a 1993 Department of Justice, Bureau of Justice Statistics (BJS) survey.[3] It states that during 1993, there were an "estimated" 17,120 publicly-funded State and local law enforcement agencies. The survey included sheriffs' departments, State police and special police agencies with limited jurisdiction (such as park, transit system, airport or school police). The results of the 1993 survey revealed 622,913 full-time sworn officers and 42,890 part-time sworn officers, with 206,522 full-time civilians and 44,986 part-time civilians. Although conducted two years before the 1995 UCR, the number of law enforcement agencies, sworn officers and civilian employees is greater in the 1993 survey. And since 1993, the Federal government has sought to fund an additional 100,000 law enforcement officers at the local level.

Number of City, County and State Police Agencies



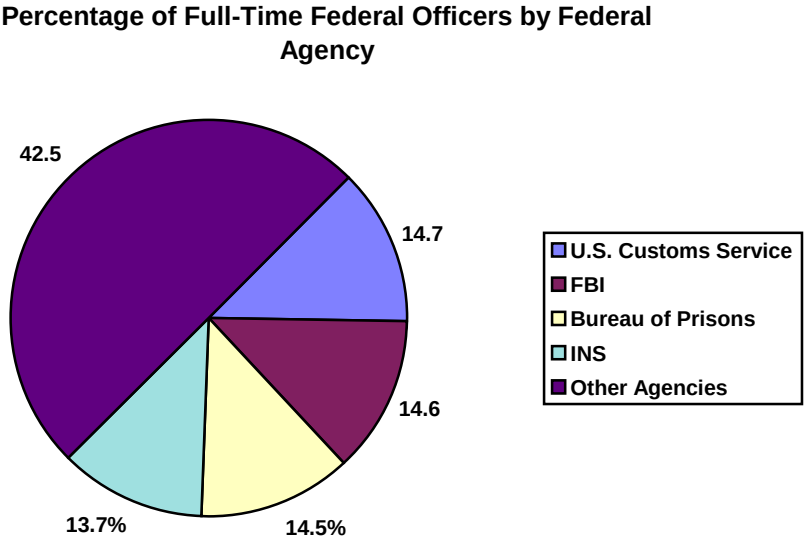
In December 1994, the Department of Justice reported results of the 1993 survey as pertains to Federal law enforcement officers in 17 Federal agencies having 500 or more sworn officers.[4] It identified "about 69,000" full-time Federal officers authorized to make arrests and carry firearms. The U.S. Customs Service had the greatest number (10,120), followed by the FBI

[2] Crime in the United States 1995 Uniform Crime Reports, Louis J. Freeh, Director, FBI October 13, 1996, p. 278.

[3] U.S. Department of Justice, Bureau of Justice Statistics, "Local Police Departments," Bulletin NCJ-148822, April 1996.

[4] U.S. Department of Justice, Bureau of Justice Statistics, Bulletin NCJ-151116, December 1994.

(10,075), the Bureau of Prisons (9,984) and the Immigration and Naturalization Service (9,466), to list the four largest. Of the approximately 69,000 Federal law enforcement officers, about half were assigned in five locations: California, Texas, New York, Washington D.C. and Florida.



A firm number by which to measure one facet of the broader criminal justice system involves the National Crime Information Computer (NCIC). The Federal Bureau of Investigation (FBI), which is the manager of the NCIC system, advises there are a total of 81,629 agency identifiers assigned to NCIC users.[5] Each of these agencies may have multiple terminals, but those terminals are clearly identified as belonging to one of the 81,629 user agencies. Of the 81,629 user agencies, some are law enforcement agencies; others are prosecutors' offices; and still others are assigned to prison systems, parole or probation offices, local, State and Federal courts, and the like.

How are Law Enforcement Agencies Organized, and How Do They Interact with Each Other?

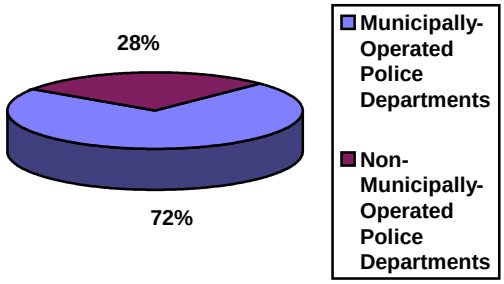
Given the broad diversity of law enforcement agencies at the Federal, State and local levels, there is no universal model for how law enforcement agencies are organized, what their jurisdictions are, how or if they collaborate, what mutual aid agreements might be in place (if any), or how they otherwise interact. Nevertheless, some generalities about authorities and interaction apply

[5] Mr. Demry Bishop, Section Chief, Criminal Justice Information Systems, FBI, conversation November 8, 1996.

in many circumstances. What follows is a somewhat representative model, but does not have universal application.

The responsibility for law enforcement in the United States begins at the lowest political level. Within the boundaries of the Constitution, and limits set by State legislatures, each village, town or city has the authority to establish its own criminal code and provide a criminal justice structure to enforce it. Each law enforcement agency so created is, in the first instance, responsible to the community which granted it jurisdiction. Of the estimated 17,120 publicly-funded law enforcement agencies identified in the 1993 BJS study, 72 percent (12,361) were estimated to be general purpose local police departments.[6] Some 99 percent of these were estimated to be operated by the municipal governments.

Publicly-Funded Law Enforcement Agencies



At the next level of government, usually the county or its equivalent, there is a sheriff or similar official whose law enforcement powers usually extend throughout the entire county. Sheriffs are usually elected officials, are generally somewhat autonomous, and often appoint their deputies. Only 1 percent of the estimated agencies surveyed by BJS in 1993 were county police agencies such as the sheriff.[7] As a practical matter, sheriffs' deputies often cover only the unincorporated areas of the county not covered by other law enforcement agencies. The sheriff generally operates the county jail and may be involved in other duties, such as providing deputies for security in courts, serving warrants and court documents, or transporting prisoners.

At the next higher level of government, the State, there may be a State bureau of investigation, State police, highway patrol, agricultural authorities, park police or fish and wildlife officers, or any combination thereof. Generally speaking, these State law enforcement officers can exercise their authority anywhere in the State, but, depending on their charter, generally confine themselves to matters on State lands, State highways or incidents in which the State is the victim. State law enforcement and/or correctional officers generally operate the State prison system and provide security in State courts, or conduct other State-related criminal justice activities similar to those of the sheriff at the county level.

---

[6] Bulletin NCJ-148822, April 1996.

[7] Ibid., p. 1.

At the village, town or city level, the powers of the law enforcement officer may extend only to the end of the political boundary of the village, town or city. This is almost always the case as pertains to misdemeanors or other minor crimes, including violations of local ordinances. This geographic limitation sometimes also applies to the authority to investigate felonies and other major crimes. In some States however, law enforcement officers who meet certain training standards may be granted authority by the State to exercise police powers for felonies committed in their presence anywhere in the State.

In most police jurisdictions, there are mutual assistance agreements between law enforcement agencies. Typically, such agreements provide for mutual assistance in the event of major disturbances or other events specified in the agreement. For example, a village, town or city police jurisdiction may receive assistance from the county sheriff or State police. Adjoining counties may have mutual assistance agreements. A governor can authorize State law enforcement officers to assist or even supplant local jurisdictions when appropriate conditions are met. In a worst-case scenario, such as a major riot, or take-over of a State prison, a governor can mobilize the State national guard in its non-Federal capacity as a State militia to enforce the laws of the State. The Federal Posse Comitatus statute limiting the use of Federal military forces for law enforcement purposes does not apply if the national guard has not been federalized.

Where communities flow together in a more-or-less seamless fashion, there may be agreements regarding hot pursuit of felons across jurisdictional boundaries, or other matters of mutual interest. Where there are adjoining cities on opposite sides of State borders, or along the borders with Mexico and Canada, police may have a mutual assistance task force to deal with cross-border crimes. These typically address such things as stolen cars and other property, smuggling and/or violations involving tax avoidance on commodities.

Federal Law Enforcement Organization and Interaction with State and Local Law Enforcement Agencies

At the Federal level, there is a similar jurisdictional patchwork. Federal law enforcement jurisdiction is based on statutory jurisdiction assigned either by Congress at the time it enacts criminal statutes, or by the Attorney General. In many instances, there are shared or overlapping jurisdictions among Federal agencies. Sometimes part of one criminal statute will be assigned to one agency and another part of the same statute is assigned to another agency. As a generalization, Federal criminal jurisdiction is based on the power of the Federal government to regulate interstate and foreign commerce, such as:crossing a State or international border; involving a means of interstate or foreign commerce, such as the telephone; involving a Federal

interest, such as robbery of a Federally insured bank; or relating to defrauding the government. With the exception of the latter, such crimes are often also violations of State or local laws.

The fact that there is often overlapping jurisdiction between local and Federal law enforcement agencies sometimes results in agreements between State and Federal prosecutors about which crimes will be handled by Federal and which by State or local officers. Such decisions are sometimes made on the basis of the level of financial loss, the need to conduct out-of-state or foreign leads, or the nature of investigative techniques to be used. In the latter category, for example, in some States, wiretaps are not a lawful investigative technique for State authorities, but may be used by Federal authorities operating pursuant to Federal law.

There is generally no requirement for local or State officials to coordinate their activities with Federal law enforcement agencies, nor the latter with the former. However, because of overlapping jurisdictions between State and Federal officials, the Federal government will sometimes fund joint task forces made up of Federal, State and local officials, often from multiple local jurisdictions. Where metropolitan areas flow across State borders, a task force could include local officers from both sides of the border. A Federal task force is intended to bring a coordinated focus to a problem such as drug trafficking, which can at the same time be a violation of Federal, State or local laws. In some areas, the FBI has created joint terrorism task forces. A Federal task force is funded, and thus controlled, by the Federal agency that creates it. The local officers who participate in such a task force are typically given some sort of limited Federal criminal investigative authority, such as that of a Special Deputy United States Marshal.

At the Federal level, there are any number of requirements for Federal law enforcement agencies to coordinate their investigative activities. The extent to which such coordination takes place is not possible to measure. However, Executive Order 12656 of November 18, 1988, entitled, "Assignment of Emergency Preparedness Responsibilities" vests certain authorities in the Attorney General to:

1. Coordinate the development of procedures by which military assistance to civilian law enforcement authorities may be requested, considered and provided;[8]

2. Coordinate Federal domestic law enforcement activities related to national security emergency preparedness, including Federal law enforcement liaison with, and assistance to, State and local governments;

3. Coordinate contingency planning for national security emergency law enforcement activities that are beyond the capabilities of State and local agencies;

4. Develop intergovernmental and interagency law enforcement plans and counterterrorism programs to interdict and respond to terrorism incidents in the

[8] U.S., President, Executive Order (EO) 12656, "Assignment of Emergency Preparedness Responsibilities" Part 5, ¶ 12, November 18, 1988.

United States that may result in a national security emergency, or that occur during such an emergency; and

5. Develop intergovernmental and interagency plans to respond to civil disturbances that may result in a national security emergency, or that occur during such an emergency.[9]

Executive Order 11396 of February 7, 1968, entitled "Coordination By Attorney General of Federal Law Enforcement and Crime Prevention Programs" designates the Attorney General as the "chief law officer" of the Federal government.[10] As such, the Attorney General facilitates and coordinates:

1. The criminal law enforcement activities and crime prevention programs of all Federal departments and agencies; and

2. The activities of such departments and agencies relating to the development and implementation of Federal programs that are designed in whole or in substantial part to assist State and local law enforcement agencies and crime prevention activities.

Regardless of any authority the Attorney General may have over Federal law enforcement officers, both within and outside the Department of Justice, the Attorney General has no authority to direct or control the activities of State and local law enforcement authorities.

Just as a State governor can use the national guard of that State to enforce the law in emergency situations, so too can the President of the United States take action to place Federal military personnel in roles providing direct support to law enforcement. In November 1987, President Reagan did just that after Cuban prisoners seized control of the Federal Penitentiary in Atlanta, Georgia.

By means of a Presidential Proclamation[11] and an Executive Order[12], the President placed Federal troops at the disposal of the Attorney General to restore law and order in the Federal Prison. Military logistics, medical, and operational forces were deployed at the prison under military command. They were assigned assorted missions and asked to plan how such missions would be conducted under their command structure if authorized by the civilian authorities in charge.

The plans were reviewed by FBI and Bureau of Prisons officials at the scene, and by senior officials of the FBI and the Department of Justice (including the Director of the FBI and the

---

[9] Ibid., Part 11, ¶ 2, 3, 7, 8.

[10] U.S., President, Executive Order 11396, "Coordination By Attorney General of Federal Law Enforcement and Crime Prevention Programs," February 7, 1968.

[11] U.S., President, Proclamation 5748, "Law and Order in the State of Georgia," November 24, 1987.

[12] U.S., President, Executive Order 12616, "Providing for the Restoration of Law and Order in the State of Georgia," November 24, 1987.

Attorney General of the United States). Once the plans were approved, had the need arisen to implement them, the military forces would have executed their plans as ordered by civilian authority.

Possible Issues for Further Commission Review

Because law enforcement in the United States is not homogenous and lacks central policy control or direction, it is impossible to make any but the most general comments about its collective needs as they relate to the mission of this Commission. There are four areas, however, which may prove to be relevant. These are:

1. Radio frequency allocation by the Federal government, which has sold or is selling to the private sector, certain radio frequencies traditionally used by law enforcement and other emergency services;

2. Training for local officials in terrorism matters, including sharing of threat and vulnerability information;

3. The need for local law enforcement officials to share information concerning cyber attacks and intrusions with the Federal government; and,

4. The security and assurance of common criminal justice information support systems presently in existence or in an advanced stage of development. Representative examples include the National Crime Information Center (NCIC) computer system, the National Law Enforcement Telecommunications Systems (NLETS) and the Integrated Automated Fingerprint Identification System (IAFIS).

Issue 1: Radio Frequency Allocation

The issue of radio frequency allocation was addressed in a recent report of the Public Safety Wireless Advisory Committee (PSWAC).[13] According to that report, in 1993, as part of the legislation authorizing the use of spectrum auctions, Congress required the Federal

[13] "Final Report of the Public Safety Wireless Advisory Committee to the Federal Communications Commission and the National Telecommunications and Information Administration," September 11, 1996.

Communications Commission (FCC) to conduct a study of the current and future spectrum needs of State and local government public safety agencies through the year 2010.

PSWAC was chartered as a Federal Advisory Committee to advise the Chairman of the FCC and the Assistant Secretary of Commerce supervising the National Telecommunications and Information Administration (NTIA). The report identifies the following four unique radio frequency operational requirements of public safety users;[14]

1. Dedicated capacity and/or priority access available at all times (and in sufficient amounts) to handle unexpected emergencies;

2. Highly reliable (redundant) networks that are engineered and maintained to withstand natural disasters and other emergencies;

3. Ubiquitous coverage within a given geographic area; and

4. Unique terminal equipment (mobile or portable units) designed for quick response in emergency situations.

PSWAC notes that police and other public safety agencies have operational requirements that necessitate different radio spectrum solutions. For example, correctional facilities with their concrete and steel structures pose one type of communications challenge. Others need to communicate over long distances, perhaps over hundreds of miles or where foliage may be a problem for higher frequencies. Communications between air and ground units can be an issue. Still other agencies need reliable coverage inside buildings in urban areas. The system propagation characteristics for these operational requirements may well be contradictory.

Reallocating all public safety users to a single new band is not feasible due to the need to maintain different propagation characteristics for different public safety missions, the cost of replacing the installed base of current equipment, and the lack of any single spectrum block of sufficient size to accommodate all public safety users.[15] At least part of the installed base, covering the lowest microwave frequencies in the 2 GHz band, was apparently used to carry signals from base stations to control sites that, if we understand correctly, then propagated them further. That spectrum has now been reallocated for commercial use for personal communications systems[16].

The sale of the radio frequency spectrum by the Federal government may create huge costs and technical problems for law enforcement and other emergency service providers. To address these problems, PSWAC proposed several options. One of these is that money should be set aside from the revenue generated by the sale of the radio spectrum, and that those funds should be

[14] Ibid., p. 14, ¶ 1.23.

[15] Ibid., p. 20, ¶ 2.1.11.

[16] Ibid., p. 40, ¶ 4.4.49; p. 42, ¶ 4.2.35; p. 57, ¶ 4.4.11.

available to pay the costs of swapping out installed equipment necessitated by the sale of previously-used, or adding new, radio spectrum. Other proposals include user fees for non-public safety users, amendments to the Federal asset forfeiture laws, matching funds, or block grants.[17]

The issue of radio frequency allocation for law enforcement purposes, and for all public safety services, is a complex one, worthy of further review and analysis by the Commission. It should be explored through interaction with at least the Association of Public-Safety Communications Officials, the International Association of Chiefs of Police, the National Sheriffs' Association, the National Governors' Association, the National League of Cities, the Advisory Policy Board to the FBI's Criminal Justice Information Services (CJIS) Division, and the International Association of Fire Chiefs. Other logical groups may be identified through contact with these groups. The Federal perspective should be obtainable through the Department of Commerce and the FCC.

Issue 2: Training for Local Officials in Terrorism Matters Including Sharing of Threat and Vulnerability Information

In July, 1994, the Criminal Justice Research Program of RAND published the results of its two-year study of State and local law enforcement preparedness to deal with terrorism.[18] The report was completed under contract to the National Institute of Justice (NIJ) of the U.S. Department of Justice. To ensure it was of appropriate scope and depth, the survey upon which the research was based was reviewed on multiple occasions by the FBI and NIJ, as well as by an advisory panel of experts in the fields of terrorism and law enforcement.[19] The survey included 52 State law enforcement and 52 State emergency management offices of the 50 States, the District of Columbia and Puerto Rico. Local law enforcement agencies that participated in the survey were carefully selected from all regions of the country, and incorporated agencies from representative population sizes, counties and municipalities.[20]

The research was completed in January 1993, one month before the bombing of the World Trade Center in New York, and over two years before the bombing of the Alfred P. Murrah Federal Building in Oklahoma City on April 19, 1995. It nonetheless represents the only comprehensive research on this topic of which we are aware and is of such breadth, depth and scope that it would be impossible to update its findings within the lifetime of this Commission.

Not surprisingly, the RAND researchers encountered a broad array of definitions of what constitutes terrorism, and in the end relied upon the FBI definition:

---

[17] Ibid., p. 24, ¶ 2.2.12

[18] K. J. Riley & B. Hoffman, "Domestic Terrorism: A National Assessment of State and Local Law Enforcement Preparedness," RAND, July 1994.

[19] Ibid., p. 3.

[20] Ibid., pp. 7-11.

> "Terrorism is the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof in furtherance of political or social objectives.[21]"

The researchers noted that poor communication between Federal, State and local law enforcement may have accounted for lack of uniformity in defining terrorism and what constitutes a terrorist act.[22] They also concluded that, despite near universal acknowledgment of the potential for terrorism, there was no agreement on what to do about it. Training, communications, coordination, and procedures were found to vary between cities and even between law enforcement agencies within a city.[23]

The researchers also noted that the FBI is the lead Federal agency for countering terrorism in the United States. As of then (1993), the FBI has established joint terrorism task forces with State and local law enforcement agencies in Boston, Chicago, Denver, Houston, Los Angeles, Miami, Newark, New York, Philadelphia and San Diego. The report noted the extremely high cost of these task forces, in that the FBI pays overtime to the participating local law enforcement officers, provides vehicles, office space, specialized equipment and other general services support. However, the result has been extremely close relations and coordination between the FBI and their law enforcement partners.[24]

In contrast to the terrorism task forces, however, the research determined that only 25 percent of the survey respondents had received FBI assistance in review of terrorism contingency plans.[25] Some 41 percent of the reporting municipalities advised they had never had contact with Federal agencies concerning terrorism issues. In localities with less than 100 officers, 53 percent reported never having met with Federal authorities of any kind.[26] These percentages are surprisingly high, if only because the researchers determined that counter and anti-terrorism training was being provided to localities by the FBI; the Bureau of Alcohol, Tobacco and Firearms (BATF); the Department of Energy; the U.S. Army; the Secret Service; and the Department of State Bureau of Diplomatic Security.[27] Some believe that such training programs have not been coordinated at the Federal level and are sometimes competitive and/or contradictory.

---

[21] Ibid., p. 4.

[22] Ibid., p.6 (including footnote 3).

[23] Ibid., p. 28.

[24] Ibid., p. 37 (including footnote 13).

[25] Ibid., p.33.

[26] Ibid., p. 35.

[27] Ibid., p. 46.

The issue is perhaps crystallized for this Commission in the following summary from the RAND study:

> "The FBI and many large police departments, through joint terrorism task forces, have taken significant steps to develop plans and countermeasures to protect the most vulnerable or likely terrorist targets. However, equally attractive and lucrative targets--such as military installations, fuel supplies, telecommunications nodes, power plants, and other vital infrastructure--potentially exist in smaller, less-populated jurisdictions.[28]"

A more up-to-date, but perhaps less scientific, sampling of opinions came at the National Governors' Association (NGA)Workshop in Rancho Mirage, California, September 18-19, 1996. This workshop was held to identify the nature, impact, and response issues associated with a nuclear, biological, or chemical (NBC) terrorist incident; to discuss the adequacy of both Federal and State plans and response capabilities to an incident involving mass casualties; and to begin formulating next steps for developing a coordinated Federal, State and local response framework.[29]

Prior to the workshop, the NGA conducted a survey of 26 States, 22 of which responded. The 26 were chosen because of "their large urban areas and other factors which could potentially make them targets for a terrorist incident."[30] What these factors were, and whether they encompassed the infrastructure contexts being examined by this Commission, is not yet known.

At the workshop, in what are apparently representative comments, panelists dealing with law enforcement issues (from California, Illinois, New York State and Utah) all noted in some fashion the role of intelligence and the need for close Federal/State law enforcement and emergency management interaction and information exchange concerning terrorism in general and NBC threats in particular.[31] In a related comment, the NGA survey determined that most States receive satisfactory intelligence information about potential terrorist groups operating in their States and that their State police departments generally have a good relationship with the FBI.[32] This notwithstanding, to assist their planning, the attending States expressed the desire to receive periodic assessments of risks and trends in terrorism affecting their region.

In addition, the States expressed a desire to see improved coordination at the Federal level to avoid duplication of effort at both the State and Federal level, and to make it easier to access Federal resources. Toward that end, some States suggested that the Federal Emergency

---

[28] Ibid., p. xi.

[29] Ann Beauchesne, National Governors' Association. Summary of the National Governors' Association Workshop Preparing for and Managing the Consequences of Terrorism, October 24, 1996.

[30] Ibid., p. 3.

[31] Ibid., pp. 8-10.

[32] Ibid., p. 3.

Management Agency (FEMA) be the key coordinating agency for information from, and access to, other Federal agencies.[33] Although the suggestion that FEMA be the coordinator of information flow and access to other Federal agencies may, on its face, sound appropriate, the reality is that the primary flow of terrorism-related information domestically is, and will likely remain, within the Department of Justice and the FBI.

However, recognizing from the RAND study that a problem exists in the area of terrorism information exchange, the Department of Justice, Bureau of Justice Assistance (BJA), has funded a grant to address this information and training shortfall. It created a program through which State and local law enforcement officials will be given training in terrorism matters, including potential threats from international and domestic groups. The FBI provided instructors for at least one pilot effort held in Utah in May, 1996. The goal of the program, is to provide a forum for Federal, State and local law enforcement interaction and information exchange in those areas of the country where no joint terrorism task forces exist. Following the initial training, enhanced liaison with local FBI offices will supposedly follow. If successful, this program could go a long way toward addressing some of the problem areas identified in the RAND report, as well as the concerns articulated at the NGA conference.

Another Federal effort to enhance emergency preparedness is the authorization of $36 million by the Department of Defense to, among other things, improve Federal, State, and local response capability.[34] One mechanism for improving response capability is training for local officials in terrorism matters. Such training began in May, 1997, when emergency responders in twenty-six cities received Federal training and funds to enable them to better recognize and respond to NBC terrorist attacks.

The issue of information sharing and training among Federal, State and local law enforcement agencies is a simple one on its face, but complex in its implementation. It seemingly warrants further review and analysis by the Vital Human Services Sector of the PCCIP. The issue can be further explored through interaction with the International Association of Chiefs of Police, the National Sheriffs' Association, the NGA and the Advisory Policy Board to the FBI's Criminal Justice Information Services (CJIS) Division. Privacy advocates and civil libertarians have expressed great concern about the expansion of Federal law enforcement efforts in this arena.

[33] Ibid., p. 2.

[34] Ann Beauchesne, National Governors' Association. National Governors' Association Issue Brief: Terrorism - Is America Prepared? February 2, 1997.

Issue 3: The Need for Local Law Enforcement Officials to Share Information Concerning Cyber Attacks and Intrusions with the Federal Government

This issue is clear-cut and straight-forward. Information sharing within the law enforcement community concerning cyber attacks is a substantial and missing piece in any attempt to achieve a comprehensive understanding of cyber threats and vulnerabilities. Such information is not presently being collected. On December 12, 1996, we spoke to the senior personnel of the CJIS Advisory Policy Board. This Board represents the 83,000-plus users of the NCIC system. They also influence the manner in which criminal justice statistics are reported. They are very amenable to future dialogue regarding specialized reporting of computer intrusions, and welcome further contact regarding this issue.

Issue 4: The Security and Assurance of Criminal Justice Automated Information Systems

As noted above, law enforcement in the United States is neither centrally-directed, nor homogeneous. As such, the patchwork of law enforcement and criminal justice jurisdictions in the United States do not readily fit the definition of infrastructure. However, there are automated criminal justice information systems that do meet that definition. They are as structurally diverse as the patchwork of agencies and jurisdictions they serve. However, these information systems are increasingly interconnected electronically, and as such, may collectively represent the most cohesive common ground of an otherwise eclectic community.

As interconnectivity increases, the collective security of all the systems are dependent on the individual security of each of the connected parts. A compromise of one could lead to a compromise of all. With this in mind, the following three examples of automated information systems are intended to be a representative sampling of a rich and diverse set of automated law enforcement information systems.

4.a. National Crime Information Center

The NCIC computer system is conceivably an example of a single point of failure. Recently-obtained information demonstrates that security procedures of the NCIC system could be improved, thereby lessening the risk of cyber attack and intrusion. In addition, because there is no mirror or “hot backup” for NCIC, system outages have nationwide consequences.

The NCIC system is operated by the FBI for all participating U.S. law enforcement and other criminal justice agencies, such as prisons, parole agencies, courts, and prosecutors' offices. As previously noted, there are a total of 81,629 user agencies, each of which might have multiple terminals. Among other things, the NCIC computers maintain records of certain types of arrest warrants, information about wanted persons, information about stolen property of various types, and certain kinds of criminal history information.

The NCIC system was designed to enable a law enforcement officer in one part of the country to quickly and easily establish whether a person is a fugitive from another jurisdiction or whether property has been reported stolen, and identify members of violent gangs or terrorist organizations, deported felons, etc. The system can also protect a police officer by alerting him or her that the fugitive might be armed and dangerous, or that a suspect has a prior criminal history.

Historically, the threat to the integrity of NCIC information has come from insiders, such as corrupt criminal justice system employees illegally using and accessing information in the NCIC system. However, there are no known instances of the NCIC system being placed at risk through such unauthorized activity.

Today, there is a less obvious threat to the integrity of the NCIC system. Without the knowledge or permission of the FBI, NCIC system access in some agencies has been commingled on terminals used for Internet and/or Intranet communications, without any firewalls or other safeguards being used. Upon learning of the unprotected commingling of systems, it was immediately recognized that, because of the inherent vulnerabilities of distributed systems, particularly Internet-connected systems, the integrity of the data in the NCIC system was at risk. Should common Internet penetration techniques be targeted against terminals that have commingled unprotected NCIC and Internet functionality, it is conceivable that false information could be entered into the NCIC system, that its records could be altered or removed, and that the privacy and integrity of criminal justice records could be violated. An NCIC Security Committee of the CJIS Advisory Policy Board has been formed, and a firm instruction sent to all NCIC users to take remedial action.

There is no indication that any compromise of the NCIC system has been attempted using the Internet. Had this potential security compromise not been recognized, it is instructive to understand what the impact could have been. The potential compromise of the integrity of NCIC records could represent a threat to the operation of the NCIC system itself. Introduction of malicious code into the system could cause havoc and confusion that might not be sorted out for an extended period. To have to simultaneously reload operating software for over 80,000 computers and thereafter reboot and reconfigure the entire system would be a daunting task. The cost and time necessary to conduct an audit of the entered records to be sure of their integrity following a clandestine intrusion would be, perhaps, more daunting. If State criminal records systems were also corrupted through their connectivity with NCIC, the consequences would be even more calamitous.

An additional worry expressed by diverse members of the criminal justice community is that NCIC has no backup or mirror site. Historically, NCIC has been remarkably resilient, with unscheduled service breaks being both unusual and of short duration. In early 1997, in an exception to the rule, a breakdown in the information pathway at FBI Headquarters caused a system outage of some 10-hours duration. Absent a backup system, during that entire time, no police officer anywhere in the United States had direct access to NCIC system information. Because NCIC is so crucial to the safe and efficient operation of many important parts of the criminal justice network, the FBI is in the final stages of a plan to protect the system from such an outage in the future. A redundant pathway and other work-arounds are in progress.

4.b. National Law Enforcement Telecommunications Systems (NLETS)

Following a series of meetings among the States seeking to facilitate the exchange of law enforcement information among agencies of the criminal justice system, the Arizona Highway Patrol volunteered in 1966 to house the Law Enforcement Teletype System. It consisted of a punched-paper-tape message switching system connecting all the States. All staff and funding came from the State of Arizona and American Telephone and Telegraph (AT&T). The system became so successful that the volume of message traffic overwhelmed it. In 1970, the National Law Enforcement Telecommunications Systems, Inc., was incorporated in Delaware as a not-for-profit group, operated and controlled by the States.[35]

Following massive equipment and technology upgrades over the years, and operating 24-hours-per-day, 7 days per week, by 1997, NLETS was handling some 400,000 messages daily. These messages contain vehicle registration information, drivers license information, and State criminal justice records not contained in Federal systems like NCIC. Its value is perhaps reflected by the fact that, with the exception of a 1973 system upgrade, all subsequent upgrades have been paid entirely by the States without Federal funding. Federal systems, such as NCIC, also have access to the system.[36]

Unlike the FBI's NCIC system, NLETS has taken the expensive, but necessary, step of building a system with fully-redundant computer switching capability.[37] This redundant capacity is, of course, one of the key factors in assuring availability of key infrastructures, and a key component of assuring availability of this critical service.

[35] Training brochure, NLETS, Inc., February 1995.

[36] Ibid.

[37] Ibid., p. 2.

4.c. Integrated Automated Fingerprint Identification System (IAFIS)

As the Executive Agency for criminal identification and criminal history information, on a daily basis, the FBI receives over 100,000 electronic requests for criminal history information. In addition, nearly 35,000 fingerprint card requests (for criminal justice and non-criminal justice purposes) and approximately 14,000 system updates to the criminal history file are logged in each day. Delays and backlogs in the processing of this avalanche of information requests, updates, and new criminal records are at levels that compromise the quality of law enforcement activities throughout the nation. Advances in electronic communications, expanding legislative mandates, and increased sophistication of law enforcement technology are expected to double the number of criminal history information requests by the end of this century, and without significant technology and automation improvements, this system of criminal records will grind to an absolute standstill.

In full collaboration with the other members of the U.S. law enforcement and criminal justice communities and appropriate Congressional committees, the FBI is managing the upgrading of IAFIS to fully integrate automated, electronic information management and fingerprint imaging capabilities. When completed, this computer system will dramatically improve the identification of criminals and location of criminal history records. Integrated with a major upgrade to NCIC, known as NCIC 2000, the IAFIS computer system will make possible more timely, fingerprint-based checks of criminal history records. Expanding legislative mandates, such as the so-called Brady Bill concerning the purchase of firearms, require such real-time capabilities. The Housing Opportunity Extension Act of 1996 and the National Child Protection Act of 1993 are representative examples of other expanding legislative mandates.

In short, a new, powerful law enforcement and criminal justice tool is being created. It will represent a new critical infrastructure for law enforcement, and its protection and security from physical and cyber threats and vulnerabilities will become increasingly important. Planning today for protective measures to assure the availability, reliability and integrity of IAFIS will be critical to its successful operation, and protect the huge financial investment it represents.

Conclusion

As this examination of the law enforcement infrastructure reveals, local, State, and Federal law enforcement agencies each have their own manifold jurisdictions and operating procedures. This diversity protects the infrastructure from any single physical vulnerability, or group of vulnerabilities, that could debilitate the law enforcement system. However, the four issues examined in this paper -- radio frequency allocation, terrorism training, information sharing, and criminal justice information systems -- are issues that warrant attention by those in the law enforcement community and others interested in domestic security. Cyber vulnerabilities of criminal justice networked information systems place the security of the entire network at the lowest level of system security found anywhere in the network.

Interaction with various associations, advisory groups, and Federal agencies is likely required to achieve a balanced and permissible Commission response to these issues. A comprehensive understanding of law enforcement threats and vulnerabilities would be inadequate without such interaction.