**U.S. Department of Justice**

Office of the Deputy Attorney General

The Deputy Attorney General

*Washington, D.C. 20530*

January 31, 2002

MEMORANDUM FOR THE ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION
ALL UNITED STATES ATTORNEYS
THE DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION
THE ADMINISTRATOR OF THE DRUG ENFORCEMENT ADMINISTRATION
THE COMMISSIONER OF THE IMMIGRATION AND NATURALIZATION SERVICE
THE DIRECTOR OF THE UNITED STATES MARSHALS SERVICE

FROM: Larry D. Thompson
Deputy Attorney General

SUBJECT: Procedures for the Use of Classified Investigative Technologies in Criminal Cases

The widespread availability of new technologies, such as encryption, can present significant problems in searching for and obtaining evidence of crimes. At the same time, technological advances may be available to law enforcement to surmount these problems. However, the use of sophisticated technologies in criminal investigations can raise novel and difficult issues of law and policy, especially where significant law enforcement or national security interests could be implicated by the public disclosure of details relating to those technologies during the course of legal proceedings.

To ensure that the use of such technologies in criminal investigations is approached in a careful and coordinated manner, I am hereby instituting the following measures. The requirements of this memorandum are intended to meet two objectives: first, that we make fully informed decisions about whether and how to use classified investigative technologies in criminal cases; and second, that we draw on the fullest possible range of legal and technical expertise in determining how best to proceed in obtaining evidence in increasingly complex technical settings.

I. Scope of this Memorandum.

(A) "Classified investigative technology". For purposes of this memorandum, the term "classified investigative technology" means any hardware, software, or other investigative technology that satisfies the following criteria:

(1) the hardware, software, or other investigative technology is designed to intercept or acquire information of evidentiary value as a result of a system or process which is based, in whole or in part, upon information which, at the time of its use, has been classified pursuant to Executive Order 12958 of April 17, 1995, as amended, or any successor Executive Order; and

(2) there is a reasonable possibility that–

(a) the evidentiary information to be obtained by the technology will be sought to be introduced into evidence in order to prove any charge brought by the United States;

(b) disclosure of details concerning such technology will be necessary to authenticate evidentiary information sought to be introduced into evidence in order to prove any charge brought by the United States; *or*

(c) the use of the particular technology will be the subject of a motion to suppress or other such litigation.

(B) "Deployment in a criminal investigation". This memorandum applies only to technologies deployed in connection with an authorized criminal investigation. This memorandum does not apply to the deployment of a technology in any collection activity authorized under the Foreign Intelligence Surveillance Act of 1978, as amended (FISA), or Executive Order No. 12333 (United States Intelligence Activities), 46 Fed. R. 59941 (December 4, 1981). The requirements and procedures applicable in such matters remain unaffected by this memorandum.

II. Procedures with Respect to Classified Investigative Technologies.

(A) Prior Approval Required for Deployment of Classified Investigative Technologies in Criminal Investigations. Prior to the deployment of a classified investigative technology in a criminal investigation, the relevant United States Attorney's Offices, as well as any Departmental investigative agency involved, shall promptly notify the Criminal Division of the proposed deployment. Thus, for example, the Federal Bureau of Investigation, the Drug Enforcement Administration, the Immigration and Naturalization Service, and the United States Marshals Service must bring any proposed deployment of a classified investigative technology in a criminal investigation to the attention of the Criminal Division. To the extent that an investigative agency has not already done so, it shall at the same time also notify the relevant United States Attorney's Offices of any such proposed deployment.

Upon such notification, the Assistant Attorney General for the Criminal Division (AAG) shall ensure that the Criminal Division promptly and fully consults with the relevant investigative agency involved, and (in any case in which the technology in question is one

developed in whole or in part by the Federal Bureau of Investigation) with the FBI. The AAG shall thereafter make a recommendation regarding the contemplated deployment, taking into account the nature of the investigation, the nature of the evidence to be obtained, the type of judicial or other authorization required to obtain the evidence, the risk of public disclosure of the method during the course of litigation, the law enforcement or national security interests that could be implicated by disclosure of the method, the privacy interests at stake, and the availability of court-ordered protective measures. The recommendation shall promptly be forwarded to the Deputy Attorney General for review and approval or disapproval of the recommendation.

In reviewing a proposed deployment, the Criminal Division should consider the extent to which different forms of judicial orders could affect the risk that a classified investigative technology will later be ordered to be disclosed. For example, it is important to recognize that the use of novel methods in the course of an interception or seizure of computer data can present significant questions about the appropriate form of judicial order to be sought in a particular case. Highly technical considerations, with respect both to configuration of the object of the order and to the investigative method to be used, may, for example, dictate whether a search warrant or Title III order is appropriate. Thus, part of the Criminal Division's role in reviewing the use of classified investigative technologies will be to draw on available technical expertise, as needed, in the consideration of legal and policy issues.

(B) Prompt Notification of Legal Challenges to Classified Investigative Technologies. The United States Attorneys' Offices shall promptly notify the Criminal Division of any legal proceeding in which there may be potential access to, and/or disclosure of, classified investigative technologies that have been used in a criminal investigation. Thus, for example, the Criminal Division should be immediately notified of any demand or motion for the disclosure of a classified investigative technology. Similarly, if any case is being prosecuted, or considered for prosecution, in which a classified investigative technology was deployed without adherence to the procedures set forth in paragraph (A), the relevant United States Attorney's Office shall notify the Criminal Division as soon as it learns of any such deployment. The Assistant Attorney General for the Criminal Division shall supervise all litigation regarding the potential disclosure of classified investigative technologies.

(C) Exception for Emergencies Involving Imminent Danger. Notwithstanding paragraph (A), the Deputy Attorney General, the Assistant Attorney General for the Criminal Division, or any person designated by either of them, may authorize, in accordance with and to the extent permitted by applicable law and any required court process, immediate deployment of a classified investigative technology if he or she reasonably determines that an emergency involving either immediate danger of death or serious physical injury to any person or imminent harm to the national security requires deployment without delay. The Deputy Attorney General shall be promptly notified of all deployments authorized under this paragraph.

(D) Adherence to National Security Information Protocols. All Department personnel are reminded that all notifications and transmittals under this memorandum must adhere to all applicable protocols and requirements governing the transmission of National Security Information.

(E) Initial Point of Contact for Required Notifications. Agents or attorneys may initially contact the Criminal Division, as follows, in order to arrange for proper transmission of any required notifications:

Maureen H. Killion, Director
Office of Enforcement Operations
Criminal Division/DOJ
John C. Keeney Building
1301 New York Avenue, N.W.
Washington, D.C. 20530
Phone: (202) 514-6809
Fax: (202) 616-8256

(F) Construction of this Memorandum. This Memorandum is limited to improving the internal management of the Department and is not intended to, nor does it, create any right, benefit, or privilege, substantive or procedural, enforceable at law or equity, by any party against the United States, the Department of Justice, their officers or employees, or any other person or entity. Nor should this Memorandum be construed to create any right to judicial review involving the compliance or noncompliance of the United States, the Department, their officers or employees, or any other person or entity, with this Memorandum.