Section by Section Analysis

USA PATRIOT Amendments Act of 2009

Sec. 1. Short title and table of contents. Section 1 names this Act the "USA PATRIOT Amendments Act of 2009" and provides a table of contents for the entire bill.

Title I—USA PATRIOT Act Related Amendments

Sec. 101. Roving Wiretaps. Sec. 101 clarifies that when the government only provides a description of the target of surveillance for purposes of obtaining a warrant (whether or not that warrant is for a regular or roving FISA warrant), that description must be sufficient to allow a court to determine that the target is a single individual.

Sec. 102. Extension of Sunset of Sections 206 and 215 of USA PATRIOT Act. Sec. 102 extends the sunset dates of roving wiretaps and FISA business records to December 31, 2013.

Sec. 103. Access to Certain Tangible Things under section 501 of the Foreign Intelligence Surveillance Act of 1978. Sec. 103 (§215 tangible things) requires a statement of specific and articulable facts showing that the tangible things sought are relevant to an authorized investigation, other than a threat assessment. The "specific and articulable" language is not present in the current law, and is a more exacting standard for government to meet.

This section also retains the concept that certain types of records are "presumptively relevant" to a counterterrorism or counterintelligence related investigation (assuming an appropriate statement containing specific and articulable facts). The retention of the "presumptive relevance" for documents pertaining to foreign powers or agents of a foreign power accomplishes two important goals. First, it puts the government and a court on notice that these types of records are the type of documents that Congress generally expects the government will be pursuing in furtherance of authorized counterterrorism and counterintelligence investigations. The presumptive relevance standard does not, however, allow the government to obtain the documents merely by showing relevance to a foreign power or agent of a foreign power through a statement of "specific and articulable facts." A court must also find that the requested records are actually relevant to an authorized investigation.

Second, the government may be able to acquire certain records even if it cannot show that the documents are relevant to a foreign power or agent of a foreign power. However, these types of records, which do not fall into the "presumptively relevant" category, would be evaluated with a

higher degree of scrutiny by a court. The court would determine whether or not the government presented specific and articulable facts to show relevance to an authorized investigation.

With respect to judicial review, current law requires the recipient of a nondisclosure order associated with a § 215 order to wait a year before seeking judicial review of the nondisclosure order. Sec. 103 allows a recipient to challenge both the underlying order and any associated nondisclosure order immediately. In addition, the government must notify the recipient of a right to challenge the legality of the production order or nondisclosure order, and the procedure to follow to file such a petition at the time the government serves the § 215 order on the recipient. Absent bad faith on the part of the government, current law also allows a certification by a high level official to conclusively defeat a challenge to a nondisclosure order. Sec. 103 eliminates the concept of a "conclusive certification" entirely.

Compliance assessments of minimization procedures pertaining to §215 orders are now facilitated by allowing FISA court judges to review government compliance with minimization procedures associated with specific orders. A request for §215 records cannot be made to a library or bookseller for documentary materials that contain personally identifiable information concerning a patron. None of these elements are present in the current law.

Sec. 104. Sunset Relating to Individual Terrorists as Agents of Foreign Powers. Sec. 104 allows the "Lone Wolf" provision to sunset on December 31, 2009. "Lone Wolf" is not reauthorized.

Sec. 105. Audits. Sec. 105 requires the DOJ Inspector General to audit and submit reports to Congress for §215 tangible thing orders, National Security Letters (NSLs), and FISA pen register/trap and trace orders for all calendar years through 2013.

Sec. 106. Criminal "sneak and peek" searches. Sec. 106 requires the government to seek an extension for delaying notice of the search after seven (7) days, not the current thirty (30) days. Any extension to delay notice granted by a court cannot be longer than 21 days at a time. In addition, any application for extension must be made by the Senate-confirmed United States Attorney for the district seeking the delay. This section also narrows the circumstances under which the government could obtain a "sneak and peek" warrant by eliminating "otherwise seriously jeopardizing an investigation or unduly delaying a trial" as a situation that would permit the issuance of a "sneak and peek" warrant.

Sec. 107. Use of Pen Registers and Trap and Trace Devices under title 18, United States Code. Sec. 107 requires the application for a pen register to contain a statement of specific and articulable facts showing that the information likely to be obtained is relevant to an ongoing criminal investigation. Current law only requires a certification by the applicant.

Sec. 108. Orders for Pen Registers and Trap and Trace Devices for Foreign Intelligence Purposes. Sec. 108 requires the application for a pen register to contain a statement of specific and articulable facts relied upon by the applicant to justify the belief that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation. Current law only requires a certification by the applicant. This section also requires the implementation of minimization procedures for pen registers and trap and trace devices, and allows FISA court judges to assess the government's compliance with these minimization procedures. These are new requirements

Sec. 109. Public Reporting on the Foreign Intelligence Surveillance Act. Sec. 109 requires annual public reporting of aggregate numbers of requests for surveillance that also include a breakdown of requests for (a) electronic surveillance, (b) physical searches, (c) orders for tangible things (Section 215 orders), and (d) pen registers. Current law requires only public reporting of the above categories in the aggregate.

Sec. 110. Challenges to Nationwide Orders for Electronic Surveillance. Sec. 110 allows a provider of electronic communication service or remote computing service to challenge a subpoena, order, or warrant requiring disclosure of customer communications or records in either the district in which the order was issued or the district in which the order was served.

Title II—National Security Letter Reform

Sec. 201. Short Title. Sec. 201 indicates that title II shall be cited as the "National Security Letter Reform Act of 2009."

Sec. 202. Sunset. Section 202 provides a sunset date of December 31, 2013 for national security letters, with the effect of returning the relevant national security letter statutes to read as they read on October 25, 2001.

Sec. 203. National Security Letter defined. Sec. 203 defines "national security letter," for the purposes of this bill, as a request for information under one of the enumerated provisions of law.

Sec. 204. Modification of Standard. Sec. 204 requires an official with authority to issue a national security letter to document and retain a statement of specific and articulable facts showing that there are reasonable grounds to believe that the information sought pertains to a foreign power or agent of a foreign power. This standard changes the focus of the "relevance" required under current law from "authorized investigation" to "foreign power or agent of a foreign power." In addition, current law does not directly couple the relevance standard with "specific and articulable" facts as support for relevance—a more exacting standard for the government to meet. Current law also does not require the government to create and maintain a record of such facts at the time the national security letter is issued.

Sec. 205. Notification of Right to Judicial Review of Nondisclosure Order. Sec. 205 requires the government to notify a recipient of a national security letter of (1) a right to judicial review of any nondisclosure requirement imposed in connection with that national security letter and, (2) that the nondisclosure requirement will remain in effect during the pendency of any judicial review proceedings. Current law does not require such notification.

Sec. 206. Disclosure for Law Enforcement Purposes. Sec. 206 requires the Attorney General to authorize the use of any information acquired or derived from a national security letter in a criminal proceeding. Current law does not require such "use authority" for national security letters.

Sec. 207. Judicial Review of National Security Letter Nondisclosure Order. Sec. 207 establishes additional procedures for a recipient to seek judicial review of a nondisclosure requirement imposed in connection with a national security letter. If the recipient wishes to have a court review a nondisclosure requirement, the recipient must notify the government. Not later than thirty days after the receipt of notification, the government must apply for a court order prohibiting the disclosure of information about the national security letter or the existence of the national security letter. The nondisclosure requirement remains in effect during the pendency of any judicial review proceedings. The government's application for a nondisclosure order must include a certification from the Attorney General, Deputy Attorney General, or the Director of the FBI (or the head of another agency if not part of DOJ) containing a statement of specific and articulable facts indicating that disclosure may result in a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person. If a court determines that there is reason to believe that disclosure will result in one of the enumerated harms, the court will issue a nondisclosure order for no longer than 180 days. The government can seek renewals of nondisclosure orders for additional periods of not longer than 180 days each. If there comes a time when the facts supporting a nondisclosure order issued by the court cease to exist, the government must promptly notify a recipient who sought judicial review of a nondisclosure order that the nondisclosure is not longer in effect.

Current law neither requires the recipient to formally notify the government if "he" wishes to seek judicial review, nor specifies that the government will initiate such court review by applying for a court order. The government is also not required to notify a recipient who sought judicial review of a nondisclosure if or when such an order would cease to exist based on a change in facts supporting the nondisclosure order. In addition, absent bad faith on the part of the government, current law also allows a certification by a high level government official to conclusively defeat a challenge to a nondisclosure order if the challenge is filed within one year of the request for records. Current law also allows a recertification made by high level officials to be treated as conclusive, unless made in bad faith. Sec. 207 eliminates the concept of a "conclusive certification" entirely. Moreover, this section corrects constitutional defects in the

nondisclosure orders pertaining to national security letters as addressed in *Doe v. Mukasey*, 549 F.3d 861 (2nd Cir. 2008).

Sec. 208. Minimization Procedures. Sec. 208 requires the Attorney General to establish minimization and destruction procedures to ensure that information obtained pursuant to a national security letter regarding persons that are no longer of interest in an authorized investigation is destroyed.