



U.S. Department of Justice

Office of Information and Privacy

Telephone: (202) 514-3642

Washington, D.C. 20530

MAR - 8 2007

Mr. Steven Aftergood
Federation of American Scientists
1717 K Street NW, Suite 209
Washington, DC 20036

RE: AG/04-R0014
OLA/04-R0015
PAO/04-R0016
CLM:VRB:SBL:GEB

Dear Mr. Aftergood:

This is our final response to your Freedom of Information Act request dated October 2, 2003, and received in this Office on October 9, 2003, for a copy of the prepared testimony given by former Attorney General Janet Reno before the Senate Select Committee on Intelligence on June 14, 2000. This response is made on behalf of the Offices of the Attorney General, Legislative Affairs (OLA), and Public Affairs.

A search was conducted in OLA and one document, totaling seventeen pages, responsive to your request was located. I have determined that this document is appropriate for release without excision, and a copy is enclosed.

Inasmuch as this constitutes a full grant of your request, I am closing your file in this Office.

Sincerely,

A handwritten signature in black ink, appearing to read "C. Mallon", written in a cursive style.

Carmen L. Mallon
Chief, Initial Request Staff

Enclosure



Department of Justice

STATEMENT

OF

JANET RENO
ATTORNEY GENERAL
U.S. DEPARTMENT OF JUSTICE

BEFORE

THE

SENATE SELECT COMMITTEE
ON INTELLIGENCE

CONCERNING

UNAUTHORIZED DISCLOSURE OF CLASSIFIED INFORMATION

JUNE 14, 2000

OLA-1

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to appear before you to discuss the difficult problem of unauthorized disclosures of classified information. I share Committee's concerns regarding this important subject.

Although there are a number of types of unauthorized disclosures, the most damaging are leaks of classified information to the news media. Media leaks have frustrated Administration after Administration - Democrat and Republican - for decades, and numerous potential legislative and administrative remedies have been explored - all with little success. Congress has held repeated hearings on leaks over the last twenty years, and interagency review groups have suggested various solutions, but the fact is that there is no easy answer to preventing leaks or catching leakers.

At the outset, I want to assure this Committee that the Department understands full well the very serious damage to the national security caused by leaks of classified information. When intelligence agencies alert us to media leaks, they describe

for us the effect of the disclosure on the national security. From these descriptions, it is clear that virtually all the elements of the Intelligence Community and the Defense Department have suffered severe losses of sources, methods, and important liaison relationships due to leaks. Leaks also have caused damage in the conduct of our diplomatic efforts. Moreover, these leaks are frequently brazen. Some leakers are willing to give members of the media extraordinarily sensitive details about intelligence sources and technical capabilities and even to provide copies of highly classified intelligence reports.

I also want to emphasize leaks do not just affect other Departments and agencies. They have had a direct and serious impact on the Justice Department itself; leaks of sensitive intelligence information have hampered some of our most sensitive espionage and terrorism investigations and have jeopardized our prosecutions. So, we are certainly motivated to want to do something about this problem.

Accordingly, I want to emphasize today that the Department of Justice is absolutely committed to investigating and prosecuting those responsible for leaking classified information, or for bringing civil actions against them where appropriate.

Like other Attorneys General before me, I personally am extremely frustrated about the problem of leaks. I have had numerous discussions over the last seven years with the National Security Advisor, the DCI, the Secretary of Defense, and the Secretary of State about ways to address the problem. I have met regularly with the Criminal Division to discuss particular leak investigations and to explore ways to improve our investigations and bring more prosecutions. I have also received and read the letters this Committee has written to me over the last several years regarding specific media leaks. (I might add that we have opened a criminal investigation into almost every one of these cases.)

Now, I would like to describe the process by which investigations are opened and pursued. Our Criminal Division is usually notified of a leak in writing by the agency whose information was disclosed through established crimes reporting procedures. As you know, Executive Order 12333 requires that the Intelligence Community report violations of Federal law by employees to the Department of Justice. A Memorandum of Understanding between the Department of Justice and the Intelligence Community agencies requires that such crimes, including unauthorized disclosures of classified information, be

reported to the Criminal Division. In practice, the overwhelming majority of crime reports regarding unauthorized disclosures are submitted by CIA and NSA.

During the last several years, we have received roughly 50 crime reports each year of leaks to the media of classified information. Because of the large number of leaks and the recognition that the Department and the FBI have limited investigative resources, intelligence agencies do not request criminal investigations of every unauthorized disclosure of classified information. Instead, they request investigations of the most damaging leaks, usually around 20-25 cases a year for the last several years. We have opened investigations into almost all of the leaks requested by the victim agencies.

Before opening a criminal investigation, the Criminal Division generally requires the agency requesting the investigation to submit the answers to eleven specific questions regarding what was leaked and who had access to it. Generally, when submitting an initial crime report, an intelligence agency will advise us that it is conducting a preliminary internal investigation and will provide the answers to the eleven questions later if it decides to ask for a criminal

investigation. Occasionally, if the leak is of especially sensitive or closely-held information, the answers to the eleven questions will accompany the initial crime report. A few investigations have been opened as a result of an oral request by a senior intelligence community official without receipt of the answers to the eleven questions.

The requirement that the agency answer the 11 questions before an investigation is authorized dates to at least 1969. We believe that the eleven questions serve an important screening function in at least two respects. First, they require that the classified information at issue, and any source document from which it arose, be identified with specificity. Second, and most important, they require the agency to make a good faith estimate of the extent of the dissemination of the classified information.

We believe that the eleven questions are essentially the equivalent of filing a police report. They provide the information we need to determine whether a criminal investigation is likely to be productive and, if so, where to start. I want to emphasize that we do not inflexibly insist on the eleven questions in every case. In especially egregious cases or cases where the victim agency knows that the dissemination is very

limited, we have been willing to open an investigation and to take investigative steps in the absence of the eleven questions or even in the absence of the crime report required under the Crime Reporting MOU.

Once the answers to the eleven questions and a request for investigation are received, our Internal Security Section evaluates the information and, where appropriate, sends a memorandum to the National Security Division of the FBI requesting an investigation. The extent of the dissemination is a key element in the evaluation, but we have not adopted a precise number as being dispositive of the decision to proceed with an investigation.

After an investigation has been opened, it is conducted by FBI agents and supervised by the Internal Security Section of our Criminal Division. Lawyers in this section have extensive experience supervising media leak as well as espionage investigations. Internal Security attorneys meet directly with the FBI case agents, as appropriate, to devise overall investigative strategy, to coordinate on sensitive interviews (such as interviews of senior officials or of Members of

Congress), and to ensure that all leads are covered consistent with Department policy in this sensitive area.

When conducting a media leak investigation, the Department's longstanding practice - both in this Administration and prior Administrations - has been to focus the investigation on the universe of potential leakers rather than on the reporter. While this practice has made our job far more difficult, it represents a policy judgment that takes into account concerns that a free press not be unduly chilled in the exercise of its newsgathering function. For over twenty years, a Department regulation (28 C.F.R. 50.10) has prohibited Department employees from questioning members of the media, or from issuing subpoenas to, or for the telephone toll records of, members of the media without the specific approval of the Attorney General. In practice, we have almost never issued subpoenas to reporters or used sensitive investigative techniques, such as physical or electronic surveillance or pen-registers, to investigate their contacts. Although one can reasonably argue that reporters are breaking the law by receiving and publishing classified information, both Democratic and Republican Administrations have sought to avoid the constitutional and public policy questions that would be posed by subjecting the media to compulsory process

or using sensitive techniques against members of the media.

However, this does not mean that such means are never justified in balancing national security interests against the interests of the press.

Given that we focus our investigations on the pool of people who had access to the leaked information, rather than the single reporter who received and published it, identifying leakers is an extremely difficult task. FBI investigators work very hard on these investigations, often conducting hundreds of interviews. Almost inevitably, we find that the universe of individuals with authorized access to the disclosed information is so large as to render impracticable further efforts to identify the leaker. Even in cases in which we are initially told that a particular sensitive report was distributed to only a handful of senior Cabinet officials and Members of Congress, we inevitably find that, because of the busy schedule of the senior official or for other reasons, the report was in fact distributed to dozens of members of their staffs. This problem has increased as more and more information becomes accessible through shared computer databases such as Intelink.

Moreover, leak investigations are complicated by the fact that, unlike most other crimes, there are usually no witnesses and there is usually no forensic evidence. The leak usually involves only two people - the government official and the reporter - and is usually done orally and in person.

Because of the enormous difficulty of conducting leak investigations, almost all leak investigations are closed without our having identified a suspect. Of course, investigators and prosecutors may have their suspicions, but a prosecutor cannot bring criminal charges unless he or she believes that he can prove beyond a reasonable doubt that the defendant committed the crime.

I know that both the Intelligence Community and this Committee are concerned by the fact that more people have not been prosecuted for media leaks. Indeed, it is true that the last prosecution we brought was in 1985. I find this dearth of prosecutions highly frustrating as well. Certain government officials are getting away with very serious violations of law. But the sad fact is that in the vast majority of leak cases, including all the most damaging leaks regarding intelligence

capabilities, we simply have not been able to identify the people responsible.

To be sure, there have been a handful of cases where the Department has declined to prosecute even though the leaker had been identified, even from the start. I understand that my staff has discussed with Committee staff our reasons for declining prosecution in each of these cases. In general, either the intelligence agency did not believe that the disclosure was of sufficient gravity to warrant a criminal investigation or we decided not to prosecute because we concluded that we could not convince a jury beyond a reasonable doubt that the person had committed every element of the offense or that a jury would likely refuse to convict notwithstanding the evidence.

You also asked me to address the adequacy of the criminal statutes currently available to us to prosecute leaks. As you know, there is no general criminal statute penalizing the unauthorized disclosure of "classified information." Nevertheless, we believe that the criminal statutes currently on the books are adequate to allow us to prosecute almost all leak cases. We have never been forced to decline a prosecution solely because the criminal statutes were not broad enough. Several

statutes address conduct, including disclosure, with respect to certain categories of information such as classified information concerning the communication activities of the United States (18 U.S.C. §798) and Restricted Data relating to atomic weapons or energy (22 U.S.C. §§2274, 2277). Of more general application are two provisions of the Espionage Act, subsections (d) and (e) of 18 U.S.C. §793. They make it a crime punishable by 10 years' imprisonment for an authorized or unauthorized possessor of documents or information "relating to the national defense" to "wilfully communicate" the same to "any person not entitled to receive it." The term "relating to the national defense" is a term of art requiring the government to prove that the documents or information were closely held and that, in the words of the Supreme Court in Gorin v. United States, "refer to the military and naval establishments and the related activities of national preparedness." In 1985, in U.S. v. Morison, we successfully prosecuted a Naval intelligence official under sections 793(d) and (e) for providing copies of classified satellite photographs to Jane's Defence Weekly.

I should add that we would make full use of the Classified Information Procedures Act in a leak prosecution, much as we would in an espionage case. This would include the entry of a

protective order under Section 3 of the Act, application to the court for limitations on discovery as necessary under Section 4, notice by the defendant of the classified information he intends disclose under Section 5, and a hearing to determine the use or admissibility of classified information at trial under Section 6. CIPA has been an extremely valuable tool in the prosecution of an increasing number of Federal crimes implicating national security issues and classified information. We must recognize, however, and the agency which "owns" the leaked information must be prepared to accept that a leak prosecution will inevitably confirm the accuracy of the information and its importance and would also likely lead to additional disclosures of classified information as a result of intense media coverage.

I have reviewed Section 303 of the FY2001 Intelligence Authorization Act, which this Committee reported earlier this month. Section 303 would add a new Section 798A to Title 18, which would prohibit certain current or former government officials or other persons with access to classified information from knowingly or willfully disclosing any classified information to a person who is not a U.S. government official and who does not have authorized access to the information. Although we appreciate this Committee's interest in creating a more

generalized leak statute, we believe that this provision should not be enacted as currently drafted. We can provide you with our precise comments, but in general we believe that this provision might criminalize inadvertent disclosures, such as to a person who did not have the correct clearance level. We also believe that a generalized unauthorized disclosure statute should include an exception to allow U.S. officials with authority to do so to disclose classified information to foreign persons or agents, such as in the course of authorized diplomatic or intelligence activities.

While we are prepared to prosecute vigorously those who are responsible for leaks of classified information, and I believe that a successful leak prosecution would be very helpful in our continuing efforts to deter leaks, I also want to say that the Department of Justice believes that criminal prosecution is not the most effective way to address the leak problem. I would note that this was also one of the principal conclusions of the so-called "Willard Report," the interagency group commissioned by then Attorney General William French Smith in 1982 to review the problems of media leaks. In addition to the difficulties of identifying leakers, bringing leak prosecutions is highly complex, requiring overcoming defenses such as apparent

authority, improper classification, and First Amendment concerns, and prosecutions are likely to result in more leaks in the course of litigation. While we certainly agree that government officials who intentionally leak classified information should be criminally prosecuted where the requisite criminal intent can be established, in general we believe that the better way to address the problem of leaks is to try to prevent them through stricter personnel security practices, including prohibitions on unauthorized contacts with the press, regular security reminders, and through administrative sanctions, such as revocation of clearances. It is much easier for a department or agency to strip the clearances from a government official suspected of leaking than to bring a successful criminal prosecution against him or her.

The Department of Justice's Civil Division is also fully committed to pursuing appropriate civil actions for injunctive relief or monetary remedies against government officials who violate their secrecy agreements or who make financial profits from unauthorized disclosures of classified information. We are also prepared to support other Departments or agencies who take administrative actions, such as withdrawal of security

clearances, against officials who are determined to have made unauthorized disclosures.

Finally, I want to say that the Department is constantly looking for better ways to handle media leaks. Several years ago, I asked the Criminal Division to conduct a comprehensive review of our procedures for investigating and prosecuting leaks and to review all past efforts. Based on this review, we have taken a number of actions to try to improve our investigations and to be more pro-active. For example, we have been working with the intelligence agencies to devise methods to help narrow the pool of suspects. We have asked intelligence agencies to identify those leaks that are most damaging so that we can concentrate our investigative resources on those cases. And we have asked the FBI to analyze patterns in leaks and to treat certain leaks as part of a continuing investigation, rather than waiting for individual crime reports.

In closing, I want to re-emphasize that we share the frustration and dismay of the Intelligence Community and the Congress about the damage that is being done to our national security by leaks of highly classified information, and our apparent inability to identify and sanction those who are

responsible. As I have noted, some of these leaks of classified information have had a direct impact on the Department of Justice as well. I appreciate the Committee's interest in this subject, and the Department is prepared to work with you to develop additional initiatives to address this difficult problem. I am now prepared to answer any questions you may have.