Calendar No. 701

106TH CONGRESS, *2d Session* | SENATE | REPORT 106–352

THE COUNTERINTELLIGENCE REFORM ACT OF 2000

JULY 20, 2000.—Ordered to be printed

Mr. SHELBY, from the Select Committee on Intelligence, submitted the following

REPORT

[To accompany S. 2089]

The Select Committee on Intelligence, to which was referred the bill (S. 2089) to amend the Foreign Intelligence Surveillance Act of 1978 to modify procedures relating to orders for surveillance and searches for foreign intelligence purposes, and for other purposes, having considered the same, reports favorably thereon with amendments and recommends that the bill as amended do pass.

PURPOSE

The proposed legislation is intended to improve coordination within and among the U.S. Government agencies investigating and prosecuting espionage cases and other cases affecting national security. The legislation clarifies in statute the obligations of each of the affected agencies, ensures accountability in decisionmaking by relevant agency heads, and codifies current law and practice with respect to a determination of "probable cause" under the statute.

SCOPE OF COMMITTEE REVIEW

The Committee conducted a detailed review of the Counterintelligence Reform Act of 2000. The Committee conducted hearings and received comments from the affected agencies of the intelligence and law enforcement communities. The following report explains the Committee's amendments to the bill as reported by the Judiciary Committee on May 23, 2000, and highlights several additional issues that the Committee considered in the course of its evaluation of S. 2089.

Background

Investigations into espionage by the People's Republic of China (PRC) against Department of Energy (DOE) nuclear weapons laboratories and other U.S. Government facilities have identified extensive problems and shortcomings in the government's response to this critical counterintelligence threat.[1] At the structural level, attention has focused primarily on reforming and reorganizing DOE security, counterintelligence, and national security structures and programs, as well as altering attitudes toward security among DOE scientists. Concern over PRC espionage, in particular the PRC's use of sophisticated, non-traditional methods, has also fueled existing concerns over the adequacy of government wide counterintelligence structures, programs, and policies to address both emerging threats and traditional adversaries using cutting edge technologies and tradecraft in the 21st century.

At the operational level, investigations into PRC nuclear espionage have identified extensive problems in the DOE and FBI investigations into the compromise of classified information on the W–88 warhead and other U.S. nuclear weapons, including:

- the FBI's failure to devote adequate resources and attention to this critical investigation;
- extensive failures in coordination, information-sharing, and follow-through, both within and between the DOE and the FBI, that led to many missed opportunities and critical failures to act; and
- problems in the Department of Justice's response to the FBI's application for surveillance pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA).

Since March 1999, the Senate Select Committee on Intelligence (SSCI) held numerous hearings and briefings on PRC espionage against DOE labs and the resulting damage to U.S. national security; the DOE and FBI investigations, including the use of the FISA; longstanding DOE security and counterintelligence problems; and DOE reorganization. In addition, the Committee held three hearings and Member briefings on counterintelligence policies and programs government wide, including two sessions on the Administration's draft counterintelligence reorganization plan entitled "Counterintelligence for the 21st Century."

In response to some of the issues identified in the investigation of espionage at the DOE labs, on February 24, 2000, Senators Specter, Torricelli, Thurmond, Biden, Grassley, Feingold, Helms, Schumer, Sessions and Leahy introduced the "Counterintelligence Reform Act of 2000" (S. 2089). In early April 2000, the SSCI held a closed hearing to receive testimony on S. 2089 and other issues involving the FISA. The bill was considered by the Senate Judiciary Committee on May 18, 2000, and ordered favorably reported with an amendment in the nature of a substitute. On May 23, S. 2089 was reported to the Senate and immediately referred to the SSCI for consideration.

---

[1] PRC espionage and the U.S. Government's response have been the subject of investigations by, inter alia, the Senate Select Committee on Intelligence, the House Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China, the President's Foreign Intelligence Advisory Board (PFIAB), the Senate Committee on Governmental Affairs, the Senate Judiciary Subcommittee on Administrative Oversight and the Courts, and most recently, the Attorney General's Review Team ("Bellows Report").

The Office of Intelligence Policy and Review

The Office of Intelligence Policy and Review (OIPR) in the Department of Justice is responsible for advising the Attorney General on matters relating to the national security of the United States. As part of its responsibilities, the OIPR prepares and presents to the Foreign Intelligence Surveillance Court (FISC) all applications for electronic surveillance and physical searches under the Foreign Intelligence Surveillance Act of 1978.

In June 2000, the National Commission on Terrorism (referred to as the Bremer Commission) issued its report entitled, "Countering The Changing Threat of International Terrorism." One of the significant findings of the Bremer Commission was that the Department of Justice applies the FISA statute in a "cumbersome and overly cautious manner." Based on testimony before the Select Committee on Intelligence and agency discussions, the Committee agrees with the conclusions of the Bremer Commission regarding the Justice Department's application of the FISA statute. Agencies have informed the Committee that the FISA application process, as interpreted by the OIPR is administratively burdensome and, at times, extremely slow. Many applications undergo months of scrutiny before submission to the court because the OIPR prescribes standards and restrictions not imposed by the statute.

In its substitute amendment to S. 2089, the Judiciary Committee added a provision authorizing a substantial increase in funds for the OIPR. While the Committee agrees that the OIPR must act immediately to address the issues highlighted above, the Committee doubts that the significant infusion of funds authorized in Section 6, by itself, will remedy the majority of these problems. Since many of these problems stem from policy restrictions rather than resource constraints, the Committee expects the OIPR to conduct a review of the way it conducts business, including a "zero-based" review of all requirements and restrictions imposed upon the FISA application process to ensure they are specifically mandated by the statute. In order to ensure that the OIPR is properly addressing these issues, the Committee has prohibited the expenditures of funds authorized in Section 6 until the OIPR submits a report to the appropriate committees setting forth how it will utilize these additional funds to remedy the issues addressed above, and the results of the "zero-based" review described above.

Prior agent relationships

Sections 2(a) and 3(a), as adopted by the Judiciary Committee, require FISA applications for counterintelligence purposes to include a detailed description of any current or relevant prior relationship of the subject of an investigation with any intelligence or law enforcement agency. Although these sections were deleted in the Intelligence Committee mark, the Committee believes that a current relationship between an agency within the U.S. Intelligence Community and the subject of a counterintelligence investigation should be acknowledged, to the extent practicable and with due regard for the protection of sources and methods, in any FISA request targeting that particular subject.

The Committee also notes that, in certain cases, prior relationships between an agency within the U.S. Intelligence Community and the subject of a counterintelligence investigation may be useful

in the consideration of a request for a FISA order targeting that subject. The Committee expects that any agency requesting an order to conduct electronic surveillance or physical searches under the FISA will fully inform the OIPR, to the extent practicable and with due regard for the protection of sources and methods, of any current or relevant prior relationship between the agency and the target of the FISA application.

Past activities in establishing probable cause

The Department of Justice has been criticized for its failure, in the summer of 1997, to approve for submission to the FISC the FBI's application for FISA surveillance of Dr. Wen Ho Lee and his wife, Sylvia Lee, suspects in the FBI investigation into the compromise of classified information relating to the W–88 warhead. In particular, the OIPR has been criticized for an overly restrictive interpretation of the FISA "currency" requirement. This is the issue of how recent a subject's activities must be to support a finding of probable cause that the subject is engaged in clandestine intelligence gathering activities.

Subsection 2(c) of S. 2089 amends the FISA to state explicitly that past activities of a target may be considered in determining whether there is probable cause to believe that the target of electronic surveillance is an "agent of a foreign power." Subsection 3(c) adds an identical provision governing FISA applications for physical searches.

While existing law does not specifically address "past activities," it does not preclude, and legislative history supports, the conclusion that past activities may be part of the totality of circumstances considered by the FISC in making a probable cause determination. This reflects the practical consideration, well-known to the drafters of the FISA, that espionage is by its very nature clandestine, and that to maintain cover, a clandestine agent may lie dormant, often for years, between espionage activities.

The OIPR and the FBI have informed the Committee that in their view, this provision represents a codification of current law and practice. This is precisely the Committee's intent: to clarify and make explicit, for the benefit of future FBI agents, OIPR attorneys, and FISC judges, that the FISA contemplates, and always has contemplated, that the past activities of a target may be considered in a determination of probable cause.

Classified Information Procedures Act

Originally, an additional amendment to S. 2089 was proposed by one of the bill's cosponsors for consideration when the bill reached the full Senate that would have amended the Classified Information Procedures Act (CIPA) (18 U.S.C. App.) to address concerns about the handling of the Dr. Peter H. Lee case by the Department of Justice, the Department of Defense, and the U.S. Navy. Lee, a former employee of Los Alamos and Lawrence Livermore Nuclear Laboratories and TRW Inc., in December 1997 pled guilty to transmitting classified national defense information to the PRC in viola-

tion of 18 U.S.C. 793(d) and making false statements about his contacts with PRC nationals in violation of 18 U.S.C. 1001.[2]

The proposed amendment reflected a belief that there was a lack of coordination and cooperation between the Department of Justice and other agencies that affected adversely the decision-making process in the case. This Committee is concerned that the original proposed amendment would allow excessive intrusion into the prosecutorial function.

In light of this Committee's concerns with the potential impacts of the proposed amendment, the Committee agreed to include a much narrower amendment to the bill in Committee. Accordingly, Section 7 of S. 2089 codifies existing practice followed by Department of Justice prosecutors in cases involving classified information. Section 7 requires the Assistant Attorney General for the Criminal Division and the United States Attorney, or their designees, to provide briefings to the head of the agency that originated the classified information at issue in the case. These briefings will begin as soon as practicable and appropriate, consistent with rules governing grand jury secrecy, and will continue thereafter, as needed, to keep the agency head fully and currently informed. The purpose of the briefings is to make sure that the agency head understands the scope and volume of the CIPA procedures. In addition, the agency head will have an opportunity at various stages of the case to make his or her views known to the prosecutors as to whether sources and methods and other classification concerns are receiving adequate protection. The Committee notes that a successful prosecution depends on informed prosecutors, and believes that this provision will aid in ensuring an appropriate flow of information between prosecutors and affected agencies.

The Committee believes that the Department of Justice has a responsibility to ensure that its prosecutors, and affected agency officials, are fully aware of, and understand, the CIPA procedures. The CIPA has proven to be a successful mechanism for enabling prosecutions that involve national security information to proceed in a manner that is both fair to the defendant and protective of classified information. Before the CIPA, the United States Government sometimes had to make the difficult choice between either dismissing a criminal case or proceeding in the face of the risk that classified information might be made public. Neither alternative was in the best interests of the intelligence or law enforcement agencies—or of the American people. The CIPA provided pre-trial procedures for the court to resolve in camera and ex parte these issues in a manner that protects both the national security and the defendant's right to a fair trial. The government may take an immediate appeal of adverse rulings and, if the issues cannot be resolved in a manner that protects national security, may then make informed decisions on whether to dismiss some or all of the charges.

In any case in which classified information is at issue, the so-called "victim agency" that originated the information is the agency whose equities are most directly implicated. The head of that agency is responsible for protecting the information and, accordingly,

[2] Dr. Peter Lee was sentenced to 12 months in a halfway house, a $20,000 fine, and 3,000 hours of community service.

will have a strong interest in the key decisions made by the prosecutors as the case develops. The Committee believes that, in the vast majority of cases, the lawyers from the Department of Justice and the United States Attorneys Offices who are responsible for making the prosecutorial decisions consult on a regular basis with the agency head or his or her designee. While prosecutorial discretion ultimately rests with Department of Justice officials, it stands to reason that in cases designed to protect the national security—such as espionage and terrorism cases—prosecutors should ensure they do not make decisions that, in fact, end up harming the national security.

Sharing within the Intelligence Community of information collected under FISA court orders

By definition, information collected pursuant to a court order issued under the Foreign Intelligence Surveillance Act is foreign intelligence not law enforcement information. Accordingly, the Committee wants to clarify that the FISA "take" can and must be shared by the Federal Bureau of Investigation with appropriate intelligence agencies. For the intelligence mission of the United States to be successful, there must be a cooperative and concerted effort among intelligence agencies. Any information collected by one agency under foreign intelligence authorities that could assist another agency in executing its lawful mission should be shared fully and promptly. Only then can the United States Government pursue aggressively important national security targets including, for example, counterterrorist and counternarcotics targets.

The Committee has been briefed on the recent efforts by the Federal Bureau of Investigation and the Central Intelligence Agency to enhance their ability to share valuable information collected under FISA orders. The Committee commends these efforts and expects them to continue and to be broadened to include all areas of the foreign intelligence mission. Only when an efficient and effective program is in place to ensure full sharing of information possessed by the United States Government will the Committee be satisfied that the national security needs of the country are being protected.

SECTION-BY-SECTION ANALYSIS AND EXPLANATION

Section 1. Short title

The bill is entitled the "Counterintelligence Reform Act of 2000."

Section 2. Orders for electronic surveillance under the Foreign Intelligence Surveillance Act of 1978

Subsection 2(a) of S. 2089 requires the Attorney General to review personally any application to conduct electronic surveillance under the Foreign Intelligence Surveillance Act (FISA), if requested to do so in writing by the Director of Central Intelligence, the Director of the Federal Bureau of Investigation, the Secretary of Defense, or the Secretary of State. If the Attorney General disapproves the application, the disapproval must be in writing and must set forth the modifications, if any, to the application that would be necessary for the DOJ to forward the request to the FISC. Delegation of either the request or the review may occur in cases where the agency head is disabled or otherwise unavailable. The

Committee adds a technical amendment to ensure the delegation authority functions as intended. The Committee notes that this provision is intended to be an extraordinary authority, permitting an opportunity for the heads of the enumerated agencies and departments to appeal a decision to the Attorney General, who ultimately is charged by statute to approve FISA applications for review by the FISA court. The Committee will monitor implementation of this provision to ensure it remains a process for appeal of FISA applications that are particularly sensitive and warrant personal review by the Attorney General.

Subsection 2(b) amends the FISA to state explicitly that past activities of a target may be considered in determining whether there is probable cause to believe that the target of electronic surveillance is an "agent of a foreign power." Current law does not specifically address "past activities," but nothing precludes, and legislative history supports, that past activities be part of the probable cause determination. The Committee understands that the FISC will assess the relevance of past activities in determining probable cause.

Section 3. Orders for physical searches under the Foreign Intelligence Surveillance Act of 1978

Subsection 3 of S. 2089 adds the identical requirements, as described in Subsection 2, for applications relating to unconsented physical searches.

Section 4. Disclosure of information acquired under the Foreign Intelligence Surveillance Act of 1978 for law enforcement purposes

The Committee modifies Section 4 as adopted by the Committee on Judiciary and replaces the provision with an amendment to current semi-annual reporting requirements under Section 108(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1808(a)). The Attorney General will be required to track the use of FISA material for law enforcement purposes, either as leads or as evidence at trial, and to include such data in the Attorney General's Semi-Annual report to the Committees on Intelligence. Additionally, the Attorney General is directed to submit a report on the authorities and procedures utilized by the Department of Justice for determining whether to disclose information acquired under the FISA for law enforcement purposes. This report will be submitted to the House and Senate Committees on Intelligence and the Judiciary.

Section 5. Coordination of counterintelligence with the Federal Bureau of Investigation

Section 5 of S. 2089 establishes specific procedures regarding the conduct and coordination of counterintelligence investigations. The Committee believes that the determination of whether to leave a subject in place should be retained by the host agency. The Committee modifies subsection 5(a) to require the FBI to provide a written assessment of the potential impact of agency actions on a counterintelligence investigation, rather than a written finding that the subject of a counterintelligence investigation should be left in place. The host agency shall use the assessment as an aid in determining whether a target should be retained in place, and, if so,

under what circumstance, and provide written notification of the determination to the FBI. The Committee envisions that there will be a give-and-take between the two agencies in reaching the best result.

Subsection 5(b) adds "in a timely manner" to the statutory requirement that the FBI provide information and consultation to a concerned agency or department regarding an espionage investigation pertaining to the personnel, operations, or information of such agency or department.

Subsection 5(c) requires the FBI to notify appropriate executive branch officials of the commencement of a full field espionage investigation of an executive branch employee. The head of a department or agency is required by this subsection to consult and coordinate with the FBI prior to conducting a polygraph examination, interrogation, or other action that is likely to alert a subject of an investigation.

Section 6. Enhancing protection of national security at the Department of Justice

At the request of the OIPR, the Judiciary Committee added Section 6 of S. 2089 which authorizes additional resources to meet increased personnel demands to process FISA applications, combat terrorism, participate effectively in counterespionage investigations, provide policy analysis on national security issues, and enhance secure computer and telecommunications facilities. The Committee amends the provision in a manner that does not change authorization requirements, but adds the Intelligence Committees as recipients of the Attorney General's report required by the section.

The Committee notes that the OIPR received $4.089 million for fiscal year 2000. Due to the substantial increase in funds authorized by this provision for the OIPR, the Committee further amends Section 6 to make the authorization of additional resources subject to the Attorney General submitting a report to the appropriate committees on how these resources will be used by the OIPR to improve and strengthen its oversight of field offices, streamline and increase efficiency of the FISA application process, and address issues identified in the April 2000 semiannual report of the Attorney General to the Intelligence Committees under section 108(a) of Foreign Intelligence Surveillance Act of 1978.

Section 7. Coordination requirements relating to the prosecution of cases involving classified information

Section 7 amends the Classified Information Procedures Act to require the Department of Justice to brief senior officials, including the agency head or his designee, of an affected agency as soon as practicable after the prosecution team determines that a case involving classified information could result in a prosecution, and at such other times as to ensure that appropriate officials are fully and currently informed regarding the status of the case.

Section 8. Severability

This section is simply a savings clause that ensures that any section in the Act that is held invalid will not prejudice any other provision of the Act.

COMMITTEE ACTION

On July 18, 2000, by a vote of 15–0, the Select Committee on Intelligence approved the bill with amendments and ordered that it be favorably reported as amended.

ESTIMATE OF COSTS

No Congressional Budget Office estimate was available at the time the report was filed. The Committee will publish the estimate in the Congressional Record as soon as it is received from the Congressional Budget Office.

EVALUATION OF REGULATORY IMPACT

In accordance with paragraph 11(b) rule XXXVI of the Standing Rules of the Senate, the Committee finds that no regulatory impact will be incurred by implementing the provisions of this legislation.

CHANGES IN EXISTING LAW

It is the opinion of the Committee that it is necessary to dispense with the requirements of section 12 of rule XXVI of the Standing Rules of the Senate in order to expedite the business of the Senate.