



Office of the Attorney General

Washington, D.C. 20530

April 11, 2002

MEMORANDUM FOR THE DEPUTY ATTORNEY GENERAL, THE ASSISTANT ATTORNEY GENERAL FOR THE CRIMINAL DIVISION, THE ASSISTANT ATTORNEY GENERAL FOR LEGAL POLICY, THE DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION, THE COMMISSIONER OF THE IMMIGRATION AND NATURALIZATION SERVICE, THE ADMINISTRATOR OF THE DRUG ENFORCEMENT ADMINISTRATION, THE DIRECTOR OF THE EXECUTIVE OFFICE OF UNITED STATES ATTORNEYS, THE DIRECTOR OF THE MARSHALS SERVICE, AND THE DIRECTOR OF THE FOREIGN TERRORIST TRACKING TASK FORCE.

FROM

THE ATTORNEY GENERAL

A handwritten signature in black ink, appearing to read "John Ashcroft", written over the printed name of the Attorney General.

SUBJECT:

Coordination of Information Relating to Terrorism

The prevention of terrorist activity is the overriding priority of the Department of Justice. By memoranda dated November 8 and 13, 2001, I directed Department components to review their policies and procedures to ensure information sharing, information analysis, and coordination of activities with federal, state and local agencies to prevent acts threatening public safety and national security. The Deputy Attorney General has reported to me the specific actions taken to implement those directives. I commend you on the substantial progress the Department has achieved in analyzing information, sharing intelligence, and coordinating activities in the multi-front effort to combat terrorism.

I am hereby directing you to undertake further action to institutionalize the Department's ongoing efforts to coordinate information and activities to prevent and disrupt terrorist activities.

Expand Terrorist Information in Law Enforcement Databases.

The Federal Government maintains a number of databases that provide real-time information to officials in foreign diplomatic outposts, at border points of entry, and for interior domestic law enforcement. Expansion of information in such databases relating to known and suspected terrorists will greatly enhance the ability of federal, state, and local officials to prevent terrorists from obtaining visas to enter the United States, to deny them entry into our borders, to detect and apprehend those already in the country, and to gather

intelligence on the plans and activities of terrorist conspiracies. Accordingly, I hereby direct all investigative components within the Department of Justice to establish procedures to provide, on a regular basis and in electronic format, the names, photographs (if available), and other identifying data of all known or suspected terrorists for inclusion in the following databases:

- **The Department of State TIPOFF System.** This system is designed to detect known or suspected terrorists who are not U.S. citizens as they apply for visas overseas or as they attempt to pass through U.S., Canadian, and Australian border entry points. Expanding terrorist information in the database will preclude the issuance of visas to known terrorists; warn U.S. diplomatic posts of the security risk posed by certain applicants; and alert intelligence and law enforcement agencies of the travel plans of suspected terrorists.
- **The FBI National Crime Information Center (NCIC).** The NCIC is the nations principal law enforcement automated information sharing tool. It provides on-the-street access to information to over 650,000 U.S. local, state, and federal law enforcement officers. The inclusion of terrorist information in this powerful database will assist in locating known foreign terrorists who have entered the U.S. undetected, warn law enforcement officers of a potential security risk, and alert intelligence and law enforcement agencies of the presence of a suspected terrorist at a specific location and time. Agencies contributing terrorist information should establish procedures and protocols for direct electronic input of the data into NCIC, observing applicable restrictions on the entry of classified information into the system. To expand further local and state law enforcement access to relevant terrorist information, the FBI shall establish procedures with the Department of State that will enable, on a recurring basis, the inclusion of qualifying TIPOFF data into NCIC. The FBI shall establish procedures that inform law enforcement officers what action should be taken when encountering suspected terrorists. Furthermore, the NCIC must properly characterize individuals as either suspected terrorists or known terrorists, with the latter designation reserved for individuals against whom sufficient evidence exists to justify such a determination.
- **The U.S. Customs Service Interagency Border Inspection System (IBIS).** This system is the primary automated screening tool used by both the Immigration and Naturalization Service (INS) and U.S. Customs Service at ports-of-entry. The inclusion of terrorist data in this integrated database will help preclude the entry of known and suspected terrorists into the U.S., warn inspectors of a potential security threat, and alert intelligence and law enforcement agencies that a suspected terrorist is attempting to enter the U.S. at a specific location and time. Such information on known or suspected

foreign terrorists must be placed in IBIS unless it is already accessible through an automated IBIS query of NCIC.

The procedures established for providing information to the databases listed above may allow for case-by-case exceptions where the component head or his responsible designee determines that disclosure would compromise classified information, jeopardize an investigation, or compromise a confidential source.

2. Coordinate Foreign Terrorist Information.

The international response to the September 11th attacks has been defined by multilateral cooperation and resolve to restore security and liberty to freedom-loving people of the world. The success of the response has depended in large part on improved sharing among governments of information relating to terrorists, their associates, and their activities. Continued vigilance against international terrorist conspiracies requires procedures to institutionalize such information coordination. Accordingly, I hereby direct the FBI, through its Legal Attaches, to establish procedures to obtain on a regular basis the fingerprints, other identifying information, and available biographical data of all known or suspected foreign terrorists who have been identified and processed by foreign law enforcement agencies. The FBI shall also coordinate with the Department of Defense to obtain, to the extent permitted by law, on a regular basis the fingerprints, other identifying information, and available biographical data of known or suspected foreign terrorists who have been processed by the U.S. Military. Such information shall be placed into the Integrated Automated Fingerprint Identification System (IAFIS) and other appropriate law enforcement databases to assist in detecting and locating foreign terrorists.

3. Establish Secure System for Information Coordination with State and Local Partners.

The various information systems described above are databases, triggered by a name query, that serve as an alert mechanism and pointer index. Effective information coordination requires more sophisticated mechanisms for expanded searches, multipoint information flow, and integrated analysis. Federal agencies have the benefit of classified systems that enable keyword searches of relevant documents, secure e-mail, and other important collaborative information sharing tools. However, there is no corresponding national system with comparable capability for integrated information coordination on counterterrorism with and among state and local law enforcement agencies.

By memorandum of November 13, 2001, I directed all U.S. Attorneys to develop protocols for coordinating information to, from, and among our state and local partners in law enforcement. I encouraged the use, where practicable, of technologies already available and currently in use by the Department to facilitate information-sharing. I hereby direct the Deputy Attorney General to coordinate among the applicable components the development of a secure but unclassified web-based system to enable local, state, and federal users to post,

retrieve, and read information, restrict access to certain products, send secure e-mail, and receive automatic e-mail notifications when new items are posted. This integrated system should allow for future capabilities, such as imagery and photographs, instant messaging and database access and restricted access to classified information at least at the Secret level and ideally in higher classifications.

4 Analyze Foreign Terrorist Data

On October 30, 2001, the President directed that the Department establish the Foreign Terrorist Tracking Task Force (FTTTF). The mission of the FTTTF is to keep foreign terrorists and their supporters out of the United States by providing critical and timely information to border control and interior enforcement agencies and officials. To do so requires electronic access to large sets of data, including the most sensitive material from law enforcement and intelligence sources. Analyzing such data will enable the FTTTF to discern patterns and probabilities of terrorist activities.

I hereby direct the FTTTF to identify the agency information systems and data sets needed to fulfill its mission. Each agency is to provide to the FTTTF unfiltered, timely and electronic access to the information systems and data sets deemed relevant by the Director of the FTTTF, subject to any legal restrictions on the sharing of such information.

5 Standardize Procedures for Sharing of Sensitive Information

Section 203 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. 107-56, authorizes the sharing of foreign intelligence and counterintelligence information obtained as part of a criminal investigation, including through grand jury proceedings and Title III electronic surveillance, with relevant Federal officials to assist in the performance of their duties. The officials receiving such information may use it only as necessary in the conduct of their official duties and subject to any limitations on the unauthorized disclosure of such information. The Criminal Division has developed and distributed model forms to be used to notify the supervising court when grand jury information has been shared pursuant to section 203.

Section 905 of the USA PATRIOT Act requires the Department and other Federal agencies with law enforcement responsibilities to share expeditiously foreign intelligence obtained in the course of a criminal investigation with the Director of Central Intelligence, subject to limitations otherwise provided by law and exceptions delineated in regulations to be issued by the Department. In the types of criminal cases in which foreign intelligence information is commonly encountered -- including terrorism, drug trafficking, and organized crime investigations -- strong relationships for information-sharing and coordination with the Intelligence Community are already in place.

I hereby direct the Assistant Attorney General for Legal Policy, in consultation with the Criminal Division, FBI, and other relevant components, to draft, for my consideration and promulgation, procedures, guidelines, and regulations to implement sections 203 and 905 of the USA PATRIOT Act in a manner that makes consistent and effective the standards for sharing of information, including sensitive or legally restricted information, with other Federal agencies. Those standards should be directed toward, consistent with law, the dissemination of all relevant information to Federal officials who need such information in order to prevent and disrupt terrorist activity and other activities affecting our national security. At the same time, the procedures, guidelines, and regulations should seek to ensure that shared information is not misused for unauthorized purposes, disclosed to unauthorized personnel, or otherwise handled in a manner that jeopardizes the rights of U.S. persons, and that its use does not unnecessarily affect criminal investigations and prosecutions. The standards adopted will govern the coordination of information directed by this memorandum, and well as other voluntary or mandated sharing of criminal investigative information.

* * *

The September 11 attacks demonstrate that the war on terrorism must be fought and won at home as well as abroad. To meet this continuing threat, law enforcement officials at all levels of government -- federal, state, and local -- must work together, coordinating information and leveraging resources in the joint effort to prevent and disrupt terrorist activity. You have worked hard and accomplished much in this common fight, but more remains to be done to help secure America and protect her people. I thank you for your continued service, dedication, and cooperative spirit in this time of continuing national need.