JOINT STATEMENT FOR THE RECORD

OF

J. BRADFORD WIEGMANN
DEPUTY ASSISTANT ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

MICHAEL J. ORLANDO
DEPUTY ASSISTANT DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

AND

SUSAN MORGAN
NATIONAL SECURITY AGENCY

BEFORE
THE COMMITTEE ON THE JUDICIARY
U.S. HOUSE OF REPRESENTATIVES

AT A HEARING CONCERNING
OVERSIGHT OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

SEPTEMBER 18, 2019

JOINT STATEMENT FOR THE RECORD

OF

J. BRADFORD WIEGMANN
DEPUTY ASSISTANT ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

MICHAEL J. ORLANDO
DEPUTY ASSISTANT DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

AND

SUSAN MORGAN
NATIONAL SECURITY AGENCY

BEFORE
THE COMMITTEE ON THE JUDICIARY
U.S. HOUSE OF REPRESENTATIVES

AT A HEARING CONCERNING
OVERSIGHT OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

SEPTEMBER 18, 2019

INTRODUCTION

Chairman Nadler, Ranking Member Collins, distinguished members of the Committee, thank you for the opportunity to testify today about four important provisions of the Foreign Intelligence Surveillance Act ("FISA") that will expire at the end of this year unless reauthorized by Congress. As indicated in the Director of National Intelligence's letter to this Committee, the Administration strongly supports permanent reauthorization of these provisions.

Three of the authorities—the roving wiretap, business records, and lone wolf provisions—have been part of FISA for well over a decade and have been renewed by Congress multiple times, most recently in the USA FREEDOM Act of 2015 ("FREEDOM Act"). Before that, these same authorities were reauthorized multiple times between 2005 and 2011, each time following extensive congressional review and deliberation. Each renewal gained bipartisan support.

Two of the authorities, the "roving wiretap" and "business records" provisions, have been part of FISA since 2001. These provisions are important in national security investigations and are comparable to provisions available in ordinary criminal investigations. The roving wiretap

authority enables the Government to continue surveilling a court-approved national security target when the target takes steps to thwart the surveillance. The business records authority allows the Government to collect records, papers, and other documents that are relevant to a national security investigation. The Government has used these important national security authorities judiciously, with the approval of the Foreign Intelligence Surveillance Court ("FISC"), and in the interest of national security.

The "lone wolf" provision was added to FISA in 2004 to close a gap in the Government's ability to surveil a foreign person who is engaged in international terrorism or international proliferation of weapons of mass destruction, but who lacks traditional connections to a terrorist group or other foreign power. Without the authority, the Government could not rely on FISA to respond to those kinds of threats. Although the Government has not used the lone wolf provision to date, it is critical this authority remain in the Government's toolkit for the future, as international terrorist groups increasingly seek to inspire individuals to carry out attacks, without necessarily providing the kind of coordination or support that would authorize traditional FISA surveillance.

The fourth authority—the Call Detail Records ("CDR") provision—permits the targeted collection of telephony metadata but not the content of any communications. Congress added this authority to FISA four years ago in the FREEDOM Act as one of several significant FISA reforms designed to enhance privacy and civil liberties. It replaced the National Security Agency's ("NSA") bulk telephony metadata collection program with a new legal authority whereby the bulk metadata would remain with the telecommunications service providers. As this Committee's 2015 report described, the CDR authority provides a "narrowly-tailored mechanism for the targeted collection of telephone metadata for possible connections between foreign powers or agents of foreign powers and others as part of an authorized investigation to protect against international terrorism." H. Rep. 114-109, at 17 (2015). The FREEDOM Act also permanently banned bulk collection under FISA's business records and pen-trap provisions and under the National Security Letter statutes. As this Committee is aware, the NSA recently discontinued the CDR program for technical and operational reasons. But the CDR program retains the potential to be a source of valuable foreign intelligence information. The CDR program may be needed again in the future, should circumstances change. NSA's careful approach to the program, and the legal obligations imposed by the FREEDOM Act in the form of judicial oversight, legislative oversight, and transparency, support the reauthorization of the CDR program.

We urge the Committee to consider permanently reauthorizing these authorities based not only on the Government's demonstrated record and the importance of the authorities to national security, but also on the significant reforms contained in the FREEDOM Act. These include authorizing the FISC to appoint *amici curiae* to address privacy and civil liberties concerns and enhancing public transparency and reporting requirements under FISA. Four years ago, the FREEDOM Act was passed after extensive oversight and comprehensive hearings, and it was reported out of this Committee with unanimous support. In the wake of repeated reviews and bipartisan authorizations over nearly two decades, the Administration's view is that the time has come for Congress to extend these authorities permanently.

Roving Wiretap

First, Congress should permanently reauthorize the "roving wiretap" provision. The authority outlined in this provision is similar to the roving wiretap authority that has been available since 1986 in criminal investigations, under the Wiretap Act, and which has repeatedly been upheld in the courts.

The "roving wiretap" provision provides the Government an effective tool to use in response to adversaries attempting to thwart detection. To understand the importance of this authority, the Committee must consider how FISA functions in ordinary, non-roving cases, and how roving authority is necessary for targets who try to avoid surveillance. Under both regular and roving FISA authority, the Government's application for a court order must identify the target of the surveillance with particularity and must establish probable cause that the target is a foreign power or an agent of a foreign power. If the Court approves the application, it issues one order to the Government and a "secondary" order to a third-party—such as a telephone company—directing it to assist the Government in conducting the wiretap. *See* 50 U.S.C. § 1805(c)(1-2). The secondary order is necessary because, in most cases, the Government needs the assistance of a company to implement the surveillance. In an ordinary case, if the target switches to a new communications service provider, the Government must submit a new application and obtain a new set of FISA orders. However, where the Government can demonstrate in advance to the FISA Court that the target's actions may have the effect of thwarting surveillance, such as by rapidly and repeatedly changing providers, FISA's roving wiretap provision allows the FISC to issue a generic secondary order that the Government can serve on the new provider to commence surveillance without first going back to the Court. *See* 50 U.S.C. § 1805(c)(2)(B). The Government's probable cause showing that the target is an agent of a foreign power remains the same, and the Government must also demonstrate to the FISC, normally within 10 days of initiating surveillance of the new facility, probable cause that the specific target is using, or is about to use, the new facility. *See* 50 U.S.C. § 1805(c)(3).

The roving wiretap authority has proven to be an important intelligence-gathering tool. The Government has used the authority in a relatively small number of cases each year. Those cases tend to involve highly-trained foreign intelligence officers operating within the United States, or other important investigative targets, including terrorism-related targets, who have shown a propensity to engage in activities deliberately designed to thwart surveillance. Similar authority designed to prevent suspects from thwarting surveillance has been a permanent part of our criminal law for over thirty years, and this provision has been renewed as part of FISA repeatedly since 2001 without controversy or evidence of abuse. It remains an important tool, and we strongly support permanent reauthorization.

Business Records

Second, we also support permanent reauthorization of the so-called "business records" provision, which was enacted as section 215 of the USA PATRIOT Act in 2001. This provision authorizes the Government to apply to the FISC for an order directing the production of business records or other tangible things that are relevant to an authorized national security investigation. It allows the Government to obtain in a national security investigation many of the same types of records

and other tangible things that the Government can obtain through a grand jury subpoena in an ordinary criminal investigation. The Government has used the business records provision to obtain, for example, driver's license records, hotel records, car rental records, apartment leasing records, and the like. An application for such records, and other sensitive records, must come from the FBI Director, Deputy Director, or Executive Assistant Director. *See* 50 U.S.C. § 1861(a)(3).

Importantly, the business records provision contains several statutory safeguards. To obtain a FISC order approving a business records application, the Government must make a showing to the FISC that (1) it is seeking information in an authorized national security investigation conducted pursuant to guidelines approved by the Attorney General; (2) where the investigative target is a U.S. person, the Government has demonstrated that the investigation is not based solely on activities protected by the First Amendment; and (3) the Government must demonstrate that the information sought is relevant to the authorized investigation. *See* 50 U.S.C. § 1861(a)(1-2). The Government must also adhere to Attorney General guidelines and minimization procedures that limit the retention and dissemination of any information collected concerning U.S. persons. *Id.* §§ 1861(a)(2)(A) & (g). Recipients of an order seeking business records also have the opportunity to challenge the legality of the order in court, although, to date, no recipient has done so.

Some criticize the business records provisions as running afoul of the Fourth Amendment because business records orders are not issued under a "probable cause" standard. But an order issued under the business records provision does not authorize the Government to enter premises, or to search for or seize records or other tangible things. Thus, the Fourth Amendment's probable cause standard generally does not apply. Rather, the records the Government is authorized to obtain—pursuant to a FISC order—are similar to those that the Government could obtain in ordinary criminal or civil investigations—without *any* court order in most instances—pursuant to a grand jury subpoena in an ordinary criminal case, or pursuant to an administrative subpoena in a civil case. Like a grand jury subpoena or an administrative subpoena, a business records order merely requires the recipient to identify and produce responsive records or other tangible things.

Critics have also questioned the need for the business records provision in view of the Government's ability to seek similar records pursuant to a grand jury subpoena. But not every national security investigation involves criminal activity; thus, a grand jury subpoena is not always available to the Government. Additionally, business records orders issued by the FISC are often supported by classified information that cannot be disclosed to the grand jury and cannot be declassified without compromising important national security interests. Thus, reauthorization of this provision remains critically important.

To be sure, this authority has generated substantial controversy because it was employed, with FISC approval, to support NSA's bulk telephony metadata collection program. However, that program has been terminated and replaced by the more targeted collection of telephony metadata authorized under the CDR provisions of the FREEDOM Act, as discussed below. The FREEDOM Act permanently banned bulk collection altogether under the business records authority and required the use of a "specific selection term" to justify an application for a

business records order. The law defines "specific selection term" as a term that "specifically identifies a person, account, address, or personal device, or any other specific identifier [that] is used to limit, to the greatest extent reasonably practicable, the scope of tangible things sought, consistent with the purpose for seeking the tangible things." 50 U.S.C. § 1861(k)(4)(A)(i). It does not include terms, or a combination of terms, that are not so limited. *See id.* § 1861(k)(4)(A)(ii). Moreover, the FREEDOM Act provided that the FISC may evaluate the adequacy of minimization procedures issued under the business records provisions, and may require additional, particularized minimization procedures beyond those otherwise required, with regard to the production, retention, or dissemination of certain business records, including requiring the destruction of such records within a reasonable period of time. *See id.* § 1861(g)(3).

The Government has used the business records authority judiciously. On average, between 2015 and 2018, the Government sought and obtained records under this provision less than 76 times per year. The number of business records applications approved has decreased every year since 2012. Many of these investigations seek records that are outside the scope of the National Security Letter statutes, and often a business records order is sought because national security interests preclude the use of less secure criminal authorities, or because there may be no criminal investigation underway. Given the importance of the authority, the absence of any evidence of abuse, and the additional safeguards Congress imposed in 2015, we urge the Committee to support permanent reauthorization of this provision.

Lone Wolf

The third expiring provision is the so-called "lone wolf" provision of FISA. It allows the FISC to authorize surveillance of *non-United States persons* engaged in international terrorism or the international proliferation of weapons of mass destruction, without the need to show that the target is acting on behalf of a particular terrorist group or other foreign power.

The "lone wolf" provision is contained within the definition of an "agent of a foreign power" in FISA. Electronic surveillance under FISA can only be directed at a "foreign power" or "agent of a foreign power," as defined in the statute. *See* 50 U.S.C. § 1804(a)(3)(A). A foreign power under FISA is defined for counterterrorism purposes to include a group engaged in international terrorism. Accordingly, without the lone wolf provision, the Government would need to establish that a terrorism-related surveillance target was an *agent of an international terrorist group*. The lone wolf provision specifies that a foreign individual is also considered an "agent of a foreign power" under FISA if the individual is engaged in international terrorism—even if the individual is not directly connected to a foreign terrorist group.

There are two key points to understand about this provision. First, it applies only to non-U.S. persons (not to American citizens or aliens lawfully admitted for permanent residence), *see* 50 U.S.C. § 1801(b)(1)(C), and second, only when they engage or prepare to engage in "international terrorism," *see id.* § 1801(c). In practice, to establish the probable cause necessary to secure a FISC order under the lone wolf provision, the Government must know a great deal about the target, including the target's purpose and plans for terrorist activity, to satisfy the definition of "international terrorism."

Although the Government has not used the lone wolf authority to date, it fills an important gap in the Government's collection capabilities. The provision allows for the surveillance of a foreign terrorist who might be *inspired by* a foreign group, but who is not technically an agent of that group. For example, the provision would allow for surveillance of a foreign person who has self-radicalized through internet propaganda of a foreign terrorist organization, or a known international terrorist who severs his connection with a terrorist group. The Government's decision not to employ this authority to date does not mean that it should be abandoned. To the contrary, it shows that the Government will use this provision only where necessary and legally available. Terrorist groups like ISIS and al-Qaida actively seek to encourage lone wolf attacks. The continued availability of the lone wolf provision ensures the Government retains the authority to surveil isolated foreign terrorist actors who are inspired, but not directed by, foreign terrorist groups.

Call Detail Records

Finally, as we have explained, in addition to reauthorizing these longstanding provisions of FISA in 2015, the FREEDOM Act banned bulk collection and established a new, narrowly-tailored mechanism for the targeted collection of CDRs from U.S. telecommunications service providers. The new provisions were enacted after comprehensive oversight, including hearings addressing recommendations of a presidentially-appointed group of outside experts and the Privacy and Civil Liberties Oversight Board, which weighed in on the privacy and civil liberties effects of the authorities and their importance to national security.

The CDR provision represents a carefully tailored balance between the interest in individual privacy and the need to protect against the activities of international terrorist groups. In support of an authorized counterterrorism investigation, the CDR authority provides a way for Government investigators, pursuant to a FISC order, to identify contacts of suspected terrorists who may be within the United States. It permits the Government to seek an order from the FISC compelling the production on an ongoing basis of CDR information based on a specific selection term, such as a telephone number. The Government must demonstrate to the FISC that (1) there are reasonable grounds to believe that the data sought is relevant to an authorized counterterrorism investigation; and (2) there is a reasonable, articulable suspicion that the specific selection term is associated with a foreign power or an agent of a foreign power engaged in international terrorism or activities in preparation of international terrorism. *See* 50 U.S.C. § 1861(b)(2)(C). Critically, the provision authorizes the collection of certain metadata associated with telephone calls, such as the originating or terminating telephone number and date and time of a call, but *does not authorize* collecting the content of any communication, the name, address, or financial information of a subscriber or customer, or cell site location or global positioning system information. *See id.* § 1861(k)(3). With FISC approval, the Government may require the production of CDRs two "hops" from the seed term—i.e., the CDR's associated with the initial specific selection term and those associated with the CDRs identified in the initial "hop." *See id.* § 1861(c)(2)(F).

The Government has used this authority responsibly. In 2018, the NSA identified certain technical irregularities in data it received from telecommunications service providers under the CDR provision. Because it was not feasible for NSA to resolve the issue technologically, in May of 2018, NSA began the process of deleting all CDR data that it had received since 2015. Then, after balancing the program's intelligence value, associated costs, and compliance and data integrity concerns caused by the unique complexities of using these company-generated business records for intelligence purposes, NSA suspended the CDR program.

NSA's decision to suspend the CDR program does not mean that Congress should allow the CDR authority to expire. Rather, that decision shows that the Executive Branch is a responsible steward of the authority Congress afforded it, and that the numerous constraints on the Government imposed by the FREEDOM Act, including oversight by the FISC, are demanding and effective. As technology changes, our adversaries' tradecraft and communications habits continue to evolve and adapt. In light of this dynamic environment, the Administration supports reauthorization of the CDR provision so that the Government will retain this potentially valuable tool should it prove useful in the future.

The Administration looks forward to working with this Committee and the rest of the Congress to reauthorize on a permanent basis these important national security provisions.