Department of Justice

STATEMENT OF

DAVID KRIS
ASSISTANT ATTORNEY GENERAL

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ENTITLED

"REAUTHORIZING THE USA PATRIOT ACT:
ENSURING LIBERTY AND SECURITY"

PRESENTED

SEPTEMBER 23, 2009

Statement of
David Kris
Assistant Attorney General
Before the
Committee on the Judiciary
United States Senate
For a Hearing Entitled
"Reauthorizing the USA PATRIOT Act: Ensuring Liberty and Security"
Presented
September 23, 2009

Chairman Leahy, Ranking Member Sessions, and Members of the Senate Judiciary Committee, thank you for inviting me to speak to you today about the Administration's position regarding three Patriot Act Provisions that will, by their terms, expire on December 31, 2009. We believe that the best legislation will emerge from a careful and collaborative examination of these matters. As you know, today's hearing has been preceded by extensive discussion and deliberation within the legislative and executive branches, and constructive discussions have recently begun between Administration officials and Congressional staff. I would like to extend the Attorney General's gratitude for providing the Department with this opportunity to present the Administration's views formally to the Members of this Committee today.

Before I address each of the three expiring authorities, I would like to address a concern raised often during our discussions with Committee staff. The Department understands that Members of Congress may propose modifications to the legislation governing the three expiring authorities and other related authorities with the goal of providing additional protection for the privacy of law abiding Americans. The protection of privacy and civil liberties is of deep and abiding concern to the Department of Justice, and to the Administration as a whole. We are ready and willing to work with Members on any specific proposals you may have to craft legislation that both provides effective investigative authorities and protects privacy and civil liberties.

With respect to the three expiring authorities, we recommend reauthorizing section 206 of the USA PATRIOT Act, which provides for roving surveillance of targets who take measures to thwart FISA surveillance. It has proven to be an important intelligence-gathering tool in a small but significant subset of FISA electronic surveillance orders.

This provision states that where the Government sets forth in its application for a surveillance order "specific facts" indicating that the actions of the target of the order "may have the effect of thwarting" the identification, at the time of the application, of third parties necessary to accomplish the ordered surveillance, the order shall direct such third parties, when identified, to furnish the Government with all assistance necessary to accomplish surveillance of the target identified in the order. In other words, the "roving" authority is only available when the Government is able to provide specific information that the target may engage in counter-

surveillance activity (such as rapidly switching cell phone numbers). The language of the statute does not allow the Government to make a general, "boilerplate" allegation that the target may engage in such activities; rather, the Government must provide specific facts to support its allegation.

There are at least two scenarios in which the Government's ability to obtain a roving wiretap may be critical to effective surveillance of a target. The first is where the surveillance targets a traditional foreign intelligence officer. In these cases, the Government often has years of experience maintaining surveillance of officers of a particular foreign intelligence service who are posted to locations within the United States. The FBI will have extensive information documenting the tactics and tradecraft practiced by officers of the particular intelligence service, and may even have information about the training provided to those officers in their home country. Under these circumstances, the Government can furnish specific facts in its application to the FISA Court that demonstrate that the actions of the individual may have the effect of thwarting the identification of third parties whose assistance is needed to conduct the surveillance.

The second scenario in which the ability to obtain a roving wiretap may be critical to effective surveillance is the case of an individual who actually has engaged in counter-surveillance activities or in preparations for such activities. In some cases, individuals already subject to FISA surveillance are observed to be engaging in counter-surveillance or instructing associates on how to communicate with them through more secure means. In other cases, non-FISA investigative techniques have revealed counter-surveillance preparations (such as buying "throwaway" cell phones or multiple calling cards). The Government then offers these specific facts to the FISA court as justification for a grant of roving authority.

Since the roving authority was added to FISA in 2001, the Government has sought to use it in a relatively small number of cases (on average, twenty-two applications annually for 2003-2008). We would be pleased to brief Members or staff regarding specific case examples in a classified setting. The FBI uses the granted authority only when the target actually begins to engage in counter-surveillance activity that thwarts the already-authorized surveillance, and does so in a way that renders the use of roving authority feasible.

Roving authority is subject to the same court-approved minimization rules that govern other electronic surveillance under FISA and that protect against the acquisition or retention of non-pertinent information. The statute generally requires the Government to notify the FISA court within 10 days of the date upon which surveillance begins to be directed at any new facility. Over the past seven years, this process has functioned well and has provided effective oversight for this investigative technique.

We believe that the basic justification offered to Congress in 2001 for the roving authority remains valid today. Specifically, the ease with which individuals can rapidly shift between communications providers, and the proliferation of both those providers and the services they offer, almost certainly will increase as technology continues to develop.

International terrorists, foreign intelligence officers, and espionage suspects — like ordinary criminals — have learned to use these numerous and diverse communications options to their advantage. Any effective surveillance mechanism must incorporate the ability to address rapidly an unanticipated change in the target's communications behavior. The roving electronic surveillance provision has functioned as intended and has addressed an investigative requirement that will continue to be critical to national security operations. Accordingly, we recommend reauthorizing this feature of FISA.

We also recommend reauthorizing section 215 of the USA PATRIOT Act, which allows the FISA court to compel the production of "business records." The business records provision addressed a gap in intelligence collection authorities that had previously existed and has proven valuable in a number of contexts.

The USA PATRIOT Act made the FISA authority relating to business records roughly analogous to that available to FBI agents investigating criminal matters through the use of grand jury subpoenas. The original FISA language, added in 1998, limited the business records authority to four specific types of records, and required the Government to demonstrate "specific and articulable facts" supporting a reason to believe that the person to whom the requested records pertain was a foreign power or an agent of a foreign power. In the USA PATRIOT Act, the authority was changed to encompass the production of "any tangible things" and the legal standard was changed to relevance to an authorized investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.

The Government first used the USA PATRIOT Act business records authority in 2004 after extensive internal discussions over its proper implementation. The Department's inspector general evaluated the Department's implementation of this new authority at length, in reports that are now publicly available. Other parts of the USA PATRIOT Act, specifically those eliminating the "wall" separating intelligence operations and criminal investigations, also had an effect on the operational environment. The greater access that intelligence investigators now have to criminal tools (such as grand jury subpoenas) reduces but does not eliminate the need for intelligence tools, such as the business records authority. The operational security requirements of most intelligence investigations still require the secrecy afforded by the FISA authority.

For the period 2004-2008, the FISA court has issued about 236 orders to produce business records. Of these, 173 orders were issued in 2004-06 in combination with FISA pen register orders to address an anomaly in the statutory language that prevented the acquisition of subscriber identification information ordinarily associated with pen register information. Congress corrected this deficiency in the pen register provision in 2006 with language in the USA PATRIOT Improvement and Reauthorization Act. Thus, this use of the business records authority became unnecessary.

The remaining business records orders issued between 2004 and 2007 were used to obtain transactional information. As many Members are aware, some of these orders were used

to support important and highly sensitive intelligence collections. The Department can provide additional information to Members or their staff in a classified setting.

It is noteworthy that no recipient of a FISA business records order has ever challenged the validity of the order, despite the availability, since 2006, of a clear statutory mechanism to do so. At the time of the USA PATRIOT Act, there was concern that the FBI would exploit the broad scope of the business records authority to collect sensitive personal information on constitutionally protected activities, such as the use of public libraries. This simply has not occurred, even in the environment of heightened terrorist threat activity. The oversight provided by Congress since 2001, the specific oversight provisions added to the statute in 2006, and the requirement that the government make a specific showing to the FISA Court in each application have helped to ensure that the authority is being used as intended.

Based upon this operational experience, we believe that the FISA business records authority should be reauthorized. There will continue to be instances in which FBI investigators need to obtain transactional information that does not fall within the scope of authorities relating to national security letters and are operating in an environment that precludes the use of less secure criminal authorities. Moreover, in some instances, such as counterintelligence investigations, the use of criminal authorities may be inappropriate because the investigation is not focused on a violation of criminal law. Many of these instances will be mundane (as they have been in the past), such as the need to obtain driver's license information that is protected by State law. Others will be more complex, such as the need to track the activities of intelligence officers through their use of certain business services. In all these cases, the availability of a generic, court-supervised FISA business records authority is the best option for advancing national security investigations in a manner that protects privacy and civil liberties. The absence of such an authority could force the FBI to sacrifice key intelligence opportunities, to the detriment of the national security.

Finally, the Department recommends reauthorizing Section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004, which defines a "lone wolf" agent of a foreign power and allows a non-United States person who "engages in international terrorism activities" to be considered an agent of a foreign power under FISA.

Enacted in 2004, this provision arose from discussions inspired by the Zacarias Moussaoui case. The basic idea behind the authority was to cover situations in which information linking the target of an investigation to an international group was absent or insufficient, although the target's engagement in "international terrorism" was sufficiently established. The definition is quite narrow: it applies only to non-United States persons; the activities of the person must meet the FISA definition of "international terrorism"; and the information likely to be obtained must be foreign intelligence information. What this means, in practice, is that the Government must know a great deal about the target, including the target's purpose and plans for terrorist activity (in order to satisfy the definition of "international terrorism"), but still be unable to connect the individual to any group that meets the FISA definition of a foreign power.

To date, the Government has not encountered a case in which this definition was both necessary and available, *i.e.*, the target was a non-United States person. Thus, the definition has never been used in a FISA application. We do not believe, however, that this means the authority is now unnecessary. Subsection 101(b) of FISA provides ten separate definitions for the term "agent of a foreign power" (five applicable only to non-United States persons, and five applicable to all persons). Some of these definitions cover the most common fact patterns; others describe narrow categories that may be encountered rarely. Although the latter group may be rarely encountered, it includes legitimate targets that cannot be accommodated under the more generic definitions and will escape surveillance but for the more specific definitions.

We believe that the "lone wolf" provision falls squarely within this class. While we cannot predict the frequency with which it may be used, we can foresee situations in which it would be the only avenue to effect surveillance. For example, we could have a case in which a known international terrorist affirmatively severs his connection with his group, perhaps following some internal dispute. Although the target still would be an international terrorist and an appropriate target for intelligence surveillance, the Government could no longer represent to the FISA court that he is currently a member of an international terrorist group or acting on its behalf. In the absence of the "lone wolf" definition, the Government would have to postpone FISA surveillance unless and until the target could be linked to another group. The absence of a known connection would not, however, necessarily mean that the individual did not pose a real and imminent threat. The lone wolf provision may also be required to conduct surveillance on an individual who "self-radicalizes" by means of information and training provided via the Internet. Although this target would have adopted the aims and means of international terrorism (and therefore be a legitimate national security target), he would not actually be acting as an agent of a terrorist group. Without the lone wolf definition, the Government might be unable to establish FISA surveillance.

These scenarios are not remote hypotheticals; they are based on trends we observe in current intelligence reporting. We cannot determine how common these fact patterns will be in the future or whether any of the targets will so completely lack connections to groups that they cannot be accommodated under other definitions. The continued availability of the lone wolf definition eliminates any gap. The statutory language of the existing provision ensures its narrow application, so the availability of this potentially useful tool carries little risk of overuse. We believe that it is essential to have the tool available for what we believe will be the rare situation in which it is necessary rather than to delay surveillance of a terrorist in the hopes that the necessary links are established or even to forego it entirely because such links cannot be established.

In short, the Department and the Administration believe that each of these three provisions provides important and effective investigative authorities. We believe that the current statutory scheme, together with the rules, guidelines, and oversight mechanisms observed by the Executive branch with respect to these authorities, safeguard Americans' privacy and civil liberties. We look forward to working with the Committee to reauthorize these important

authorities in a manner that continues to protect both national security and privacy and civil liberties.