The Willard Report

REPORT OF THE INTERDEPARTMENTAL GROUP ON UNAUTHORIZED DISCLOSURES OF CLASSIFIED INFORMATION--MARCH 31, 1982

(reprinted from House Committee on the Judiciary, Subcommittee on Civil and Constitutional Rights, hearings on "Presidential directive on the use of polygraphs and prepublication review," Ninety-eighth Congress, April 21, 28, 1983, and February 7, 1984, Published 1985, Appendix pp. 166-180.)

Chairman.-Richard K. Willard, Deputy Assistant Attorney General, Department of ,Justice. Members: Daniel W. McGovern, Deputy Legal Adviser, Department of State; Jordan Luke, Assistant General Counsel, Department of the Treasury; Kathleen A. Buck, Assistant General Counsel; L. Britt Snider, Director for Counterintelligence and Security Policy, Department of Defense, James W. Culpepper, Deputy Assistant Secretary for Security Affairs, Department of Energy, and Ernest Mayerfeld, Deputy General Counsel, Central Intelligence Agency.

EXECUTIVE SUMMARY

Unauthorized disclosure of classified information is a longstanding problem that has increased in severity over the past decade. This problem has resisted efforts at solution under a number of Administrations. Yet the protection of national security information remains a fundamental constitutional duty of the President. The continuing large number of unauthorized disclosures has damaged the national security interests of the United. States and has raised serious questions about the government's ability to protect its most sensitive secrets from disclosure in the media. We must seek more effective means to prevent, deter, and punish unauthorized disclosures. At the same time, we must recognize that this complex problem is unlikely to be solved easily or quickly.

The scope of this report is limited to unauthorized disclosures of classified information where there is no apparent involvement of a foreign power. Such disclosures primarily occur through media "leaks" by anonymous government employees, or in publications and statements by former employees. Beyond the scope of this report are the following kinds of disclosures: Clandestine disclosures of classified information to foreign powers or their agents, which is espionage in the classic sense; authorized disclosures of classified information by government officials who are not publicly identified; leaks of unclassified information; and compromise of classified information through negligence. Although the foregoing kinds of disclosures also present serious problems, we have limited the scope of this report in order to produce a more comprehensible set of recommendations.

It should be noted that some high ranking officials erroneously believe they have the authority to leak classified information in furtherance of government policy. Such disclosures may only be made by persons with declassification authority under Executive Order 12065 or otherwise from the President. Without such authority, "friendly" leaks are just as unlawful as any other unauthorized disclosure of classified information.

LAWS PERTAINING TO UNAUTHORIZED DISCLOSURES

The unauthorized disclosure of classified information has been specifically prohibited by a series of Executive orders (1) dating back at least to 1951. Such disclosures also violate (2) numerous more general standards of conduct for government employees based on statutes and regulations. It is clear that any government employee may be discharged or otherwise disciplined for making unauthorized disclosures of classified information. Moreover, in virtually all cases the unauthorized disclosure of classified information potentially violates one or more federal (3) criminal statutes.

However, there is no single statute that makes it a crime as such for a government employee to disclose classified information without authorization. With the exception of certain specialized categories of information, the government must ordinarily seek to prosecute unauthorized disclosures as violations of the Espionage Act or as the theft of government property. Such prosecutions have not been undertaken because of a variety of legal and practical problems.

Therefore, it would be helpful if Congress enacted a law providing criminal penalties for government employees who, without authorization, disclosure information that is properly classified pursuant to statute or Executive order. Such a law would be appropriate in view of the substantial body of criminal statutes punishing unauthorized disclosure of other kinds of sensitive information by government employees, such as banking, agricultural and census data. Classified national security information deserves at least the same degree of protection.

A promising development in recent years has been the judicial recognition that the government may enforce secrecy agreements through civil litigation. Many government employees sign secrecy agreements as a condition of employment with intelligence agencies or to obtain access to classified information. In a series of cases culminating in the Supreme Court's 1980 decision in United States v. Snepp, the Justice Department has obtained injunctions and monetary remedies from individuals who seek to publish classified information in violation of their secrecy obligations. Such civil litigation avoids many of the procedural problems that would he encountered in criminal prosecutions. The effectiveness of this program would be increased by greater use of properly drafted secrecy agreements.

PROTECTIVE SECURITY PROGRAMS

The overall effectiveness of the government's programs for safeguarding classified information undoubtedly affects the frequency of leaks. Tight security measures-¬including limiting access to classified information to those with a real "need to know" - reduce the opportunities for unauthorized disclosure. By contrast, lax security measures may encourage leaks by causing employees to believe that classified information does not really require protection.

As a general rule, protective security programs serve a number of objectives besides prevention of unauthorized disclosures, and therefore this report does not consider these programs in great detai1. The following observations are made:
Greater emphasis should be given to security education programs for senior officials;
Better controls on copying and circulation of classified documents would reduce dissemination and aid the task of investigating leaks; and
The federal personnel security program under E.O. 10450 and implementing regulations should be revised and updated.

We also considered whether there should be a government-wide program to regulate contacts with media representatives by government officials with access to classified information. Such contacts, especially when they occur on a frequent and informal basis, may give rise to deliberate as well as negligent disclosures of classified information. However, the operational considerations among the agencies vary greatly. Therefore, each agency should be required to develop its own policy regarding contacts between journalists and employees who have access to classified information.

PAST EXPERIENCES WITH LEAK INVESTIGATIONS

Leaks are extremely difficult to investigate because they involve a consensual transaction. Both the leaking official and the receiving journalist have a strong incentive to conceal the source of the information.

Leak investigations do not focus on the receiving journalist for a variety of reasons. Rarely is there sufficient probable cause to justify a search or electronic surveillance of the journalist. The use of some kinds of investigative techniques may raise First Amendment concerns to which we should be sensitive. Finally, journalists are unlikely to divulge their sources in response to a subpoena for documents or testimony before a grand jury, and contempt sanctions against journalists in other types of cases have not been effective.

Therefore, leak investigations generally focus on government employees who have had access to the information that is leaked. In most situations, hundreds or thousands of employees have had access to the information, and there is no practical way to narrow the focus of the inquiry. Also, the leaking official is unlikely to confess his offense in response to a simple inquiry. The polygraph can be an effective tool in eliciting confessions, but existing regulations do not permit compulsory use of the polygraph for many employees.

Leaks of classified information constitute a potential violation of the espionage laws and other statutes that fall within the FBI's investigative jurisdiction. (By contrast, many agencies that originate classified information are not authorized to go beyond their own employees in investigating leaks.) However, FBI has been reluctant to devote its resources to leak investigations. The burden of such investigations falls almost entirely on the Washington Field Office. Such investigations frequently involve high ranking

government officials, who may be uncooperative. Sometimes a time-consuming investigation is undertaken, only to reveal that the source of the leak was a White House or Cabinet official who was authorized to disclose the information. Finally, it is very rare for an investigation to identify the leaking official, and even rarer that a prosecutable case is developed or that administrative action is taken against a leaker.

The Criminal Division of the Justice Department has developed the practice of screening leak cases before referral to FBI, for the purpose of eliminating those that are unlikely to lead to criminal prosecution. This practice involves the frequently criticized "eleven questions" that agencies are expected to answer when they report leaks to the Criminal Division and that include an advance commitment to provide and declassify such classified information as may be required to support a prosecution.

In summary, the past approach to leak investigations has been almost totally unsuccessful and frustrating to all concerned. There have been frequent disputes between the Justice Department and agencies complaining about leaks. This ineffectual system has led to the belief that nothing can be done to stop leaks of classified information.

PROPOSED NEW APPROACH TO LEAK INVESTIGATIONS

Unless new criminal legislation is enacted, we should recognize that leak investigations are unlikely to lead to successful criminal prosecutions. However, the present system would be greatly improved if employees who leak classified information could be identified and fired from their jobs. Therefore, we should recognize that the likely result of a successful leak investigation will be the imposition of administrative sanctions except for cases in which exacerbating factors suggest that criminal prosecution should be considered.

We should also recognize that resources are available to investigate only a small fraction of leaks. All leaks should be evaluated in light of criteria developed through consultation between the Justice Department and affected agencies. These criteria would include: the level of classified information disclosed; the resulting damage to national security; the extent to which the information had been disseminated at the time it was leaked; and the presence of specific "leads" to narrow the focus of investigation.

Agencies should be encouraged to conduct more extensive preliminary investigations before referring leaks to the Department of Justice for investigation. Affected agencies should be consulted by the Department of Justice in determining which leak cases warrant investigative priority. A decision to undertake criminal prosecution would not be required as a prerequisite to FBI investigation. FBI should be specifically authorized to investigate unauthorized disclosures that potentially violate federal criminal law, even though administrative sanctions may be sought instead of criminal prosecution.

The polygraph is an investigative technique occasionally used in leak investigations. By regulation, most federal agencies are not permitted to take adverse actions against

employees who refuse to be polygraphed. However, there is no constitutional or statutory bar to requiring federal employees to take a polygraph examination as part of an investigation of unauthorized disclosures of classified information. We recommend that existing regulations be changed to permit greater use of the polygraph in leak investigations.

Use of the polygraph is a controversial technique, but security specialists believe it can be effective in situations where a leak investigation turns a limited number of suspects. Under this approach the polygraph is used sparingly and as a last resort. Such polygraph examinations can be limited to the circumstances of the disclosure being investigated, and need not involve questions of a personal nature that some employees find offensive.

Finally, when investigations identify employees who have disclosed classified information without authority, they should not be let off with a slap on the wrist. The full range of administrative sanctions--including discharge--is available. Most employees have certain procedural rights, including notice, hearing and administrative appeal. However, an agency head who follows proper procedures should have no difficulty in disciplining or discharging leakers. It would be helpful for the Merit Systems Protection Board and other administrative bodies to adopt "graymail"-type procedures to protect classified information that may be involved in such situations.

SUMMARY OF RECOMMENDATIONS

1. The Administration should support new legislation to strengthen existing criminal statutes that prohibit the unauthorized disclosure of classified information.
2. All persons with authorized access to classified information should be required to sign secrecy agreements in a form enforceable in civil actions brought by the United States. Far persons with access to the most sensitive kinds of classified information, these agreements should also include provisions for prepublication review.
3. Agencies should adapt appropriate policies to govern contacts between media representatives and government officials, so as to reduce the opportunity for negligent or deliberate disclosures of classified information.
4. Each agency that originates or stores classified information should adopt internal procedures to ensure that unauthorized disclosures of classified information are effectively investigated and appropriate sanctions imposed for violations.
5. The Department of Justice, in consultation with affected agencies, should continue to determine whether FBI investigation of an unauthorized disclosure is warranted. The FBI should be permitted to investigate unauthorized disclosure of classified information under circumstances where the likely result of a successful investigation will be imposition of administrative sanctions rather than criminal prosecution.
6. Existing agency regulations should be modified to permit the use of polygraph examinations for government employees under carefully defined circumstances.
7. All agencies should be encouraged to place greater emphasis on protective security programs. Authorities for the federal personnel security program should be revised and updated.

THE WILLARD REPORT

REPORT OF THE INTERDEPARTMENTAL GROUP ON UNAUTHORIZED DISCLOSURES OF CLASSIFIED INFORMATION--MARCH 31, 1982

NATURE OF THE PROBLEM AND SCOPE OF REPORT

Unauthorized disclosure of classified information has become an increasingly common occurrence. It is not a new phenomenon, but its severity has increased greatly over the past decade. The theft of the "Pentagon Papers" and their publication by the New York Times in 1971 ushered in an era of heightened media interest in the exposure of classified information. Many of these disclosures occurred in the context of revealing improper government activities. After a time, however, disclosures continued while revealing no wrongdoing. Indeed, a few journalists seem to believe that quoting from "highly classified" documents is an appropriate means of entertaining, as well as informing the public. Today the unauthorized publication of classified information is a routine daily occurrence in the United States.

The harm caused by these frequent unauthorized disclosures is manifold. Particular items of information appearing in the press provide valuable intelligence for our adversaries concerning the capabilities and plans of the United States for national defense and foreign relations.

Unauthorized disclosures interfere with the ability of our government effectively to carry out its policies. This "veto by leak" phenomenon permits a single bureaucrat to thwart the ability of our democratic system of government to function properly.

Disclosures about US intelligence programs are particularly damaging, because they may causes sources to dry up. Lives of human agents are endangered and ex pensive technical systems become subject to countermeasures.

In particular, foreign governments are reluctant to cooperate with the United States because we are unable to protect confidential information or relationships.

This report has been kept unclassified, and as a result specific examples of harmful unauthorized disclosures have not been included. Such examples can be provided separately.

The scope of this report is limited to unauthorized disclosures of classified information where there is no apparent involvement of a foreign power. Such disclosures primarily occur through "leaks" by anonymous government officials to the media, or in publications or statements of former officials.

Officials who make unauthorized disclosures may persuade themselves that they are serving the larger national interest by disclosing information that the public has a right to know. Such officials may seek to advance their personal policy objectives by leaks of

classified information, on the assumption that there will be no serious harm to national security. Because leaks are so prevalent and leakers rarely caught, some officials may believe there is nothing wrong with leaking classified information and that everyone does it.

Similarly, many journalists appear to believe they have a duty to divulge virtually any newsworthy secret information that can be acquired by whatever means they choose to employ. To their way of thinking, leaks are part of a game in which the government tries to keep information secret and the media tries to find it out. Some journalists are unwilling to assume responsibility for damage to the national security in situations where they win this "game."

Under these circumstances, only a fundamental change in prevailing attitudes will alleviate the problem of unauthorized disclosures. We must seek to develop a sense of discipline and self-restraint by those who work with or obtain classified information. This goal will not be achieved easily or quickly. But without a change in attitudes, no program to deal with unauthorized disclosures can possibly be effective.

Certain kinds of disclosures are beyond the scope of this report, but should be described briefly for purposes of comparison.

1. Classic espionage.-Clandestine disclosures of classified information to foreign powers or their agents is espionage in the classic sense. Investigating such matters is primarily the responsibility of FBI's foreign counterintelligence program. The threat in this area is increasing because of the increasing number of known or suspected hostile intelligence agents in the United States. President Reagan's recent Executive Order 12333 and new implementing guidelines will strengthen FBI's ability to deal with this serious problem.

2. Authorized disclosures.-High ranking officials often believe they are authorized to disclose otherwise classified information to the press in furtherance of government policies. Since the c1assification system is established on the authority of the President, he certainly has the power to authorize disclosures that amount to a de facto declassification of such information. However, only the President can authorize the declassification of information other than as provided in Executive Order 12065. A high ranking official who discloses classified information without authorization under that Executive Order or otherwise from the President violates the law. Such disclosures should be investigated and penalized in the same manner as other unauthorized disclosures of classified information. Applying a double standard that overlooks "friendly" leaks of classified information breeds disrespect for the law and can undermine the effectiveness of any enforcement program.

3. Unclassified leaks.-Some of the most embarrassing leaks do not involve classified information at all. We believe that leaks of classified information cause more serious and long-lasting damage, and thus warrant separate treatment as provided in this report. That is not to say that nothing can or should be done about leaks of unclassified information. The government is entitled to protect a variety of information from disclosure, including

law enforcement investigatory information, proprietary data, pre-decisional memoranda and other information pertaining to internal government deliberations. Depending upon the circumstances, disclosure of such information may be unlawful, unethical, or a violation of applicable standards of conduct for government employees.

4. Negligent disclosures.-The compromise of classified information through negligence violates regulations and, depending upon the circumstances, may constitute a criminal offense. Such disclosures involve sufficiently different causes and considerations as to fall beyond the scope of this report. It is worth noting, however, that many of the apparent media leaks involve inadvertent disclosures. High ranking officials are particularly susceptible to such disclosures because they have access to a large volume of sensitive classified information and are required to deal with the press on a frequent basis. The compromise of classified information would be reduced if officials would exercise greater care in their dealings with media representatives.

LAWS PERTAINING TO UNAUTHORIZED DISCLOSURES

1. Executive orders

The protection of national security information is a fundamental constitutional responsibility of the President. This responsibility is derived from the President's powers as Chief Executive, Commander-in-Chief, and the principal instrument of United States foreign policy. The courts have recognized the constitutional dimension of this responsibility. Chicago & Southern Air Lines, Inc. v. Waterman Steamship Corp., 333 V.S. 103, 111 (1~l48); United States v. Curtiss- Wright Export Corp., 299) U.S. 304, 320 (1936}; United States v. Marchetti, 466 F.2d 1309, 1315 (4th Circ), cert. denied, 409 U.S. 1063 (1972).

In a number of civil and criminal statutes, Congress has also recognized the President's authority to safeguard national security information by adopting Executive orders providing for a system of classification, e.g., 5 U.S.C. 552b(l) (Freedom of Information Act); 5 U.S.C. 552b(c)(1) (Government in the Sunshine Act); 5 U.S.C. 2302(b)(8)(A) (Whistleblower Statute); 18 U.S.C. 798; 50 U.S.C. 783{b).

In a series of Executive Orders dating back at least to 1951, Presidents have provided for a system of classification to safeguard national security information. Since these Executive Orders are issued in fulfillment of the President's constitutional responsibilities, they have the force and effect of law.

The present Executive Order on National Security Information, Executive Order 12065, prohibits the unauthorized disclosure of classified information. It provides that officers and employees of the government shall be subject to appropriate administrative sanctions if they knowingly, willfully and without authorization disclose properly classified information or compromise such information through negligence. Sanctions may include termination of classification authority, reprimand, suspension and removal.

The new draft executive order on national security information provides for similar prohibitions and sanctions and applies to government contractors, licensees and grantees as well as government officers and employees.

2. Criminal statutes

In analyzing whether an unauthorized disclosure of classified information constitutes a criminal violation, it is necessary to consider three categories of criminal statutes: (a) those explicitly prohibiting the disclosure of "classified information"; (b) the so-called "espionage" laws, which prohibit the disclosure of "national defense" information; and (c) the stat ate prohibiting theft of government property.

(a) Classified information statutes.-There is no general criminal penalty for the unauthorized disclosure of "classified information" as such; however, several criminal statutes prohibit unauthorized disclosure of classified information in particular situations. Section 783(b) of Title 50 prohibits government employees from disclosing any classified information to agents of foreign governments or members of communist organizations. It is unlikely that this statute would be construed to apply to unauthorized disclosures of classified information to the media, even though the information could find its way into the hands of an agent of a foreign government or a member of a communist organization as a consequence of its publication.

Section 2277 of Title 42 prohibits government employees and contractors from knowingly communicating "Restricted Data" to any person not authorized to receive such information. "Restricted Data" constitutes classified information concerning atomic weapons and nuclear material. Section 2274 of Title 42 prohibits anyone having possession, access or control over Restricted Data from disclosing it with the intent or reason to believe it will be used to injure the United States or secure an advantage to a foreign nation.

In addition to these provisions" 18 U.S.C. 798 prohibits any person from disclosing to any unauthorized person "classified information" concerning communications intelligence and cryptographic activities.

These three sets of provisions are the only criminal statutes that punish the unauthorized disclosure of "classified information" as such.

(b) Espionage laws.--Certain provisions of the espionage laws may also be violated by unauthorized disclosures of sensitive information. The two provisions that would most likely be violated by an unauthorized disclosure of classified information to the media would be 18 U.S.C. 793(d) and (e). Section 793(d) prohibits any person having authorized possession of materials such as documents or photographs "relating to the national defense" or "information" relating to the national defense, if there is "reason to believe" that this information can be used "to the injury of the United States or to the advantage of any foreign nation," from transmitting such materials or information to "any

person not entitled to receive it." Similarly, section 793(e) prohibits any person having unauthorized possession or access to such materials or information from transmitting them to other unauthorized persons or failing to deliver them to an authorized government officer or employee.

These provisions have not been used in the past to prosecute unauthorized disclosures of classified information, and their application to such cases is not entirely clear. However, the Department of Justice has taken the position that these statutes would be violated by the unauthorized disclosure to a member of the media of classified documents or information relating to the national defense, although intent to injure the United States or benefit a foreign nation would have to be present where the disclosure is of "information" rather than documents or other tangible materials. These laws could also be used to prosecute a. journalist who knowingly receives and publishes classified documents or information.

One category of classified information that would probably not be covered by these provisions is information that could not fairly be characterized as "relating to the national defense. In Gorin v. United States, 312 U.S. 19, 28 (1940), the Supreme Court stated that in the context of this statute "national defense" is "a generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness." Currently information may be classified under Executive Order 12065 if it relates either to "the national defense" or to "the foreign relations" of the United States. Because the term "national defense" was so broadly defined in Gorin, it is likely to cover most information relating to "foreign relations" that is properly classified. However, it is possible that the two terms do not overlap completely, and if so, only the disclosure of information relating to the national defense would be covered by sections 793(d) or (e).

(c) Theft of Government property.-18 U.S.C. 641 provides criminal penalties for the unauthorized sale or disposal of "any record, voucher, money, or thing of value of the United States," or the knowing receipt of the same "with intent to convert it to his use or gain." Convictions under this statute have been upheld in cases where government documents or information have been taken. United States v. Friedman, 445 F.2d 1076 (9th Cir.), cert. denied, 404 U.S. 958 (1971) (conviction for receipt of copy of secret grand jury transcript); United States v. Lambert, 601 F.2d 69 (2d cir. 1979), cert. denied, 444 U.S. 871 (1979) (convictions for selling information derived from Drug Enforcement Administration computer).

There has been no definitive court test of the applicability of section 641 to unauthorized disclosures of classified information.[Compare United States v. Truong, 629 F.2d 908, 927 (4th Cir. 1980) with id. at 532; see United States v. Boyce. 594 F.2d 1246, 1252 (9th Cir.), cert. denied, 444 U.S. 855 (1979).] The Department of Justice has taken the position that prosecution under this statute would be warranted in cases of unauthorized disclosure of classified information. Of course, the substantive applicability of this statute remains to be established. In addition, many of the procedural barriers to successful criminal prosecution would remain.

(d) Practical barriers to successful prosecution.-Although there are numerous unresolved questions about the substantive applicability of the foregoing criminal statutes, it is clear that most unauthorized disclosures potentially violate one or more of these statutes. Yet the fact remains that no criminal prosecution has been attempted since Daniel Ellsberg and Anthony Russo were indicated for leaking the "Pentagon Papers." (Prosecution in that instance was dropped because of governmental misconduct in investigating the case.) One problem is that leak cases are hard to solve. But even when a suspect is identified, there are numerous practical barriers to criminal prosecution. These barriers may be summarized as follows.

First, criminal prosecution serves to confirm the accuracy and sensitivity of the information that has been disclosed. For this reason, many agencies do not want cases prosecuted, in order to maintain doubt as to the accuracy of the disclosed information.

Second, criminal prosecution generally requires the Government to prove that the disclosures in question were damaging to national security, which may require further public disclosures of classified information. Such proof is often required under the espionage statutes and, as a practical matter, is extremely helpful in giving any prosecution jury appeal.

Third, criminal trials are normally conducted before a jury and open to the public. Defendants can threaten to require disclosures of sensitive information in the course of trial--the so-called "graymail" problem. The Classified Information Procedures Act of 1980 alleviates this problem to some extent but does not solve it entirely.

In summary, the courts of criminal prosecution in terms of harm to national security are likely in many cases to outweigh the benefits of deterrence and respect for the law. Of course, the availability of criminal sanctions is important and should be considered in appropriate cases. New legislation could reduce the practical barriers to successful prosecution. But the primary focus of the effort to enforce the laws against unauthorized disclosure should involve administrative and other civil remedies.

3. Civil remedies

There is no general statute providing for civil penalties or injunctive relief in cases of disclosure of classified information. The absence of such an authorizing statute was noted by several members of the Supreme Court in the "Pentagon Papers" case. However, it appears that a majority of the Court in that case would have permitted the Government, even absent a statute, to enjoin the disclosure by the media of classified information that threatened "direct, immediate, and irreparable damage to our Nation or its people." New York Times Co. v. United States, 403 U.S. 713, 730 (1971) (Stewart, J., concurring). As applied in the Pentagon Papers case, this is an extremely difficult standard to meet. It is not clear that, as a practical matter, the First Amendment would permit a statute authorizing injunctions against the media under a significantly lower standard.

There are specific statutes providing civil remedies for unauthorized disclosure of atomic energy information. 42 U.S.C. 2167, 2168, and 2280. The latter statute was successfully relied upon in obtaining a district court injunction against disclosure of H-bomb information. United States v. Progressive, Inc., 467 F. Supp. 990 (W.D. Wis. 1979), appeal dismissed, 610 F.2d 819 (7th Cir. 1979).

Government employees who engage in unauthorized disclosures of classified information are subject to discipline or discharge for misconduct pursuant to 5 U.S.C. 7513 or equivalent statutes governing specialized employment systems. Applicable standards of conduct are found in Executive Order 12605 and implementing agency regulations prohibiting unauthorized disclosure of classified information, as well as the criminal statutes discussed previously. In addition, unauthorized disclosure of classified information would violate a number of general standards of conduct for government employees. See, e.g., 5 C.F.R. 735.201a(c) (impeding government efficiency); id. 735.201a(e) (making a government decision outside official channels); id. 735.201a(f) (affecting adversely the confidence of the public in the integrity of the government); id. 735.206 (misuse of information not made available to the general public); id. 735.209 (conduct prejudicial to the government).

In addition to the normal administrative sanctions for misconduct, 5 U.S.C. 7532 provides for suspension or removal of certain employees if such action is found to be "necessary in the interest of national security." This statute is implemented in Executive Order 10450 and various agency regulations. These authorities are part of the federal personnel security program and are designed to ensure that persons who are "security risks" do not serve in sensitive positions.

Executive Order 10450 was promulgated in 1953 and seriously needs revision to take into account subsequent court decisions and changes in government organization. These shortcomings do not prevent the government from disciplining or discharging employees for unauthorized disclosure of classified information, since such disclosures constitute misconduct for which normal administrative sanctions are available. However, revision of Executive Order 10450 would be helpful in streamlining the authority of agencies to revoke security clearances and take other personnel actions in the interest of national security.

In addition to standards imposed by regulation, many present and former government employees are bound by contractual or fiduciary obligations not to disclose classified information in an unauthorized manner. The Department of Justice has had considerable success in enforcing such obligations in civil litigation against former government employees. Since such persons no longer work for the government, the possibility of administrative sanctions is not a deterrent to their making unauthorized disclosures.

Nondisclosure agreements typically have one or both of the following key provisions. First, the employee agrees never to disclose classified information to an unauthorized person. Second, the employee promises not to publish any material related to classified activities without the express prior approval of the agency. This second provision is

implemented through a mechanism far prepublication review of manuscripts submitted by present or former employees for deletion of classified information.

Key judicial decisions have held that the government is entitled to an injunction against former employees who seek to publish without obtaining clearance pursuant to their obligations to comply with prepublication review programs. Once an agency conducts such prepublication review, it is entitled to deleted classified information subject to judicial review under the same general standards as applied in litigation under the Freedom of Information Act. Finally, a person who publishes in violation of his prepublication review obligations forfeits the right to any profits from his publication, which can be impressed with a constructive trust for the benefit of the Government. United States v. Snepp, 444 U.S. 507 (1980); Knopf v. Colby, 50:9 F2d 1362 4th Cir.), cert. denied. 421 US. 992 (1975); United States v. Marchetti, 466 F.2d 1309 (4th Cir.), cert. denied, 409 U.S. 1063 (1972). In addition, persons who violate injunctions to comply with nondisclosure obligations risk sanctions for contempt of court, which can include both civil and criminal penalties.

The present policy of the Justice Department, as stated by Attorney General Smith on September 3, 1981, is vigorous and even-handed enforcement of nondisclosure obligations under the Snepp guidelines. This policy statement revoked guidelines issued under the Carter Administration that suggested the Snepp doctrine would be invoked only under limited circumstances.

The availability of civil remedies under the Snepp doctrine suggests that greater attention should be paid to the use of nondisclosure agreements for persons with authorized access to classified information. At a minimum, all such persons should be required to agree never to disclose classified information without authorization. In addition, persons with access to the most sensitive kinds of classified information should be required to agree to a system of prepublication review.

4. Recommendations for new legislation

As indicated above, criminal sanctions for unauthorized disclosure of classified information as such apply only in limited situations involving information concerning the national defense, nuclear weapons and materials, and communications and cryptographic intelligence. Moreover, there are a number of substantive and procedural barriers to successful criminal prosecution in most cases of unauthorized disclosures to members of the media.

To close the gaps in the present law, we recommend the introduction of legislation imposing a criminal penalty for all unauthorized disclosures of classified information by government employees. Such a statute should be simple and general in order to cover all situations, and might provide as follows:

Whoever, being an officer or employee of the United States or a person with authorized access to classified information, willfully discloses, or attempts to disclose, any classified

information to a person who is not an officer or employee of the United States and who is not authorized to receive it shall be fined not more than $10,000, or imprisoned not more than three years, or both.

In addition, there should be appropriate definitions of the terms employed. It would be helpful to have a specific procedure for establishing that information forming the basis for prosecution was in fact properly classified, which does not require public disclosure of additional classified information. A similar statutory provision could be drawn to apply to former employees who disclose classified information.

An alternative approach to filling the legislative gap would be to amend 18 U.S.C. 641 to make it clear that classified information is a "thing of value" subject to the penalties of that statute.

Enactment of these or similar provisions would clarify current criminal prohibitions, close the loopholes in these statutes, and give notice that all unauthorized disclosures of classified information are sufficiently serious to warrant criminal sanctions. They would also alleviate-but not solve entirely-certain of the practical problems likely to be presented in criminal prosecutions.

Present civil statutes and regulations permitting disciplinary action for unauthorized disclosures by government employees are generally adequate, except that they apply only to persons who disclose classified information, not to those who receive it. A person who solicits and receives classified information may be no less responsible for an unauthorized disclosure of such information than the government employee who transmits it, but his conduct is not prohibited by any civil statute. Although we make no recommendation with respect to introduction of legislation providing for civil penalties or other remedies against persons who receive classified information, we believe the subject merits further study as an effective, though probably controversial, method of deterring unauthorized disclosures.

PROTECTIVE SECURITY PROGRAMS

Careful attention to the fundamental elements of a sound security program will undoubtedly discourage leaks--and have a number of other beneficial effects on the safeguarding of national security information. Among these elements are the following: Security clearances should be given only to individuals who have been determined to be trustworthy on the basis of adequate background information.

National security information should be clearly identified with the proper classification and stored in a physically secure manner.

Access to classified information should be given only to persons with the proper clearances and requisite "need to know."

These principles seem obvious-and yet they are frequently ignored in many government agencies. Violations of these rules is often most common at the highest levels of government.

To be sure, adherence to these security principles will not stop the deliberate leaker. But disregard for these principles may encourage leaks by causing employees to believe that it is not really important to protect classified information. Good security practices constantly remind people who handle classified information of their obligations for its safekeeping.

Protective security programs are generally outside the scope of this report. The Security Committee (SECOM) established by the Director of Central Intelligence in DCID 1/11 has responsibility for security programs involving intelligence and intelligence sources and methods. SECOM is composed of the directors of security for all agencies represented on the National Foreign Intelligence Council. In addition, the Information Security Oversight Office (11300) of the General Services Administration has responsibility for the government-wide program of safeguarding national security information under Executive Order 12065. Finally, the Office of Personnel Management is responsible for implementing the federal personnel security program. These organizations deserve support in their efforts to strengthen the government's protective security programs.

Two particular aspects of protective security deserve emphasis because of their impact on the problem of unauthorized disclosures. First, security education programs for senior officials deserve greater emphasis. Such officials are often too busy to receive detailed briefings on proper security procedures, yet they generally have access to the most sensitive kinds of information. In particular, senior officials need to be aware of potential pitfalls of dealing with journalists in areas where classified information is involved. SECOM has produced a security orientation especially designed for senior officials, who should be encouraged to avail themselves of this briefing.

Second, better controls on the copying and circulation of classified documents would reduce unauthorized disclosures by restricting dissemination of classified information. Such controls can also assist in leak investigations by identifying persons who had access to the information that was disclosed. A recent study ("APEX") demonstrated that there are insufficient resources to permit better controls on the tremendous volume of classified information that must be circulated within the government. This problem should be reconsidered in the context of implementing the successor to Executive Order 12065.

Another problem that deserves attention is the federal personnel security program. This program is governed by Executive Order 10450, which was adopted in 1953. The order has not been revised to take into account subsequent court decisions and changes in government organization. The FBI no longer collects information about subversive organizations so as to provide a data base for this program because of uncertainty regarding legal constraints and Attorney General guidelines. Because of these and other shortcomings, the federal personnel security program is largely defunct. It is unlikely that

improvements in this program would reveal persons who are likely to leak classified information to the media, but a better effort would reduce our vulnerability to clandestine infiltration of sensitive positions.

Finally, consideration should be given to rules concerning contacts between media representatives and government officials who have access to classified information. Such contacts-especially when they occur frequently and on an informal basis may lead to neglect or deliberate disclosures. Therefore, programs to regulate media contacts could serve to reduce unauthorized disclosures. Possible approaches would include one or more of the following elements: Requiring prior approval of a senior official before discussing official matters with a journalist; requiring all media contacts to be arranged through the agency's public affairs office; requiring a record to be kept of all media contacts; requiring reports to be prepared describing all matters discussed with journalists; and restricting access of journalists to areas where classified documents are stored and used. It would be difficult to develop a program in this area to apply throughout the government. Each agency has its own particular organizational and functional characteristics. However, each agency should be required to consider this problem and develop a specific program to reduce the opportunities for negligent and deliberate disclosures to the media. We recommend that each agency be directed to promulgate appropriate regulations (if it does not already have them) and ensure that its policy is communicated to all employees with access to classified information.

PAST EXPERIENCES WITH LEAK INVESTIGATIONS

Leaks of classified information to the media over the past twenty years have been so numerous that only a small fraction could be investigated. These investigations have rarely been successful in identifying the sources of such disclosures. In a number of the cases that were solved, no adverse action was taken against the government employee found to have leaked classified information. There has never been a successful criminal prosecution for leaking classified information.

The Government's dismal record in leak investigations has a number of explanations. By their nature, leaks to the media are difficult to investigate. Leaks are consensual transactions in which both parties-the leaking official and the receiving journalist-have a strong incentive to conceal the source of the information. Self-imposed limitations on the use of certain investigative techniques have made the task even more difficult. The development of more productive approaches to leak investigations has been hampered by misunderstandings between the Justice Department and agencies whose information is leaked. We cannot expect to do better in the future without understanding these problems encountered in the past.

Agencies whose classified information is leaked have limited powers to conduct investigations. Since most leaks of classified information potentially violate criminal statutes, leak investigations are viewed as involving a law enforcement function. The National Security Act of 1947 provides that the CIA "shall have no police, subpoena, law-enforcement powers, or internal security functions." [50 U.S.C. 403(d)(3). However,

the Director of Central Intelligence is given specific responsibility for protecting intelligence sources and methods. Id. Therefore, the DCI is appropriately concerned with leaks that endanger intelligence sources and methods.] Similar limitations apply to the military services and the Department of Energy. [18 U.S.C. 1385 (Posse Comitatus Act); 42 U.S.C. 2271(b).] Executive Order 12333, § 1.7(d), requires agencies in the intelligence community to report crimes such as leaks of classified information to the Justice Department. Implementing procedures for this provision limit agency authority to conduct preliminary investigations of such matters generally to interviews of current employees and examination of agency premises. And, as a practical matter, most government agencies do not have the capability to conduct investigations outside their own areas of programmatic responsibility.

CURRENT DEPARTMENT OF JUSTICE POLICY

These legal and practical limitations have caused the burden of leak investigations to fall on the FBI. Current Justice Department policy in this regard dates back to the early 1960's. At that time, the FBI was inundated with numerous requests for investigation regarding possible violations of the espionage laws as they relate to "media leaks" and other mishandling of classified information.

Espionage investigations that have no apparent foreign connection are investigated as "Espionage-X" matters by the FBI. Those investigations regarding the mishandling .of classified information, loss of classified information through negligence, or other violations unrelated to media disclosures, are investigated upon receipt by the FBI. In these types of investigations, the subject is generally known and the scope of investigation limited. Although the Criminal Division is notified at the inception of these investigations and is kept advised of their status, it does not initiate these investigations.

Media leaks, however, pose different problems, require more investigation, and are far more numerous. Current policy regarding media leaks requires that prior to any investigation by the FBI, eleven questions must be answered by the injured agency. These questions are utilized to the Criminal Division to determine which cases should be investigated by the FBI. Such screening is necessary due to the vast amount of media leak investigation requests and the often large number of interviews to be conducted in this type of case. The responses to the eleven questions are also crucial in targeting the early stages of any investigation that is undertaken. These questions can be dissected into three categories.

Questions 1 through 3 pertain to the identification of the article(s) contained in the media and the nature of the classified information contained therein. These questions are:
1. The date and identity of the article or articles disclosing the classified information.
2. Specific statements in the article which are considered classified and whether the data was properly classified.
3. Whether the classified data disclosed is accurate. This information is necessary to determine whether a violation has occurred and to assist the FBI in the investigation, if a violation has occurred.

Responses to questions 4 through 8 serve to identify the sources of the classified information disclosed. These questions are:
4. Whether the data came from a specific document and, if so, the original of the document and the name of the individual responsible for the security of the classified data disclosed.
5. The extent of official dissemination of the data.
6. Whether the data has been the subject of prior official releases.
7. Whether prior clearance for publication or release of the information was sought from proper authorities.
8. Whether the material or portions thereof, or enough background data has been published officially or in the press to make an educated speculation on the matter possible.

Responses to these questions are a prerequisite for FBI investigations in that they furnish initial leads and may give direction toward the person or persons responsible for the disclosure. Some of these questions further assist in determining if a violation has occurred or if the information could have been obtained from some unclassified source or prior publication.

Questions 9 through 11 pertain to the prosecutive future of the investigation.
These questions are:
9. Whether the data can be declassified for the purpose of prosecution and, if so, the name of the person competent to testify concerning the classification.
10. Whether declassification had been decided upon prior to the publication or release of the data.
11. What effect the disclosure of the classified data could have on the national defense.

The responses to these questions are used by the Criminal Division to determine if a successful prosecution can be made, should the perpetrator be identified.

If the responses to the "eleven questions" indicate it is not likely that the perpetrator will be identified due to extensive dissemination of the material and/or that successful prosecution cannot be mounted, the Criminal Division will not request that the FBI conduct an investigation. There is, however, an exception to this policy. The Criminal Division will request an FBI investigation, if, in spite of the responses to the above questions, it can be demonstrated that: (a) the disclosure constitutes a very serious compromise of classified information and it is imperative that the person responsible be identified so as to preclude further disclosures; (b) there is a real possibility that the investigation will be fruitful, e.g., the information had very limited distribution; and (c) the originating agency has not finally decided against declassification for prosecutive purposes.

PROBLEMS WITH THE CURRENT POLICY

Although current Justice Department policy requests that complaints concerning media leak matters be forwarded to the Criminal Division for their review, often the complaint is initially forwarded to the FBI. Also, agencies that report leaks occasionally omit the responses to the eleven questions or furnish incomplete information. This practice causes delay while the Criminal Division corresponds with the agency and requests responses to the eleven questions or more detail regarding the responses that may have been furnished. When the initial complaints are furnished in a complete package, FBI investigation can generally be completed in a reasonable period of time depending on the number of interviews to be conducted and other investigative considerations.

The Criminal Division receives numerous complaints requesting investigation in media leak matters which are never referred to the FBI, based upon the above criteria. If all of these complaints were fully investigated, the manpower used would be substantially higher. Leak investigations are manpower-intensive and the burden falls primarily upon FBI's Washington Field Office. Investigating a larger number of leak cases would necessarily divert FBI s resources from other Important priorities such as foreign counterintelligence and terrorism investigations.

Moreover, a number of legal and policy restrictions limit the ability of FBI to conduct effective leak investigations in cases that are referred. In most cases, the principal "lead" is the published media account of the leaked information. But investigations are generally not permitted to focus on the journalist who published the information. Rarely is there sufficient probable cause to justify use of Fourth Amendment techniques, such as searches or electronic: surveillance. Current Department of Justice regulations strictly limit the circumstances under which journalists can be questioned or subpoenaed, and require express prior approval by the Attorney General in each case. 45 Fed.Reg. 76436 (Nov. 19, 1980), to be codified at 28 CFR 50.10. Current informal policies also preclude physical surveillance of journalists or the use of informants directed at the media in leak cases. Use of these and other investigative techniques is appropriately limited because of First Amendment concerns.

Since FBI cannot investigate journalists who receive the classified information, they must focus on government employees who have had access to the information that has been leaked. Often hundreds or thousands of employees have had access to the information in question. Unless the information received more limited distribution or there are other "leads" that permit narrowing the scope of inquiry, there is no practical means to conduct an investigation.

Even where the inquiry can be limited to a manageable number of employees, FBI has very little ability to conduct a successful investigation. The leaking official is unlikely to confess in response to a simple inquiry. The polygraph can be an effective investigatory technique, but most government employees can be polygraphed only if they volunteer for the examination.

Present policy of the Office of Personnel Management (OPM) sharply limits use of the polygraph for employees in the competitive service. Federal Personnel Manual, chapter

736, appendix D; see memorandum from Llewellyn H. Fischer, Acting Associate General Counsel of OPM, to Lawrence A. Wooby, Security Appraisal Officer of DEA, September 30, 1981. This policy requires, among other things, that employees must voluntarily consent to be polygraphed and that a refusal to consent cannot be made part of their personnel file. Other agencies, including the Department of Defense and Department of State, have similar policies regarding some or all of their employees who would not otherwise be covered by the OPM policy.

Certain intelligence agencies, including NSA (for civilian employees) and CIA, regularly use the polygraph to screen candidates for employment as well as in investigations of employees. Department of Justice policy generally permits use of the polygraph in investigating unauthorized disclosure cases, and an adverse inference may be drawn from an employee's refusal to be examined. FBI policy permits an employee to be discharged for refusing an order from the Director to take a polygraph examination; an adverse inference may be drawn if the employee declines a request to be examined. See Memoranda from Attorney General Civiletti to William H. Webster and Michael E. Shaheen, dated May 4, 1980. See also Memorandum of John M. Harmon, Assistant Attorney General, Office of Legal Counsel, May 1, 1980.

In addition to limitations upon the techniques that can be employed, FBI often finds that high-ranking government officials are uncooperative with leak investigations. FBI does not have the authority to compel government employees to give interviews, sign affidavits, or--even if agency regulations are not a bar--take polygraph examinations. Such compulsion can only be exercised by agency heads who may be reluctant to discipline high-ranking officials who refuse to cooperate with leak investigations.

In summary, past experience with leak investigations has been largely unsuccessful and uniformly frustrating for all concerned. Agencies have been unable to conduct investigations outside their own organizations, and yet Justice has been unwilling to permit FBI to investigate most cases. FBI has been asked to investigate a number of leaks without being permitted to use adequate techniques to solve cases. There have been frequent disputes and misunderstandings. On the rare occasions that leaking officials are identified, they often escape even administrative sanctions. This whole system has been so ineffectual as to perpetuate the notion that the government can do nothing to stop leaks of classified information.

PROPOSED NEW APPROACH TO I~EAK INVESTIGATIONS

We should recognize that the threat of criminal prosecution is so illusory as to constitute no real deterrent to the prospective leaker. A more promising approach involves better efforts to identify leakers and the resolve to impose administrative sanctions. For most government employees, a realistic prospect of being demoted or fired for leaking classified information would serve as a deterrent. An effective administrative enforcement program would also reverse the common perception that the Government is powerless to stop leaks of classified information.

The authority and responsibility of agencies that originate classified information should be clarified. All serious leaks should be evaluated and investigated internally by the agency that originated the information. Agencies should adopt procedures to assure that these steps are taken in a timely manner.

Agencies whose classified information is the subject of an unauthorized disclosure should assume greater responsibility for conducting preliminary investigations. All agencies are authorized to conduct preliminary internal investigations of such matters, including interviews with current employees and contractors and the examination of agency premises. Agencies are also authorized to make inquiries of other agencies to which the information had been disseminated to determine the extent of further dissemination and the present location of the documents in question. Such preliminary investigations at recipient agencies may be conducted either by the recipient agency or by the originating agency with the recipient's consent.

The purposes of such preliminary investigations are: (1) to gather sufficient information for the Justice Department to decide whether FBI investigation is warranted, and (2) to provide the originating agency with data necessary to assist in properly safeguarding classified information. At any point that a preliminary investigation develops information indicating that a particular person is responsible for the unauthorized disclosure, then the matter should be immediately referred to the Department of Justice. Otherwise, unauthorized disclosures should be reported to the Department of Justice only after the preliminary investigation is completed, unless there are exigent circumstances.

Current requirements for reporting unauthorized disclosures, as reflected in the "eleven questions," should be revised so that prosecutive potential is no longer a decisive factor. FBI's authority should be clarified to include investigation of unauthorized disclosures of classified information under circumstances where the likely result of a successful investigation will be imposition of administrative sanctions rather than criminal prosecution. As a consequence, agencies would no longer be required to make a commitment to declassify information at the time of referral.

In consultation with affected agencies, the Department of Justice should develop new standards for reporting and evaluation of unauthorized disclosures for possible investigation by FBI. There is a general consensus that the following basic criteria must be considered: The level of classified information disclosed; the extent of resulting damage to national security; the extent to which the information had been disseminated at the time the disclosure occurred; and the presence of specific "leads" to narrow the focus of investigation.

For example, it would ordinarily be an inappropriate use of FBI's resources to investigate the leak of a "confidential" level document of which thousands of copies had been disseminated throughout the government. Timeliness is also an important factor, as leak investigations are more difficult to conduct when the trail is cold.
.

Even if properly evaluated and screened, there are likely to be too many leaks for FBI to investigate each one. Again in consultation with affected agencies, the Department of Justice must decide on priorities for the use of available FBI resources. Even if cases cannot be investigated, however, the process of reporting and analyzing them can provide a useful data base for developing protective security measures and investigating future leaks.

The foregoing proposals requiring consultations between the Department of Justice and affected agencies should be implemented through an interagency advisory panel. One possibility is to use an existing group such as the Security Committee (SECOM), established by the Director of Central Intelligence. However, the authority of SECOM is limited to the protection of intelligence and intelligence sources and methods. Therefore, a new advisory panel should be established, although SECOM could certainly be included in the new group.

FBI's approach to investigating unauthorized disclosure cases should be reviewed by the Department of Justice in order to remove unnecessary restrictions on the use of certain techniques.

The polygraph can be a useful tool in leak investigations under certain circumstances. It should be used selectively and its results considered within the context of a complete investigation. The polygraph should not be used for dragnet-type screening of a large number of suspects or as a substitute for logical investigation by conventional means. It is most helpful when conventional investigative approaches have identified a small number of individuals, one of whom is fairly certain to be culpable, but there is no other way to resolve the case. A polygraph examination in this situation can be limited to the unauthorized disclosure that is being investigated and should not include questions about life style that many employees would find offensive. Moreover, polygraph results should not be relied upon to the exclusion of other information obtained during an investigation.

There is no constitutional or statutory prohibition on use of the polygraph to investigate unauthorized disclosure of classified information by government employees. An employee may be discharged for refusal to cooperate with an investigation of his fitness for continued employment. See, e.g., 5. C.F.R. 735.201a(c), 735.201a(f) and 735.209; Lefkowitz v. Turley, 414 U.S. 70, 84 (1974). Statements that an employee is compelled to make in this fashion cannot be used as evidence in a criminal prosecution. Garrity. v. New Jersey, 385 U.S. 493 (1967). However, such statements may be used in an administrative proceeding to discipline or discharge the employee. Lefkowitz v. Turley, supra. This authority also supports requiring government employees to submit to polygraph examinations in connection with investigations of unauthorized disclosures. See Memorandum of Larry A. Hammond, Acting Assistant Attorney General, Office of Legal Counsel, February 22, 1980.

OPM and other agencies with more restrictive policies on use of the polygraph should be directed to amend their regulations if necessary to permit adverse consequences to follow an employee's refusal to cooperative with polygraph examinations used to investigate

unauthorized disclosures of classified information. Such polygraph examinations could be limited to the circumstances of the unauthorized disclosure being investigated, and would not include unrelated questions. The employing agency would be permitted to deny security clearances, to draw adverse evidentiary inferences, or to take other administrative action, as appropriate, against an employee who refuses to cooperate with such a polygraph examination.

Finally, agency heads should be directed to impose appropriate administrative sanctions in situations where employees fail to cooperate with investigations or are found to have disclosed classified information without authorization. This will provide assurance to all involved in the investigatory process that their efforts will be worthwhile. There is clear authority to discipline or discharge employees for the failure to cooperate with an investigation. What is required is the determination to use this authority in appropriate cases.