1551472

United States Senate

SELECT COMMITTEE ON INTELLIGENCE
WASHINGTON, DC 20510-6475

SSCI #2009-1438

March 31, 2009

The Honorable Eric H. Holder, Jr.
Attorney General
Department of Justice
Washington, D.C. 20530

The Honorable Dennis C. Blair
Director of National Intelligence
Washington, D.C. 20511

Dear Attorney General Holder and Director Blair:

Three provisions of the Foreign Intelligence Surveillance Act of 1978, as amended, are scheduled to sunset on December 31, 2009. Two of them—on roving wiretaps and business records—were enacted or significantly amended by sections 206 and 215 of the USA PATRIOT Act of 2001, and extended for four years by the USA PATRIOT Improvement and Reauthorization Act of 2005. The third—on lone wolf surveillance authority—was enacted as section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004, and also extended for four years by the Reauthorization Act.

We would like to begin consideration of these provisions soon so that legislation can be enacted in advance of the end of the year. We would, therefore appreciate receiving from you, by May 1, 2009, your recommendations together with a written presentation of the facts and reasons that support those recommendations. To the extent that national security permits, please do so in an unclassified manner to enhance public understanding of your recommendations. Please supplement that unclassified presentation with a classified annex as appropriate.

If there are further recommendations you would like to make jointly to our Committee for legislative consideration this year based on experience under the FISA Amendments Act of 2008 or other matters relating to national security investigations, please include them in your response to this request.

We intend to schedule a hearing in May that will provide the Committee with an initial opportunity to consider your recommendations.

Sincerely,

Dianne Feinstein
Chairman

Christopher S. Bond
Vice Chairman

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

September 14, 2009

The Honorable Dianne Feinstein
Chairwoman
The Honorable Christopher S. Bond
Vice Chairman
Select Committee on Intelligence
United States Senate
Washington, D.C. 20510

Dear Senators Feinstein and Bond:

Thank you for your letter requesting our recommendations on the three provisions of the Foreign Intelligence Surveillance Act ("FISA") currently scheduled to expire on December 31, 2009. We believe that the best legislation will emerge from a careful examination of these matters. In this letter, we provide our recommendations for each provision, along with a summary of the supporting facts and rationale. We have discussed these issues with the Office of the Director of National Intelligence, which concurs with the views expressed in this letter.

We also are aware that Members of Congress may propose modifications to provide additional protection for the privacy of law abiding Americans. As President Obama said in his speech at the National Archives on May 21, 2009, "We are indeed at war with al Qaeda and its affiliates. We do need to update our institutions to deal with this threat. But we must do so with an abiding confidence in the rule of law and due process; in checks and balances and accountability." Therefore, the Administration is willing to consider such ideas, provided that they do not undermine the effectiveness of these important authorities.

1. **Roving Wiretaps, USA PATRIOT Act Section 206 (codified at 50 U.S.C. § 1805(c)(2))**

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 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 represent that an individual who has been identified as an officer of that intelligence service is likely to engage in counter-surveillance activity.

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 found to be making preparations for counter-surveillance activities 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 a year). We would be pleased to brief Members or staff regarding actual numbers, along with 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 unjustified 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 rapidly address 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.

2. **"Business Records," USA PATRIOT Act Section 215 (codified at 50 U.S.C. § 1861-62)**

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 addresses a gap in intelligence collection authorities 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 target was 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 one of simple 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 2004-2007, the FISA court has issued about 220 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 that did not fall within the scope of any other national security investigative authority (such as a national security letter). Some of these orders were used to support important and highly sensitive intelligence collection operations, of which both Members of the Intelligence Committee and their staffs are aware. 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 and the specific oversight provisions added to the statute in 2006 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. 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 consistent with civil liberties. The absence of such an authority could force the FBI to sacrifice key intelligence opportunities.

3. "Lone Wolf," Intelligence Reform and Terrorism Prevention Act of 2004 Section 6001 (codified at 50 U.S.C. § 1801(b)(1)(C))

Section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004 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 even though the specific foreign power (*i.e.*, the international terrorist group) remains unidentified. We also recommend reauthorizing this provision.

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. However, we do not believe 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. However, this latter group includes legitimate targets that could not be accommodated under the more generic definitions and would 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 effective surveillance. For example, we could have a case in which a known international terrorist affirmatively severed his connection with his group, perhaps following some internal dispute. The target still would be an international terrorist, and an appropriate target for intelligence surveillance. However, the Government could no longer represent to the FISA court that he was currently a member of an international terrorist group or acting on its behalf. Lacking the "lone wolf" definition, the Government could have to postpone FISA surveillance until the target could be linked to another group. Another scenario is the prospect of a terrorist who "self-radicalizes" by means of information and training provided by a variety of international terrorist groups via the Internet. Although this target would have adopted the aims and means of international terrorism, the target would not actually have contacted 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. However, 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 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.

Thank you for the opportunity to present our views. We would be happy to meet with your staff to discuss them. The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to submission of this letter.

Sincerely,

Ronald Weich
Assistant Attorney General

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

September 14, 2009

The Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

Thank you for your letter requesting our recommendations on the three provisions of the Foreign Intelligence Surveillance Act ("FISA") currently scheduled to expire on December 31, 2009. We believe that the best legislation will emerge from a careful examination of these matters. In this letter, we provide our recommendations for each provision, along with a summary of the supporting facts and rationale. We have discussed these issues with the Office of the Director of National Intelligence, which concurs with the views expressed in this letter.

We also are aware that Members of Congress may propose modifications to provide additional protection for the privacy of law abiding Americans. As President Obama said in his speech at the National Archives on May 21, 2009, "We are indeed at war with al Qaeda and its affiliates. We do need to update our institutions to deal with this threat. But we must do so with an abiding confidence in the rule of law and due process; in checks and balances and accountability." Therefore, the Administration is willing to consider such ideas, provided that they do not undermine the effectiveness of these important authorities.

1. Roving Wiretaps, USA PATRIOT Act Section 206 (codified at 50 U.S.C. § 1805(c)(2))

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 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 represent that an individual who has been identified as an officer of that intelligence service is likely to engage in counter-surveillance activity.

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 found to be making preparations for counter-surveillance activities 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 a year). We would be pleased to brief Members or staff regarding actual numbers, along with 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 unjustified 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 rapidly address 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.

2. "Business Records," USA PATRIOT Act Section 215 (codified at 50 U.S.C. § 1861-62)

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 addresses a gap in intelligence collection authorities 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 target was 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 one of simple 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 2004-2007, the FISA court has issued about 220 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 that did not fall within the scope of any other national security investigative authority (such as a national security letter). Some of these orders were used to support important and highly sensitive intelligence collection operations, of which both Members of the Intelligence Committee and their staffs are aware. 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 and the specific oversight provisions added to the statute in 2006 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. 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 consistent with civil liberties. The absence of such an authority could force the FBI to sacrifice key intelligence opportunities.

3. "Lone Wolf," Intelligence Reform and Terrorism Prevention Act of 2004 Section 6001 (codified at 50 U.S.C. § 1801(b)(1)(C))

Section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004 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 even though the specific foreign power (*i.e.*, the international terrorist group) remains unidentified. We also recommend reauthorizing this provision.

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. However, we do not believe 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. However, this latter group includes legitimate targets that could not be accommodated under the more generic definitions and would 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 effective surveillance. For example, we could have a case in which a known international terrorist affirmatively severed his connection with his group, perhaps following some internal dispute. The target still would be an international terrorist, and an appropriate target for intelligence surveillance. However, the Government could no longer represent to the FISA court that he was currently a member of an international terrorist group or acting on its behalf. Lacking the "lone wolf" definition, the Government could have to postpone FISA surveillance until the target could be linked to another group. Another scenario is the prospect of a terrorist who "self-radicalizes" by means of information and training provided by a variety of international terrorist groups via the Internet. Although this target would have adopted the aims and means of international terrorism, the target would not actually have contacted 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. However, 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 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.

Thank you for the opportunity to present our views. We would be happy to meet with your staff to discuss them. The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to submission of this letter.

Sincerely,

Ronald Weich
Assistant Attorney General

cc: The Honorable Jeff Sessions
Ranking Minority Member

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, DC

April 30, 2010

The Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

The Honorable Dianne Feinstein
Chairman
Select Committee on Intelligence
United States Senate
Washington, D.C. 20510

The Honorable John Conyers, Jr.
Chairman
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Silvestre Reyes
Chairman
Permanent Select Committee on Intelligence
U.S. House of Representatives
Washington, D.C. 20515

Dear Madam and Messrs. Chairmen:

This report is submitted pursuant to sections 107 and 502 of the Foreign Intelligence Surveillance Act of 1978 (the "Act"), as amended, 50 U.S.C. § 1801 *et seq.*, and section 118 of USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177 (2006). In accordance with those provisions, this report covers all applications made by the Government during calendar year 2009 for authority to conduct electronic surveillance for foreign intelligence purposes under the Act, all applications made by the Government during calendar year 2009 for access to certain business records (including the production of tangible things) for foreign intelligence purposes, and certain requests made by the Federal Bureau of Investigation pursuant to national security letter authorities. In addition, while not required to do so by statute, the Government is providing information concerning the number of applications made during calendar year 2009 for authority to conduct physical searches for foreign intelligence purposes.

Applications for Electronic Surveillance Made During Calendar Year 2009
(section 107 of the Act, 50 U.S.C. § 1807)

During calendar year 2009, the Government made 1,376 applications to the Foreign Intelligence Surveillance Court (hereinafter "FISC") for authority to conduct electronic surveillance and physical searches for foreign intelligence purposes. The 1,376 applications include applications made solely for electronic surveillance, applications

made solely for physical search, and combined applications requesting authority for electronic surveillance and physical search. Of these, 1,329 applications included requests for authority to conduct electronic surveillance.

Of these 1,329 applications, eight were withdrawn by the Government. The FISC denied one application in whole, and one in part, and made modifications to the proposed orders in fourteen applications. Thus, the FISC approved collection activity in a total of 1,320 of the applications that included requests for authority to conduct electronic surveillance.

Applications for Access to Certain Business Records (Including the Production of Tangible Things) Made During Calendar Year 2009 (section 502 of the Act, 50 U.S.C. § 1862(c)(1))

During calendar year 2009, the Government made twenty-one applications to the FISC for access to certain business records (including the production of tangible things) for foreign intelligence purposes. The FISC did not deny, in whole or in part, any such application filed by the Government during calendar year 2009. The FISC made modifications to nine proposed orders in applications for access to business records.

Requests Made for Certain Information Concerning Different United States Persons Pursuant to National Security Letter Authorities During Calendar Year 2009 (USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177 (2006))

Pursuant to Section 118 of the USA PATRIOT Improvement and Reauthorization Act, Pub. L. 109-177 (2006), the Department of Justice provides Congress with annual reports regarding requests made by the Federal Bureau of Investigation (FBI) pursuant to the National Security Letter (NSL) authorities provided in 12 U.S.C. § 3414, 15 U.S.C. § 1681u, 15 U.S.C. § 1681v, 18 U.S.C. § 2709, and 50 U.S.C. § 436.

In 2009, the FBI made 14,788 NSL requests (excluding requests for subscriber information only) for information concerning United States persons. These sought information pertaining to 6,114 different United States persons.

We hope this information is helpful. Please do not hesitate to contact this office if you need additional assistance regarding this matter.

Sincerely,

FOR
Ronald Weich
Assistant Attorney General

cc: The Honorable Jeff Sessions
Ranking Minority Member
Senate Committee on the Judiciary

The Honorable Christopher S. Bond
Vice Chairman
Senate Select Committee on Intelligence

The Honorable Lamar S. Smith
Ranking Minority Member
House Committee on the Judiciary

The Honorable Peter Hoekstra
Ranking Minority Member
House Permanent Select Committee on Intelligence

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

April 29, 2011

The Honorable Joseph R. Biden, Jr.
President
United States Senate
Washington, DC 20510

Dear Mr. President:

This report is submitted pursuant to sections 107 and 502 of the Foreign Intelligence Surveillance Act of 1978 (the "Act"), as amended, 50 U.S.C. § 1801 *et seq.*, and section 118 of USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177 (2006). In accordance with those provisions, this report covers all applications made by the Government during calendar year 2010 for authority to conduct electronic surveillance for foreign intelligence purposes under the Act, all applications made by the Government during calendar year 2010 for access to certain business records (including the production of tangible things) for foreign intelligence purposes, and certain requests made by the Federal Bureau of Investigation pursuant to national security letter authorities. In addition, while not required to do so by statute, the Government is providing information concerning the number of applications made during calendar year 2010 for authority to conduct physical searches for foreign intelligence purposes.

Applications Made to the Foreign Intelligence Surveillance Court During Calendar Year 2010 (section 107 of the Act, 50 U.S.C. § 1807)

During calendar year 2010, the Government made 1,579 applications to the Foreign Intelligence Surveillance Court (hereinafter "FISC") for authority to conduct electronic surveillance and/or physical searches for foreign intelligence purposes. The 1,579 applications include applications made solely for electronic surveillance, applications made solely for physical search, and combined applications requesting authority for electronic surveillance and physical search. Of these, 1,511 applications included requests for authority to conduct electronic surveillance.

Of these 1,511 applications, five were withdrawn by the Government. The FISC did not deny any applications in whole, or in part. The FISC made modifications to the proposed orders in fourteen applications. Thus, the FISC approved collection activity in a total of 1,506 of the applications that included requests for authority to conduct electronic surveillance.

Applications for Access to Certain Business Records (Including the Production of Tangible Things) Made During Calendar Year 2010 (section 502 of the Act, 50 U.S.C. § 1862(c)(1))

During calendar year 2010, the Government made 96 applications to the FISC for access to certain business records (including the production of tangible things) for foreign intelligence purposes. The FISC did not deny, in whole or in part, any such application filed by the Government during calendar year 2010. The FISC made modifications to 43 proposed orders in applications for access to business records.

Requests Made for Certain Information Concerning Different United States Persons Pursuant to National Security Letter Authorities During Calendar Year 2010 (USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177 (2006))

Pursuant to Section 118 of the USA PATRIOT Improvement and Reauthorization Act, Pub. L. 109-177 (2006), the Department of Justice provides Congress with annual reports regarding requests made by the Federal Bureau of Investigation (FBI) pursuant to the National Security Letter (NSL) authorities provided in 12 U.S.C. § 3414, 15 U.S.C. § 1681u, 15 U.S.C. § 1681v, 18 U.S.C. § 2709, and 50 U.S.C. § 436.

In 2010, the FBI made 24,287 NSL requests (excluding requests for subscriber information only) for information concerning United States persons. These sought information pertaining to 14,212 different United States persons.

We hope that this information is helpful. Please do not hesitate to contact this office if you would like additional assistance regarding this or any other matter.

Sincerely,

Ronald Weich
Assistant Attorney General

United States Senate
WASHINGTON, DC 20510

September 21, 2011

The Honorable Eric Holder
Attorney General
United States Department of Justice
Washington, D.C. 20530

Dear Attorney General Holder:

As you know, we have been concerned for some time that the U.S. government is relying on secret interpretations of surveillance authorities that – in our judgment – differ significantly from the public's understanding of what is permitted under U.S. law.

We believe that policymakers can have legitimate differences of opinion about what types of domestic surveillance should be permitted, but we also believe that the American people should be able to learn what their government thinks that the law means, so that voters have the ability to ratify or reject decisions that elected officials make on their behalf.

Unfortunately, however, the decision to classify the government's interpretations of the law itself makes an informed debate on this issue impossible. Moreover, the absence of publicly available information about the government's understanding of its authorities increases the risk of the public being misled or misinformed about the official interpretation of public laws.

While we are sure that you would agree that government officials should not describe government authorities in a way that misleads the public, during your tenure Justice Department officials have – on a number of occasions – made what we believe are misleading statements pertaining to the government's interpretation of surveillance law.

The first set of statements that concern us are the repeated claims by Justice Department officials that the government's authority to obtain business records or other 'tangible things' under section 215 of the USA Patriot Act is analogous to the use of a grand jury subpoena. This comparison – which we consider highly misleading – has been made by Justice Department officials on multiple occasions, including in testimony before Congress. As you know, Section 215 authorities are not interpreted in the same way that grand jury subpoena authorities are, and we are concerned that when Justice Department officials suggest that the two authorities are "analogous" they provide the public with a false understanding of how surveillance law is interpreted in practice.

More recently, we were troubled to learn that a Justice Department spokesman stated that "Section 215 [of the Patriot Act] is not a secret law, nor has it been implemented under secret legal opinions by the Justice Department." This statement is also extremely misleading. As the NSA General Counsel testified in July of this year, significant

interpretations of section 215 of the Patriot Act are contained in classified opinions of the Foreign Intelligence Surveillance Court and these opinions – and the legal interpretations they contain – continue to be kept secret. In our judgment, when the government relies on significant interpretations of public statutes that are kept secret from the American public, the government is effectively relying on secret law.

Again, we hope you will agree that misleading statements of this nature are not in the public interest and must be corrected. Americans will eventually and inevitably come to learn about the gap that currently exists between the public's understanding of government surveillance authorities and the official, classified interpretation of these authorities. We believe that the best way to avoid a negative public reaction and an erosion of confidence in US intelligence agencies is to initiate an informed public debate about these authorities today. However, if the executive branch is unwilling to do that, then it is particularly important for government officials to avoid compounding the problem by making misleading statements such as the ones we have described here.

We urge you to correct the public record with regard to these statements, and ensure that everyone who speaks for the Justice Department on this issue is informed enough about it to avoid similarly misleading statements in the future.

Thank you for your attention to this matter.

Sincerely,

Ron Wyden
United States Senator

Mark Udall
United States Senator

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General — *Washington, D.C. 20530*

October 19, 2011

The Honorable Ron Wyden
United States Senate
Washington, D.C. 20510

Dear Senator Wyden:

Thank you for your September 21, 2011 letter to the Attorney General concerning the government's authority to obtain records under section 215 of the USA PATRIOT Act. We are sending an identical response to Senator Mark Udall, who joined in your letter.

As you know, section 215 allows the federal government to apply to the Foreign Intelligence Surveillance Court ("FISA Court") for a court order directing the production of any tangible things for an authorized investigation to protect against international terrorism or clandestine intelligence activities. In order to issue an order, the FISA Court must determine that there are reasonable grounds to believe that: (1) the tangible things sought are relevant to an authorized national security investigation, other than a threat assessment; (2) the investigation is being conducted under Guidelines approved by the Attorney General under Executive Order 12333; and (3) if a U.S. person is the subject of the investigation, the investigation is not being conducted solely on the basis of First Amendment protected activities. In addition, by law, the FISA Court may only require the production of records that can be obtained with a grand jury subpoena or any other court order directing the production of records or tangible things. *See* 50 U.S.C. § 1861(c)(2)(D).

The government has made public that some orders issued by the FISA Court under section 215 have been used to support important and highly sensitive intelligence collection operations, on which members of Congress have been fully and repeatedly briefed. During the last Congress (in December 2009), and in the current Congress (February 2011), the Department of Justice and the Intelligence Community provided a document to the House and Senate intelligence committees to be made available to all members of the House and Senate describing the classified uses of section 215 in detail. The Intelligence and Judiciary Committees have been briefed on these operations multiple times and have had access to copies of the classified FISA Court orders and opinions relevant to the use of section 215 in those matters. In addition, the Department of Justice has provided Congress with classified and unclassified annual and semi-annual written reports on section 215 use, and, over the years, has provided extensive briefings

and testimony on the way this statute has been implemented pursuant to lawful FISA Court orders. Most recently, in connection with the reauthorization of the PATRIOT Act, the Attorney General, the Director of the FBI, and relevant heads of Intelligence Community agencies have all testified or briefed members of Congress on the operation of section 215, in addition to multiple congressional hearings at which other senior Department of Justice and Intelligence Community officials testified and briefed the issue over the past year. Armed with this information, the Congress, on a bipartisan basis and by large majorities, has repeatedly reauthorized section 215. In May 2011, the Senate approved the legislation to reauthorize the statute and two other provisions of the USA PATRIOT Act by a vote of 72-23 and the House voted in favor of the legislation by 250-153.

Against this backdrop, we do not believe the Executive Branch is operating pursuant to "secret law" or "secret opinions of the Department of Justice." Rather, the Intelligence Community is conducting court-authorized intelligence activities pursuant to a public statute, with the knowledge and oversight of Congress and the Intelligence Committees of both Houses. There is also extensive oversight by the Executive Branch, including the Department of Justice and relevant agency General Counsels and Inspectors General, as well as annual and semi-annual reports to Congress as required by law.

To be sure, the FISA Court opinions and orders relevant to the use of section 215 and many other intelligence collection authorities are classified. This is necessary because public disclosure of the activities they discuss would harm national security and impede the effectiveness of the intelligence tools that Congress has authorized. This is true of many other intelligence activities that our government throughout its history has carried out in a classified manner in the interest of national security. Since it is not possible to disclose these activities to the public, Congress established the Senate and House intelligence committees to ensure that Congress is able to perform its proper oversight role on behalf of the American people.

We appreciate and share your interest in an informed public debate on how the government interprets and uses its intelligence collection authorities. However, the Intelligence Community has determined that public disclosure of the classified uses of section 215 would expose sensitive sources and methods to our adversaries and therefore harm national security. As you know, the Attorney General and a senior member of the Intelligence Community testified in June 2011 in a closed hearing before the Senate Select Committee on Intelligence concerning the classified uses of section 215. Their classified testimony addressed in detail the operations carried out under the statute, their legal basis, their importance to national security, and the reasons why neither the operations nor their detailed legal basis can be disclosed publicly. As they explained, the Executive Branch has done everything it can to ensure that the people's elected representatives are fully informed of the intelligence collection operations at issue and how they function.

Finally, with regard to the analogy between section 215 and grand jury subpoenas, as noted above, section 215 expressly provides that the court "may only require the production of a tangible thing if such thing can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things." 50 U.S.C. §1861(c)(2)(D). Grand jury subpoenas do not require the approval of a court but rather may be obtained with the approval of a single prosecutor and may request a wide variety of records; the government is not required to make any showing of relevance to a court before issuing such a subpoena. The records obtained pursuant to a grand jury subpoena may concern the lawful activities of U.S. citizens if those records are relevant to an investigation. A motion to quash a grand jury subpoena will be denied unless there is "no reasonable possibility" that the category of information the government seeks will produce information relevant to the general subject of the grand jury's investigation. In contrast, as discussed above, records collected under Section 215 require approval of an Article III judge sitting on the FISA Court, and the government must make an affirmative showing to that Court that the records are relevant to an authorized national security investigation. Particularly in light of the statutory requirement that a section 215 order may only obtain records that could be obtained via a grand jury subpoena (or court order), we continue to believe that the analogy between section 215 and a grand jury subpoena is apt. This is not to say, of course, that the factual context in which section 215 may be used for classified intelligence collection operations is the same as it is for ordinary criminal matters.

In sum, given the constraints as to what can be discussed in an unclassified setting, we believe that we have been as forthcoming as possible in our discussions of section 215.

Thank you for the opportunity to present our views, and please do not hesitate to contact this office if we can be of further assistance regarding this or any other matter.

Sincerely,

Ronald Welch
Assistant Attorney General

1685352 DA

ONE HUNDRED ELEVENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON THE JUDICIARY

2138 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6216

(202) 225–3951
http://www.house.gov/judiciary

October 5, 2009

The Honorable Eric H. Holder
Attorney General of the United States
U.S. Department of Justice
950 Pennsylvania Ave, NW
Washington, DC 20530

Dear Mr. Attorney General:

As the Committee continues its work concerning the USA Patriot Act and related legislation, several sections of which expire this year, we are writing to ask that the Department of Justice make publicly available additional information on the implementation of the Act. We appreciated the Department's September 22 testimony before the Subcommittee on the Constitution, Civil Rights, and Civil Liberties, in which it expressed the Administration's willingness to work with Congress on Patriot Act proposals to better protect Americans' privacy and civil liberties, and in which it publicly provided important information about the use of the "lone wolf" provision of the Act. In order for Congress to meaningfully consider whether and how to extend the "business records" section of the Act, however, we ask that the Department work to provide additional public information on the use of that provision.

Specifically, at the September 22 hearing, Deputy Assistant Attorney General Hinnen testified that orders under Section 215 of the Act, which authorizes compulsory production of "business records," have been used to obtain "transactional information" to support "important and highly sensitive intelligence collection." He explained that some members of the Subcommittee and cleared staff have received some briefings on this topic, and that additional information could be made available to them "in a classified setting."

We have appreciated the information that has been provided, and fully understand the importance of safeguarding our country's national security secrets. Too often in 2007 and 2008, however, crucial information remained unknown to the pubic and many members of Congress when Congress voted on important surveillance legislation affecting the interests of all Americans. As has also been requested in the Senate, we ask that the Department work to make publicly available additional basic information on the use of Section 215, so that Congress can

more openly and thoroughly consider the future of this authority while fully protecting our national security secrets.

Please contact the Judiciary Committee office, 2138 Rayburn House Office Building, Washington, D.C. 20515 (tel.: 202-225-3951; fax: 202-225-7680) in response to this request. Thank you for your prompt attention to this matter.

Sincerely,

John Conyers, Jr.
Chairman

Jerrold Nadler
Chairman, Subcommittee on the Constitution, Civil Rights and Civil Liberties

Bobby Scott
Chairman, Subcommittee on Crime, Terrorism and Homeland Security

cc: Ron Weich
The Honorable Lamar Smith

TOTAL P.003