

# FISA AMENDMENTS ACT OF 2008

## OVERVIEW

The Act provides critically important authority for the U.S. Intelligence Community to acquire foreign intelligence information by targeting foreign persons reasonably believed to be outside the United States. It ensures that the Intelligence Community has the flexibility and agility it requires to respond quickly to opportunities and needs within a global communication system.

The Act provides a key role for each branch of Government. It assigns responsibilities jointly to the Attorney General (AG) and the Director of National Intelligence (DNI) to ensure that the Nation's chief law enforcement and intelligence officials work together in collecting intelligence in accordance with law. It requires the Foreign Intelligence Surveillance Court (FISA Court) to review and approve, or order corrections to, the procedures required by the Act and to ensure compliance with protections for Americans under the Fourth Amendment to the Constitution. And it requires that information about the implementation of these new procedures be reported to Congress, to ensure that Congress can fulfill its oversight role.

## PRIVACY AND CIVIL LIBERTY PROTECTIONS FOR AMERICANS

**Exclusivity.** The Act strengthens the requirement that FISA and specific chapters of Title 18 are the exclusive means by which electronic surveillance and certain criminal law interceptions may be conducted. In addition to the statutes specifically listed in the exclusivity provision, the Act provides that only an express statutory authorization for electronic surveillance or interception may constitute an additional exclusive means for that surveillance or interception.

**Targeting Procedures.** Knowing if a target is outside the U.S. is key to the protection of Americans. At least annually, the AG and DNI must submit to the FISA Court for review and approval targeting procedures for making that fundamental determination which governs collection under this bill.

**Minimization Procedures.** Making sure that information that is acquired about Americans, in the course of targeting foreigners, is used only for proper intelligence or law enforcement purposes is a second line of defense for Americans. These procedures must be reviewed and approved at least annually by the FISA Court.

**Individual Judicial Orders for Surveillance of Americans.** The Act requires individual FISA Court orders based on probable cause for the targeting of Americans not only when they are within the U.S. but also, for the first time, when they are outside of the United States -- whether they are working, studying, or traveling abroad.

**Reverse Targeting Guidelines.** The Act requires adoption by the Attorney General and submission to the Congress and FISA Court of guidelines to ensure compliance with the Act's limitations, including its prohibition on reverse targeting.

## **TIMING OF COLLECTION AND JUDICIAL REVIEW**

**Timing of Judicial Review.** The Act requires that the targeting procedures shall be submitted to and approved by the FISA court before the collection begins.

**Exigent Circumstances.** In rare cases, collection can begin while the court considers authorization only if the AG and DNI certify to the court that exigent circumstances exist and critical intelligence could be lost. The AG and DNI must submit procedures within 7 days and the court would make a determination within 30 days. During this period, all relevant minimization and reverse targeting guidelines would apply.

## **LIABILITY PROTECTIONS AND OBLIGATIONS OF AMERICAN COMPANIES**

**Prospective Immunity.** The Act ensures that the cooperation shall be in accordance with law, by providing an opportunity for the companies to challenge in court the lawfulness of directives to them and for the Government to compel compliance through judicial proceedings. Companies that act in accordance with directives provided under the law shall be protected against future liability.

**Retroactive Immunity.** The Act provides standards and procedures for liability protection for electronic communication service providers who assisted the Government between September 11, 2001 and January 17, 2007, when the surveillance program was brought under the FISA Court.

A district court hearing a case against a provider will decide whether the Attorney General's certification attesting that the liability protection standard has been met and is supported by substantial evidence. In making that determination, the court will have the opportunity to examine the highly classified letters to the providers that indicated the President had authorized the activity and that it had been determined to be lawful. The plaintiffs and defendants will have the opportunity to file public briefs on legal issues and the court should include in any public order a description of the legal standards that govern the order.

The immunity provision of the Act does not apply to any actions against the Government for any alleged injuries caused by government officials. Nor does the immunity provision involve any statement by the Congress, pro or con, on the legality of the President's program.

## **OVERSIGHT AND ACCOUNTABILITY**

**Inspector General Review.** The Act directs the Inspectors General of the Department of Justice, the Office of the DNI, the National Security Agency, and the Department of Defense to complete a comprehensive review, within the oversight authority of each IG, of the President's Surveillance Program. In no later than a year, the Inspectors General shall submit a report to Congress; the report shall be unclassified but may include a classified annex. In light of the dismissals of cases that may result from implementation of the immunity title, the IG review will be an especially important vehicle for reporting to Congress on the facts of the President's program, as well as to the public, to the extent classification permits.

**Multiple Levels of Oversight.** The Act provides for multiple levels of oversight both within the Executive Branch, including by Department of Justice and Intelligence Community Inspectors General, and in regular reporting to both the Congress and the FISA Court.

**Sunset.** The Act will sunset at the end of 2012 ensuring that the next Administration, together with the Congress, will address whether the Act should be made permanent or modified based on experience.