

EXHIBIT “JJ”

FBI Finds It Frequently Overstepped in Collecting Data

By John Solomon
Washington Post Staff Writer
Thursday, June 14, 2007; A01

An internal [FBI](#) audit has found that the bureau potentially violated the law or agency rules more than 1,000 times while collecting data about domestic phone calls, e-mails and financial transactions in recent years, far more than was documented in a [Justice Department](#) report in March that ignited bipartisan congressional criticism.

The new audit covers just 10 percent of the bureau's national security investigations since 2002, and so the mistakes in the FBI's domestic surveillance efforts probably number several thousand, bureau officials said in interviews. The earlier report found 22 violations in a much smaller sampling.

The vast majority of the new violations were instances in which telephone companies and Internet providers gave agents phone and e-mail records the agents did not request and were not authorized to collect. The agents retained the information anyway in their files, which mostly concerned suspected terrorist or espionage activities.

But two dozen of the newly-discovered violations involved agents' requests for information that U.S. law did not allow them to have, according to the audit results provided to [The Washington Post](#). Only two such examples were identified earlier in the smaller sample.

FBI officials said the results confirmed what agency supervisors and outside critics feared, namely that many agents did not understand or follow the required legal procedures and paperwork requirements when collecting personal information with one of the most sensitive and powerful intelligence-gathering tools of the post-Sept. 11 era -- the National Security Letter, or NSL.

Such letters are uniformly secret and amount to nonnegotiable demands for personal information -- demands that are not reviewed in advance by a judge. After the 2001 terrorist attacks, Congress substantially eased the rules for issuing NSLs, requiring only that the bureau certify that the records are "sought for" or "relevant to" an investigation "to protect against international terrorism or clandestine intelligence activities."

The change -- combined with national anxiety about another domestic terrorist event -- led to an explosive growth in the use of the letters. More than 19,000 such letters were issued in 2005 seeking 47,000 pieces of information, mostly from telecommunications companies. But with this growth came abuse of the newly relaxed rules, a circumstance first revealed in the Justice Department's March report by [Inspector General Glenn A. Fine](#).

"The FBI's comprehensive audit of National Security Letter use across all field offices has confirmed the inspector general's findings that we had inadequate internal controls for use of an invaluable

Advertisement

The Orange Savings Account

4.50% APY
No Fees. No Minimums.

ING DIRECT
Save Your Money

Open Now Member FDIC

investigative tool," FBI General Counsel Valerie E. Caproni said. "Our internal audit examined a much larger sample than the inspector general's report last March, but we found similar percentages of NSLs that had errors."

"Since March," Caproni added, "remedies addressing every aspect of the problem have been implemented or are well on the way."

Of the more than 1,000 violations uncovered by the new audit, about 700 involved telephone companies and other communications firms providing information that exceeded what the FBI's national security letters had sought. But rather than destroying the unsolicited data, agents in some instances issued new National Security Letters to ensure that they could keep the mistakenly provided information. Officials cited as an example the retention of an extra month's phone records, beyond the period specified by the agents.

Case agents are now told that they must identify mistakenly produced information and isolate it from investigative files. "Human errors will inevitably occur with third parties, but we now have a clear plan with clear lines of responsibility to ensure errant information that is mistakenly produced will be caught as it is produced and before it is added to any FBI database," Caproni said.

The FBI also found that in 14 investigations, counterintelligence agents using NSLs improperly gathered full credit reports from financial institutions, exercising authority provided by the [USA](#) Patriot Act but meant to be applied only in counterterrorism cases. In response, the bureau has distributed explicit instructions that "you can't gather full credit reports in counterintelligence cases," a senior FBI official said.

In 10 additional investigations, FBI agents used NSLs to request other information that the relevant laws did not allow them to obtain. Officials said that, for example, agents might have requested header information from e-mails -- such as the subject lines -- even though NSLs are supposed to be used to gather information only about the e-mails' senders and the recipients, not about their content.

The FBI audit also identified three dozen violations of rules requiring that NSLs be approved by senior officials and used only in authorized cases. In 10 instances, agents issued National Security Letters to collect personal data without tying the requests to specific, active investigations -- as the law requires -- either because, in each case, an investigative file had not been opened yet or the authorization for an investigation had expired without being renewed.

FBI officials said the audit found no evidence to date that any agent knowingly or willingly violated the laws or that supervisors encouraged such violations. The Justice Department's report estimated that agents made errors about 4 percent of the time and that third parties made mistakes about 3 percent of the time, they said. The FBI's audit, they noted, found a slightly higher error rate for agents -- about 5 percent -- and a substantially higher rate of third-party errors -- about 10 percent.

The officials said they are making widespread changes to ensure that the problems do not recur. Those changes include implementing a corporate-style, continuous, internal compliance program to review the bureau's policies, procedures and training, to provide regular monitoring of employees' work by supervisors in each office, and to conduct frequent audits to track compliance across the bureau.

The bureau is also trying to establish for NSLs clear lines of responsibility, which were lacking in the past, officials said. Agents who open counterterrorism and counterintelligence investigations have been told that they are solely responsible for ensuring that they do not receive data they are not entitled to have.

The FBI audit did not turn up new instances in which another surveillance tool known as an Exigent Circumstance Letter had been abused, officials said. In a finding that prompted particularly strong concerns on [Capitol Hill](#), the Justice Department had said such letters -- which are similar to NSLs but are meant to be used only in security emergencies -- had been invoked hundreds of times in "non-emergency circumstances" to obtain detailed phone records, mostly without the required links to active investigations.

Many of those letters were improperly dispatched by the bureau's Communications Analysis Unit, a central clearinghouse for the analysis of telephone records such as those gathered with the help of "exigent" letters and National Security Letters. Justice Department and FBI investigators are trying to determine if any FBI headquarters officials should be held accountable or punished for those abuses, and have begun advising agents of their due process rights during interviews.

The FBI audit will be completed in the coming weeks, and Congress will be briefed on the results, officials said. FBI officials said each potential violation will then be extensively reviewed by lawyers to determine if it must be reported to the Intelligence Oversight Board, a presidential panel of senior intelligence officials created to safeguard civil liberties.

The officials said the final tally of violations that are serious enough to be reported to the panel might be much less than the number turned up by the audit, noting that only five of the 22 potential violations identified by the Justice Department's inspector general this spring were ultimately deemed to be reportable.

"We expect that percentage will hold or be similar when we get through the hundreds of potential violations identified here," said a senior FBI official, who spoke on the condition of anonymity because the bureau's findings have not yet been made public.

[View all comments](#) that have been posted about this article.

Post a Comment

Ad

Join the discussion. Sponsored by Cisco.  welcome to the human network. **CISCO**

[View all comments](#) that have been posted about this article.

Your washingtonpost.com User ID, rwinant, will be displayed with your comment.

You must be logged in to leave a comment. [Log in](#) | [Register](#)

Submit

Comments that include profanity or personal attacks or other inappropriate comments or material will be removed from the site. Additionally, entries that are unsigned or contain "signatures" by someone other than the actual author will be removed. Finally, we will take steps to block users who violate any of our posting standards, terms of use or privacy policies or any other policies governing this site. Please review the [full rules](#) governing commentaries and discussions. You are fully responsible for the content that you post.

Ads by Google

[Exxonmobil](#)

Review our 2006 Corporate Citizenship Report

www.exxonmobil.com

[Say "No" to Globalism](#)

America is being plundered We tell you who, how and why

www.AugustReview.com

[Sustainable Business](#)

MBA with sustainability focus. Change business for good.

BGledu.org

EXHIBIT “KK”

~~SECRET~~

**THE ATTORNEY GENERAL'S GUIDELINES FOR
FBI NATIONAL SECURITY INVESTIGATIONS
AND FOREIGN INTELLIGENCE COLLECTION (U)**

EFFECTIVE: October 31, 2003

Classified by: John Ashcroft, Attorney General

Reason: 1.4(c)

Declassify on: October 31, 2028

~~SECRET~~

~~SECRET~~

PREAMBLE (U)

The following Guidelines on national security investigations and foreign intelligence collection by the Federal Bureau of Investigation (FBI) are issued under the authority of the Attorney General as provided in sections 509, 510, 533, and 534 of title 28, United States Code. They apply to activities of the FBI pursuant to Executive Order 12333 and other activities as provided herein. (U)

~~SECRET~~

~~SECRET~~

TABLE OF CONTENTS (U)

INTRODUCTION 1

A. NATIONAL SECURITY INVESTIGATIONS 2

B. FOREIGN INTELLIGENCE COLLECTION 5

C. STRATEGIC ANALYSIS 5

D. RETENTION AND DISSEMINATION OF INFORMATION 6

I. GENERAL AUTHORITIES AND PRINCIPLES 6

A. GENERAL AUTHORITIES 6

B. USE OF AUTHORITIES AND METHODS 7

C. DETERMINATION OF UNITED STATES PERSON STATUS 9

D. NATURE AND APPLICATION OF THE GUIDELINES 10

II. NATIONAL SECURITY INVESTIGATIONS 11

A. THREAT ASSESSMENTS 12

B. COMMON PROVISIONS FOR PRELIMINARY AND FULL INVESTIGATIONS 13

C. PRELIMINARY INVESTIGATIONS 15

D. FULL INVESTIGATIONS 16

E. EXTRATERRITORIAL OPERATIONS 17

III. INVESTIGATIVE ASSISTANCE TO STATE, LOCAL, AND FOREIGN GOVERNMENTS 18

~~SECRET~~

~~SECRET~~

A.	STATE AND LOCAL GOVERNMENTS	18
B.	FOREIGN GOVERNMENTS	18
IV.	<u>FOREIGN INTELLIGENCE COLLECTION AND ASSISTANCE TO INTELLIGENCE AGENCIES</u>	19
A.	FOREIGN INTELLIGENCE COLLECTION	19
B.	OPERATIONAL SUPPORT	20
C.	CENTRAL INTELLIGENCE AGENCY AND DEPARTMENT OF DEFENSE ACTIVITIES WITHIN THE UNITED STATES	20
V.	<u>INVESTIGATIVE TECHNIQUES</u>	21
VI.	<u>STRATEGIC ANALYSIS</u>	23
VII.	<u>RETENTION AND DISSEMINATION OF INFORMATION</u>	23
A.	INFORMATION SYSTEMS AND DATABASES	23
B.	INFORMATION SHARING	24
C.	SPECIAL STATUTORY REQUIREMENTS	32
VIII.	<u>DEFINITIONS</u>	33

(U)

~~SECRET~~

~~SECRET~~

2. **Departures from the Guidelines (U)**

Departures from these Guidelines must be approved by the Attorney General, the Deputy Attorney General, or an official designated by the Attorney General. If a departure from these Guidelines is necessary without such prior approval because of the immediacy or gravity of a threat to the national security or to the safety of persons or property and the need to take immediate action to protect against such a threat, the Attorney General, the Deputy Attorney General, or an official designated by the Attorney General shall be notified as soon thereafter as practicable. The FBI shall provide timely written notice of departures from these Guidelines to the Office of Intelligence Policy and Review. Notwithstanding this paragraph, all activities in all circumstances must be carried out in a manner consistent with the Constitution and laws of the United States. (U)

3. **Interpretation (U)**

All significant new legal questions as to the coverage and interpretation of these guidelines will be resolved initially by the Office of Intelligence Policy and Review and reviewed by the Deputy Attorney General or Attorney General as appropriate. (U)

II. NATIONAL SECURITY INVESTIGATIONS (U)

The levels of investigative activity in national security investigations are: (1) threat assessments; (2) preliminary investigations; and (3) full investigations. If the available information shows at any point that the threshold standard for a preliminary investigation or full investigation is satisfied, then that level of investigative activity may be initiated immediately, without progressing through more limited investigative stages. (U)

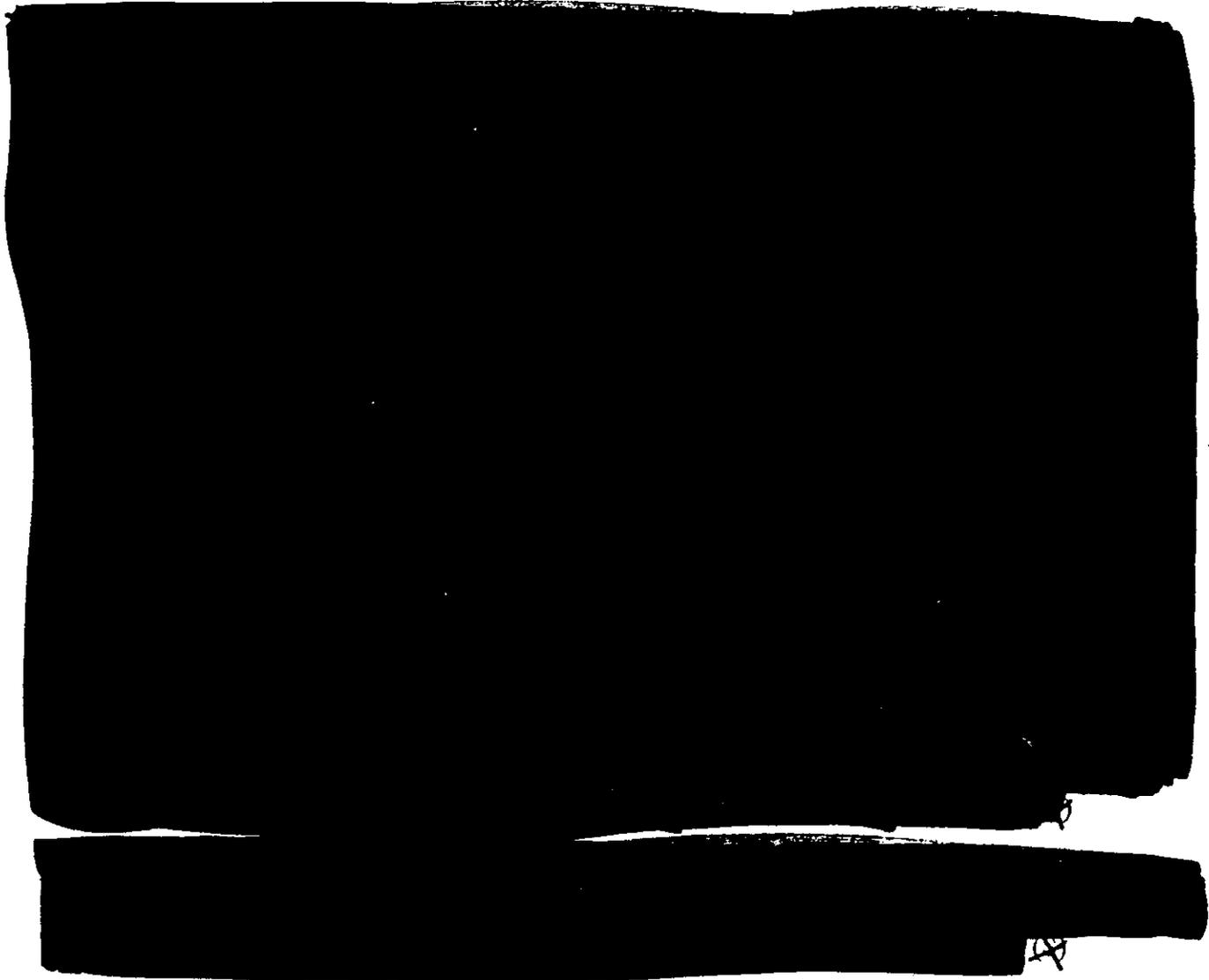
The scope of authorized activities under this Part is not limited to "investigation" in a narrow sense, such as solving particular cases or obtaining evidence for use in particular criminal prosecutions. Rather, these activities also provide critical information needed for broader analytic and intelligence purposes authorized by Executive Order 12333 and these Guidelines to protect the national security, such as strategic analysis under Part VI, dissemination of information to other agencies in the Intelligence Community under Part VII.B, and dissemination of information to appropriate White House officials under Part VII.B. Information obtained at all stages of investigative activity – threat assessments, preliminary investigations, and full investigations – is accordingly to be retained and disseminated for these purposes as provided in these Guidelines, or in FBI policy consistent with these

~~SECRET~~

~~SECRET~~

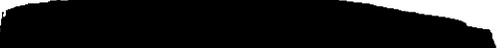
Guidelines, regardless of whether it furthers investigative objectives in a narrower or more immediate sense. (U)

A. THREAT ASSESSMENTS (U)



~~SECRET~~

~~SECRET~~

b. The number of preliminary investigations 



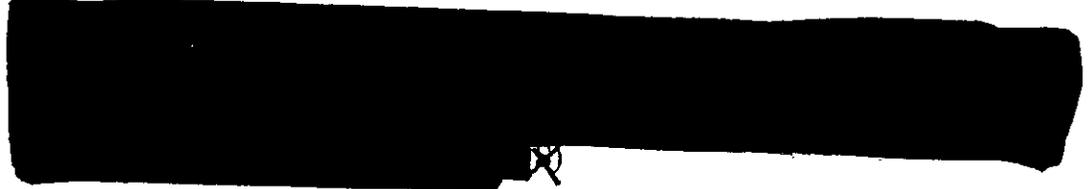
c. The number of full investigations 



d.



e.



B. INFORMATION SHARING (U)

Legal rules and Department of Justice policies regarding information sharing and interagency coordination have been significantly modified since the September 11, 2001, terrorist attack by statutory reforms and new Attorney General guidelines. The general principle reflected in current laws and policies is that information should be shared as consistently and fully as possible among agencies with relevant responsibilities to protect the United States and its people from terrorism and other threats to the national security, except as limited by specific constraints on such sharing. Under this general principle, the FBI shall provide information expeditiously to other agencies in the Intelligence Community, so that these agencies can take action in a timely manner to protect the national security in accordance with their lawful functions. This Subpart provides standards and procedures for the sharing and dissemination of information obtained in national security investigations, foreign intelligence collection, and other activities under these Guidelines. (U)

~~SECRET~~

~~SECRET~~

1. **General (U)**

- a. Information may be disseminated with the consent of the person whom the information concerns, or where necessary to protect life or property from threatened force or violence, otherwise necessary for the safety or security of persons or property or for the prevention of crime, or necessary to obtain information for the conduct of a lawful investigation by the FBI. (U)
- b. Information that is publicly available or does not identify United States persons may be disseminated for any lawful purpose. (U)
- c. Dissemination of information provided to the FBI by other Intelligence Community agencies is subject to applicable agreements and understandings with such agencies concerning the dissemination of such information. (U)

2. **Department of Justice (U)**

- a. The FBI may share information obtained through activities under these Guidelines with other components of the Department of Justice. (U)
- b. The Criminal Division and the Office of Intelligence Policy and Review shall have access to all information obtained through activities under these Guidelines except as limited by orders issued by the Foreign Intelligence Surveillance Court, controls imposed by the originators of sensitive material, or restrictions established by the Attorney General or the Deputy Attorney General in particular cases. (U)
- c. The FBI shall keep the Criminal Division and the Office of Intelligence Policy and Review apprised of all information obtained through activities under these Guidelines that is necessary to the ability of the United States to investigate or protect against threats to the national security, subject to the limits noted in subparagraph b. The FBI shall also keep the Criminal Division and the Office of Intelligence Policy and Review apprised of information concerning any crime which is obtained through activities under these Guidelines. (U)
- d. As part of its responsibility under subparagraphs b. and c., the FBI shall provide to the Criminal Division and the Office of Intelligence Policy and

~~SECRET~~

~~SECRET~~

Review notices of the initiation of investigations and annual notices and summaries as provided in Part II.B.2 and .D.4 of these Guidelines, and shall make available to the Criminal Division and the Office of Intelligence Policy and Review relevant information from investigative files. The Criminal Division shall adhere to any reasonable conditions on the storage and disclosure of such documents and information that the FBI and the Office of Intelligence Policy and Review may require. The FBI and the Criminal Division may adopt by mutual agreement exceptions to the provision of notices of the initiation of investigations and annual notices and summaries to the Criminal Division, and the FBI and the Office of Intelligence Policy and Review may adopt by mutual agreement exceptions to the provision of notices of initiation of investigations and annual notices and summaries to the Office of Intelligence and Policy Review. (U)

- e. The FBI, the Criminal Division, and the Office of Intelligence Policy and Review shall consult with each other concerning national security investigations and other activities under these Guidelines, and shall meet regularly to conduct such consultations. Consultations may also be conducted directly between two or more components at any time. Consultations may include the exchange of advice and information on all issues necessary to the ability of the United States to investigate or protect against threats to the national security, including protection against such threats through criminal investigation and prosecution. Consultations are subject to any limitations in orders of the Foreign Intelligence Surveillance Court and restrictions established by the Attorney General or the Deputy Attorney General in particular cases. Disagreements arising from consultations may be presented to the Deputy Attorney General or the Attorney General for resolution. (U)
- f. Subject to subparagraphs g. and h., relevant United States Attorneys' offices shall receive information and engage in consultations to the same extent as the Criminal Division. Thus, the relevant United States Attorneys' offices shall have access to information, shall be kept apprised of information necessary to protect national security, shall be kept apprised of information concerning crimes, shall receive notices of the initiation of investigations and annual summaries as provided in Part II.B.2 and .D.4 of these Guidelines, and shall have access to FBI files, to the same extent as the Criminal Division. The relevant United States Attorneys' offices shall receive such access and

~~SECRET~~

~~SECRET~~

information from the FBI field offices. The relevant United States Attorneys' offices also may and shall engage in regular consultations with the FBI and the Office of Intelligence Policy and Review to the same extent as the Criminal Division. (U)

- g. In espionage cases, dissemination of information to United States Attorneys' offices and consultations between the FBI and United States Attorneys' offices are subject to authorization by the Criminal Division. In an emergency, the FBI may disseminate information to, and consult with, a United States Attorney's office concerning an espionage investigation without the approval of the Criminal Division, but shall notify the Criminal Division as soon as possible thereafter. (U)
- h. Information disseminated to a United States Attorney's office pursuant to subparagraph f. shall be disseminated only to the United States Attorney and/or any Assistant United States Attorneys designated to the Department of Justice by the United States Attorney as points of contact to receive such information. The United States Attorneys and designated Assistant United States Attorneys shall have appropriate security clearances and shall receive training in the handling of classified information and information derived from FISA, including training concerning restrictions on the use and dissemination of such information. (U)

3. Intelligence Community, Federal Law Enforcement Agencies, and Department of Homeland Security (U)

- a. The FBI shall carry out the requirements of the Memorandum of Understanding Between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing ("Memorandum of Understanding"), signed by the Attorney General on March 4, 2003. As provided in the Memorandum of Understanding and subject to its provisions, these requirements include timely sharing by the FBI of covered information with other covered entities having a need-to-know, based on a broad interpretation of the missions of the prospective recipients. As used in this paragraph:
 - 1) 'covered entity' has the same meaning as in the Memorandum of

~~SECRET~~

~~SECRET~~

- Understanding, including any element of the Department of Homeland Security (and that Department itself); any element of the Intelligence Community (including the Central Intelligence Agency and the Terrorist Threat Integration Center) or of the Department of Justice; and any other entity having federal law enforcement responsibilities;
- 2) 'covered information' has the same meaning as in the Memorandum of Understanding, including terrorism information, weapons of mass destruction information, and vulnerabilities information, as well as analyses based wholly or in part on such covered information;
 - 3) 'need-to-know,' 'infrastructure,' 'terrorism information,' 'vulnerabilities information,' and 'weapons of mass destruction information' have the same meanings as in the Memorandum of Understanding; and
 - 4) 'timely sharing' of covered information means provision by the FBI of covered information, subject to section 3(h) and other provisions of the Memorandum of Understanding, to other covered entities having a need-to-know: (i) immediately where the FBI reasonably believes that the information relates to a potential terrorism or weapons of mass destruction threat, to the United States Homeland, its infrastructure, or to United States persons or interests, and (ii) as expeditiously as possible with respect to other covered information. (U)
- b. All procedures, guidelines, and mechanisms under the Memorandum of Understanding shall be designed and implemented, and all determinations with regard to sharing information covered by the Memorandum of Understanding shall be made, with the understood, overriding priority of preventing, preempting, and disrupting terrorist threats to the United States. In some cases, this priority will dictate the provision of information even where doing so may affect criminal prosecutions or ongoing law enforcement or intelligence operations. However, consistent with this overriding priority, the FBI shall act in a manner to protect, to the greatest extent possible, these other significant interests, including the protection of intelligence and sensitive law enforcement sources and methods, other classified information, and sensitive operational and prosecutorial information. (U)

~~SECRET~~

~~SECRET~~

- c. To the greatest extent possible, information should be shared among covered entities with relevant missions and responsibilities, and there should be transparency among them with regard to their activities to preempt, prevent, and disrupt terrorist attacks against United States persons and interests. Except as otherwise specified in the Memorandum of Understanding, or mandated by relevant federal statutes or Presidential Directives, procedures and mechanisms for information sharing, use, and handling shall be interpreted and implemented consistently and reciprocally regardless of the role a particular entity plays as a provider or recipient of covered information. (U)

4. Federal Authorities (U)

The FBI may disseminate information obtained through activities under these Guidelines to other federal authorities when:

- a. the information relates to a crime or other violation of law or regulation which falls within the recipient's investigative jurisdiction, or the information otherwise relates to the recipient's authorized responsibilities;
- b. the recipient is a component of the Intelligence Community, and the information is provided to allow the recipient to determine whether the information is relevant to its responsibilities and can be retained or used;
- c. the information is required to be furnished to another federal agency by Executive Order 10450 or its successor; or
- d. the information is required to be disseminated by statute, Presidential directive, National Security Council directive, Attorney General directive, or interagency agreement approved by the Attorney General. (U)

5. State and Local Authorities (U)

The FBI may disseminate information obtained through activities under these Guidelines to state and local authorities when:

- a. the information relates to a crime or other violation of law or regulation which falls within the recipient's jurisdiction, and the dissemination is consistent with

~~SECRET~~

~~SECRET~~

national security;

- b. the dissemination is for the purpose of preventing or responding to a threat to the national security, or to public safety, including a threat to the life, health, or safety of any individual or community; or
- c. the information is required to be disseminated by statute, Presidential directive, National Security Council directive, Attorney General directive, or intergovernmental agreement approved by the Attorney General. (U)

6. Foreign Authorities (U)

- a. The FBI may disseminate information obtained through activities under these Guidelines to foreign authorities when:
 - 1) the dissemination of the information is in the interest of the national security of the United States, or the information is relevant to the recipient's authorized responsibilities and its dissemination is consistent with the national security interests of the United States, and the FBI has considered the effect such dissemination may reasonably be expected to have on any identifiable United States person; or
 - 2) the information is required to be disseminated by statute or treaty, Presidential directive or executive agreement, National Security Council directive, or Attorney General directive. (U)
- b. Dissemination to foreign authorities having significant implications for foreign relations shall be coordinated with the Department of State. (U)

7. Congressional Committees (U)

Except for briefings and testimony on matters of general intelligence interest, information obtained through activities under these Guidelines may be disseminated to appropriate congressional committees when authorized by the Attorney General, the Deputy Attorney General, or an official designated by the Attorney General. Any agency requesting or involved in the collection of the information shall be consulted prior to such dissemination. A request for United States person information that has been

~~SECRET~~