Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated December 17, 2024

Foreign Intelligence Surveillance Act (FISA)

Introduction

Congress enacted the Foreign Intelligence Surveillance Act (FISA) in 1978. FISA provides a statutory framework for government agencies to obtain authorization to gather foreign intelligence by means of (1) electronic surveillance, (2) physical searches, (3) pen registers and trap and trace (PR/TT) devices (which record or decode dialing, routing, addressing, or signaling information), or (4) the production of certain business records. This In Focus describes FISA and potential issues for Congress.

FISA's Origin

Following revelations regarding widespread privacy violations by the federal government during the Watergate era, Congress enacted FISA to govern foreign intelligence information collection. FISA currently defines *foreign intelligence information* as information relating to a foreign power or that generally concerns the ability of the United States to protect against international terrorism, potential attacks by foreign powers or agents of foreign powers, or international drug trafficking. Though Congress initially limited FISA to regulating government use of electronic surveillance, Congress has amended FISA to regulate other intelligence-gathering practices, such as physical searches, the use of PR/TT devices, and compelled production of certain types of business records.

Foreign Intelligence Surveillance Courts

FISA established two specialized foreign intelligence courts to approve the use of FISA investigative authorities. The Foreign Intelligence Surveillance Court (FISC) has original jurisdiction over FISA applications, while the Foreign Intelligence Surveillance Court of Review (FISCR) hears appeals from the FISC. The FISC is composed of 11 federal judges, while the FISCR has three, all designated by the Chief Justice of the United States. The FISC and FISCR normally hear ex parte submissions by the government, but they also hear challenges to FISA orders brought by communications providers or other third parties.

The FISC and FISCR must designate at least five individuals as eligible to serve as amici curiae (essentially, independent advisors to the court). These courts may appoint one or more amici curiae when they deem this appropriate. These courts must appoint one or more amici curiae when a case "presents a novel or significant interpretation of the law" or involves targeting non-U.S. persons abroad, unless a court deems such an appointment "inappropriate."

Electronic Surveillance and Physical Search Orders

Titles I and III of FISA provide a framework by which government agencies may seek orders from the FISC authorizing electronic surveillance or physical searches to collect foreign intelligence. Before seeking a FISC order, federal officials must first obtain approval from the Attorney General (AG), Acting Attorney General, Deputy Attorney General, or, if designated, the Assistant Attorney General for National Security.

Applications for electronic surveillance or physical search orders must include the following: (1) the applicant's identity; (2) information regarding the target's identity, if known; (3) justifications for searching or surveilling the target; (4) a statement establishing a sufficient relationship between the target and the search location; (5) a description of what will be searched or surveilled; (6) a description of the nature of the information sought or of the foreign intelligence sought; (7) proposed minimization procedures (addressing the retention, use, and dissemination of intercepted communications); (8) a discussion of how the search or surveillance will be carried out; and (9) a discussion of prior applications. If electronic surveillance is sought, applications must discuss surveillance duration.

The government must also include in its applications written certifications from specified executive branch officials regarding the nature, purpose, and significance of the information sought. For the FISC to issue a FISA order, the government must show probable cause that the surveillance target is a foreign power or agent of a foreign power and that the target is using, or is about to use, the facilities or places at which the search or surveillance is directed. Specified officials must additionally certify that a "significant purpose" of electronic surveillance or a physical search is obtaining foreign intelligence information. The FISCR has interpreted this to mean that "'[s]o long as the government entertains a realistic option of dealing with the [foreign] agent other than through criminal prosecution, it satisfies' the statutory requirements for acquisition." The FISC may approve an application if the above requirements are met.

PR/TT Orders

Title IV of FISA provides procedures for the government to seek FISC orders authorizing installing PR/TT devices to obtain foreign intelligence information. Additionally, if the information sought concerns a U.S. person, a PR/TT device may be used only for counterterrorism or counterintelligence. A PR/TT application must include (1) the identity of the federal officer seeking to use a PR/TT device, (2) the applicant's certification that the information likely to be obtained is foreign intelligence information, and (3) a specific selection term to be used as the basis of the PR/TT device. Unlike electronic surveillance or physical search orders, the FISC is not required to evaluate PR/TT applications under a probable cause standard. Instead,

pursuant to Title 50, Section 1803(d)(1), of the *U.S. Code*, the court may approve applications that satisfy statutory requirements.

Business Record Orders

Title V of FISA establishes procedures for the government to apply for an order compelling certain businesses to release records in connection with a foreign intelligence or counterterrorism investigation by the Federal Bureau of Investigation (FBI). The businesses covered are common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities. An application for these records must include specific and articulable facts supporting the belief that the records pertain to an agent of a foreign power. A business that receives a FISA business records order cannot disclose receipt of the order except as necessary to produce the required records.

Surveillance of Persons Abroad

Title VII of FISA addresses methods of acquiring foreign intelligence information targeting persons outside of the United States. Section 702 establishes procedures for collecting foreign intelligence when communications travel through domestic communications infrastructure. Collections under this section are authorized programmatically rather than individually. The AG and Director of National Intelligence (DNI) must draft a certification specifying collection procedures. The AG and DNI must also attest that collection procedures comport with statutory requirements concerning targeting individuals for surveillance, minimizing the collection and improper handling of certain information, and how and when the government can search collected information. The FISC must then review any certification and either (1) order the government to correct deficiencies or (2) approve the certification and authorize collections for up to one year. Pursuant to a court-approved certification and joint AG and DNI authorization, the government may direct electronic communications service providers to assist in targeting non-U.S. persons reasonably believed to be located outside of the United States. These providers can challenge government directives before the FISC. In the event of exigent circumstances, the AG and DNI can authorize surveillance prior to submitting a certification to the FISC, but they must submit a certification to the FISC within seven days of commencing surveillance.

The certification must also contain proposed querying procedures under which federal agencies can search (i.e., query) Section 702 information using search terms. The FISC must ensure that querying procedures are consistent with the Fourth Amendment. There are numerous statutory querying restrictions specific to the FBI. For example, except in limited circumstances, FBI personnel cannot conduct queries using U.S.-person terms or identifiers solely addressing criminal activity. In addition, FBI personnel must receive supervisor or attorney approval to use U.S.-person query terms. To use query terms reasonably believed to identify U.S. elected officials, appointees, political candidates or organizations, or media personnel or organizations, FBI employees must receive approval from the deputy director of the FBI. To use query terms reasonably believed to identify U.S. religious organizations or prominent U.S. persons in such organizations, FBI personnel must receive approval from FBI attorneys. If FBI employees utilize query terms reasonably believed to identify a Member of Congress, the director of the FBI must "promptly" notify congressional leadership and the Member of Congress who is the subject of the query, unless notification would impede a national security or law enforcement investigation. The director of the FBI must also adopt "minimum accountability standards" with "escalating consequences for noncompliant querying of [U.S.-person] terms."

Section 702 expressly allows using information collected under the provision to vet "all non-United States persons who are being processed for travel to the United States." U.S.-person query terms may not be used for such vetting.

Sections 703 and 704 of FISA regulate other aspects of foreign intelligence collection. Section 703 grants jurisdiction to the FISC to "review an application and to enter an order approving targeting a U.S. person reasonably believed to be located outside the United States to domestically acquire foreign intelligence information." Section 704 mandates that, subject to certain exceptions, the government must obtain a FISA order to target a U.S. person located abroad through non-domestic intelligence acquisitions when the government would have had to obtain a warrant to conduct domestic surveillance of that person.

Legal Proceedings

Statutory provisions under Titles I, III, IV, and VII address introducing collected information in legal proceedings. Admissibility depends on whether information was lawfully acquired and whether surveillance conformed with controlling authorizations. The Supreme Court has held that these procedures do not supplant the state secrets privilege, which allows the government to avoid disclosing information when a court determines that disclosure would endanger national security. Thus, the government can assert the state secrets privilege in proceedings involving information collected under FISA to avoid disclosing such information or surveillance techniques.

Potential Issues for Congress

Lawmakers have proposed amendments addressing the FISC and FISCR. One proposed amendment would have increased the situations in which a court must appoint an amicus curiae, including when a proceeding involves activities protected by the First Amendment or novel techniques or technologies. Another proposed amendment would have allowed amici curiae to raise privacy and civil rights issues with a court, regardless of whether a court requested assistance with these issues.

Other proposed amendments concern querying. One proposed amendment would require an electronic record of every query, including terms used, date, and officer or employee identity. Another proposed amendment would limit the number of FBI officials authorized to query information to no more than five individuals in each office.

Andreas Kuersten, Legislative Attorney

IF11451

Disclaimer