



Updated April 11, 2024

Foreign Intelligence Surveillance Act (FISA): An Overview

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. Agencies request authorization for such activities from the Foreign Intelligence Surveillance Court (FISC), a specialized court created by FISA to act as a neutral arbiter of agency requests for FISA orders.

FISA's History

Following revelations regarding widespread privacy violations by the federal government during the Watergate era, Congress enacted FISA to establish guidelines for government collection of foreign intelligence. FISA defines “[f]oreign intelligence information” as information relating to a foreign power or that generally concerns the ability of the United States to protect against international terrorism or a potential attack by a foreign power or agent of a foreign power. Though Congress initially limited FISA to regulating government use of electronic surveillance, Congress subsequently 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.

Shortly after the 9/11 terrorist attacks, Congress enacted the USA PATRIOT Act (Patriot Act) to “provid[e] enhanced investigative tools” to “assist in the prevention of future terrorist activities and the preliminary acts and crimes which further such activities.” In particular, Section 215 of the Patriot Act enlarged the scope of FISA’s business records provision. Following information regarding National Security Agency bulk collection of telephone metadata under Section 215 of the Patriot Act, Congress enacted the USA FREEDOM Act, which narrowed Section 215 and FISA’s PR/TT authority and provided express authority for the FISC to appoint amici curiae to supplement its normally ex parte proceedings.

Other major changes to FISA include the FISA Amendments Act of 2008 (FAA), codified as Title VII of FISA. These amendments established procedures governing the targeting—for intelligence-gathering purposes—of non-U.S. persons located abroad. They also established statutory and procedural protections regarding surveillance of U.S. persons located outside the United States. Congress last reauthorized Title VII of FISA in early 2018. Title VII will sunset on April 19, 2024, absent congressional action.

In 2020, three provisions of FISA commonly associated with the Patriot Act lapsed. These provisions, which are discussed in more detail below, are covered by a grandfather provision which permits them to remain in effect with respect to investigations that existed before the sunset date.

Foreign Intelligence Surveillance Courts

FISA established two specialized foreign intelligence courts to approve the use of FISA investigative authorities. The FISC has original jurisdiction over FISA applications, while the Foreign Intelligence Surveillance Court of Review (FISCR) may hear appeals from the FISC. The FISC is composed of eleven federal judges, while the FISCR has three, all designated by the Chief Justice of the U.S. Supreme Court. While the FISC and FISCR normally hear ex-parte submissions by the government, the courts also have jurisdiction to hear challenges to FISA orders brought by communications providers or other third parties. Pursuant to the USA FREEDOM Act, the FISC and FISCR have also designated seven individuals as eligible to serve as amici curiae.

Electronic Surveillance and Physical Search Orders

Titles I and III of FISA provide a framework by which government agencies may seek a FISA order from the FISC authorizing electronic surveillance or physical searches for the purposes of collecting foreign intelligence. Before submitting an application for such an order to the FISC, 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) why the target may be searched or surveilled; (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 also discuss the duration of the surveillance.

The government must also include in its applications written certifications from specified executive branch officials regarding the nature, purpose, and significance of the information to be sought. For the FISC to issue a FISA

order, the government must show probable cause that the target of the surveillance is a foreign power or an 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. The FISC may approve such an application if the above requirements are met and it determines that probable cause exists to believe that the target of the order is an agent of a foreign power.

PR/TT Orders

Title IV of FISA provides procedures for the government to apply to the FISC for orders authorizing the installation of PR/TT devices to obtain foreign intelligence information. Additionally, if the information sought concerns a U.S. person, then a PR/TT device may only be used 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, and instead may approve an order after determining that it includes the required components.

Business Record Orders

Title V of FISA establishes procedures for the government to apply for an order compelling certain businesses to release records in their possession in connection with a foreign intelligence or counterterrorism investigation by the FBI. The only types of 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 giving reason to believe that the entity to whom the records pertain is an agent of a foreign power. Businesses that receive a FISA business records order are not permitted to disclose the receipt of such order to any other person except as necessary to produce the required documents.

FISA Amendments of 2008

Title VII of FISA, added by the FAA, establishes additional procedures to acquire foreign intelligence information regarding persons who are believed to be outside of the United States. These provisions affect both U.S. persons as well as non-U.S. persons, and are the only temporary provisions of FISA, scheduled to sunset on April 19, 2024.

The FAA added Section 702 of FISA, which establishes procedures to collect foreign intelligence when communications travel through the United States' communications infrastructure. Under Section 702, the government may compel electronic communications service providers for a period of up to one year to assist in targeting non-U.S. persons reasonably believed to be located outside the United States. The AG and the Director of National

Intelligence (DNI) must jointly certify that they authorize any such targeting, and the FISC must approve any program under Section 702 before its implementation. If time does not permit submitting the requisite certification to the FISC before authorization, the AG and DNI must submit their certification to the FISC within seven days of the commencement of the surveillance.

The FAA also added Sections 703 and 704 of FISA, which regulate other aspects of foreign intelligence collection. Section 703 grants jurisdiction to the FISC to “review an application and to enter an order approving the targeting of a United States person reasonably believed to be located outside the United States to 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 when the government also would have had to obtain a warrant to conduct domestic surveillance of that person.

Expired Provisions

As discussed in more detail in CRS Report R40138, *Origins and Impact of the Foreign Intelligence Surveillance Act (FISA) Provisions That Expired on March 15, 2020*, by Edward C. Liu, three provisions of FISA lapsed in 2020.

The first, Section 206 of the Patriot Act, amended FISA to permit “roving wiretaps.” Specifically, if the surveillance target is taking actions that “may have the effect of thwarting” surveillance (such as using disposable cell phone numbers or email addresses), the government could use a single FISA order to conduct surveillance on new phone numbers or email addresses used by the target without needing to apply to the FISC for a new order.

The second expired provision, Section 215 of the Patriot Act, enlarged the scope of business records that the government could request to include “any tangible thing.” Section 215 also eased the standard that an applicant must meet to obtain a FISA order compelling the production of “tangible thing[s].” As a result, an applicant for a FISA order needed only to provide “a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to” a foreign intelligence, international terrorism, or espionage investigation.

The final expired provision, Section 6001(a) of the Intelligence Reform and Terrorism Prevention Act (IRTPA), also known as the “lone wolf” provision, permitted surveillance of non-U.S. persons who are shown to be engaged in international terrorism, but without requiring evidence linking those persons to an identifiable foreign power or terrorist organization.

Edward C. Liu, Legislative Attorney

IF11451

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.