JAMES M. COLE
DEPUTY ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

GENERAL KEITH B. ALEXANDER
DIRECTOR
NATIONAL SECURITY AGENCY
CHIEF
CENTRAL SECURITY SERVICE

ROBERT S. LITT
GENERAL COUNSEL
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED
"CONTINUED OVERSIGHT OF U.S. GOVERNMENT SURVEILLANCE ACTIVITIES"

PRESENTED
DECEMBER 11, 2013

Joint Statement for the Record
of

James M. Cole
Deputy Attorney General
Department of Justice

General Keith B. Alexander
Director
National Security Agency
Chief
Central Security Service

Robert S. Litt
General Counsel
Office of the Director of National Intelligence

Before the
Committee on the Judiciary
United States Senate

At a Hearing Entitled
"Continued Oversight of United States Government Surveillance Activities"

Presented
December 11, 2013

Thank you for inviting us to continue our discussions with this Committee on our efforts to enhance public confidence in the important intelligence collection programs that have been the subject of unauthorized disclosures since earlier this year: the collection of bulk telephony metadata under the business records provision found in Section 215 of the USA PATRIOT Act, and the targeting of non-U.S. persons overseas under Section 702 of FISA. As we have

emphasized in previous appearances before this and other Committees, we remain committed, as we review any modifications to these authorities, both to protecting privacy and civil liberties in the conduct of our intelligence activities, in a manner consistent with the Constitution, the law and our values, and to ensuring that we continue to have the authorities we need to collect important foreign intelligence to protect the country from terrorism and other threats to national security. We also remain committed to working closely with this Committee as any modifications to these activities are considered.

A key step in promoting greater public confidence in these intelligence activities is to provide greater transparency so that the American people, as well as ordinary citizens around the world, understand what the activities are, how they function, and how they are overseen. As you know, many of the reports appearing in the media concerning the scope of the Government's intelligence collection efforts have been inaccurate, including with respect to the collection carried out under Sections 215 and 702. In response, the Administration has released substantial information since June to increase transparency and public understanding, while also working to ensure that these releases are consistent with national security. We welcome the opportunity to discuss ways to make more information about intelligence activities conducted under FISA available to the public in a meaningful and responsible way. At the same time, we are mindful of the need not to publicly disclose information that our adversaries could exploit to evade surveillance and harm our national security. There is no doubt that the recent unauthorized disclosures about our surveillance capabilities risk causing substantial damage to our national security, and it is essential that we not take steps that will increase that damage.

In keeping with this balance, in June the President directed the Intelligence Community to make as much information about the Section 215 and Section 702 programs available to the public as possible, consistent with the need to protect national security and sensitive sources and methods. Since then, the Director of National Intelligence has declassified and publicly released substantial information in order to facilitate informed public debate about these programs. Among other things, the Government has declassified and disclosed the primary and secondary orders from the FISA Court that describe in detail how the bulk telephony metadata collection program operates and the important restrictions on how the data collected under the program are accessed, retained, and disseminated. The Government has also released two recent FISA Court opinions, as well as an Administration white paper, that articulate in detail the legal authority and rationale for this program. We have also declassified and released to the public several other FISA Court opinions and orders concerning the two programs, including detailed discussions of compliance issues that have arisen during the programs' history and the Government's responses to these incidents. We have declassified and released extensive materials that were provided to the Congress in conjunction with its oversight and reauthorization of these authorities. Finally, just this week we have declassified and released additional materials, including FISA Court opinions relating to a separate program (no longer in operation) to collect certain internet metadata in bulk pursuant to court orders issued under the pen register/trap and trace provision of FISA (Section 402). Our efforts to promote greater transparency through declassification and public release of relevant documents are not yet complete. We will continue our efforts to promote greater transparency through declassification and public release of relevant documents, while carefully protecting information that we cannot responsibly release because of national

security concerns. These efforts are an important means of enhancing public confidence that the Intelligence Community is using its legal authorities appropriately, which has become increasingly important in the wake of confusion, concerns, and misunderstandings caused by the recent and continuing unauthorized disclosures of classified information.

As part of our ongoing efforts to increase transparency, the Director of National Intelligence has also committed to providing annual public reports that include nationwide statistical data on the Intelligence Community's use of certain FISA authorities. Specifically, for each of the following categories of FISA and related authorities, beginning in January 2014 and on an annual basis thereafter, the Intelligence Community will release to the public the total number of orders issued during the prior twelve-month period and the number of targets affected by these orders:

- FISA orders based on probable cause (Titles I and III and Sections 703 and 704 of FISA).
- Directives under Section 702 of FISA.
- FISA Business Records orders (Title V of FISA).
- FISA Pen Register/Trap and Trace orders (Title IV of FISA).
- National Security Letters issued pursuant to 12 U.S.C. § 3414(a)(5), 15 U.S.C. § 1681u(a) and (b), 15 U.S.C. § 1681v, and 18 U.S.C. § 2709.

This information will enable the public to understand how often the Intelligence Community uses these authorities nationwide, how many persons or entities are targeted by these efforts, and how these figures change over time. The Director of National Intelligence has concluded that providing this information on a nationwide basis is an acceptable course in light of the goal of public transparency, without unduly risking national security.

We also understand the concerns that specific companies have expressed as to their ability to inform their customers of how often data is provided to the Government in response to

legal process. In light of those concerns, we have authorized companies to report within certain ranges the total number of federal, state, and local law enforcement and national security legal demands they receive on a nationwide basis, and the number of user accounts affected by such orders. This allows companies to illustrate that those demands affect only a tiny percentage of their users, even taking all of the demands together, and thus to refute inaccurate reports that companies cooperate with the Government in dragnet surveillance of all of their customers. At the same time, this approach avoids the disclosure of information to our adversaries regarding the extent or existence of FISA coverage of services or communications platforms provided by particular companies.

The scope of the voluntary disclosures by the Executive Branch concerning sensitive intelligence collection activities carried out under FISA is unprecedented. We hope that the information we have released, and will continue to release, will allow the public to understand better how our intelligence collection authorities are used. We also hope the public will appreciate the rigorous oversight conducted by all three branches of government over our intelligence activities, a whole of government approach that is unique and exacting in comparison to the many governments that conduct similar intercept programs with substantially less stringent oversight. The extensive oversight that we conduct helps to ensure that our activities protect national security, balance important privacy considerations, and operate lawfully.

In addition to the unprecedented steps we have taken to promote transparency, we are open to working with Congress on legislation designed to increase public confidence in these intelligence activities and enhance the protection of privacy and civil liberties. Regarding

Section 215, we would consider statutory restrictions on querying the data that are compatible with operational needs, including perhaps greater limits on contact chaining than what the current FISA Court orders permit. We could also consider a different approach to retention periods for the data—consistent with operational needs—and enhanced statutory oversight and transparency measures, such as annual reporting on the number of identifiers used to query the data. To be clear, we believe the manner in which the bulk telephony metadata collection program has been carried out is lawful, and existing oversight mechanisms protect both privacy and security. However, there are some changes that we believe could be made that would enhance privacy and civil liberties as well as public confidence in the program, consistent with our national security needs.

On the issue of FISA Court reform, we believe that the *ex parte* nature of proceedings before the FISA Court is fundamentally sound and has worked well for decades in adjudicating the Government's applications for authority to conduct electronic surveillance or physical searches in the national security context under FISA. However, we understand the concerns that have been raised about the lack of independent views in certain cases, such as cases involving bulk collection, that affect the privacy and civil liberties interests of the American people as a whole.

Therefore, we would be open to discussing legislation authorizing the FISA Court to appoint an *amicus*, at its discretion, in appropriate cases, such as those that present novel and significant questions of law and that involve the acquisition and retention of information concerning a substantial number of U.S. persons. Establishing a mechanism whereby the FISA Court could solicit independent views of an *amicus* in cases that raise broader privacy and civil

liberties questions, but without compromising classified information, may further assist the Court in making informed and balanced decisions and may also serve to enhance public confidence in the FISA Court process.

While we remain open to working with Congress to effectuate meaningful reforms along the lines just described, we do not support legislation that would have the effect of ending the Section 215 program, which the Government continues to find valuable in protecting national security. And, while we support increased transparency, we do not support legislation that would require or permit public reporting of information concerning intelligence activities under FISA that could be used by our adversaries to evade surveillance, or which otherwise raises practical and operational concerns. The bill approved by the Senate Intelligence Committee includes a number of constructive provisions that we support and that we think will enhance protections for privacy and civil liberties without harming national security.

Finally, we want to address the Committee's interest in the legal standard for collection of records under Section 215. As the Administration explained in a white paper that it published in August, the telephony metadata program satisfies the statutory requirement that there be "reasonable grounds to believe" that the records collected are "relevant to an authorized investigation . . . to obtain foreign intelligence information . . . or to protect against international terrorist or clandestine intelligence activities." The text of Section 215, considered in light of the well-developed understanding of "relevance" in the context of civil discovery and criminal and administrative subpoenas, as well as the broader purposes of the statute, indicates that there are "reasonable grounds to believe" that the records at issue here are "relevant to an authorized investigation." Specifically, in the circumstance where the Government has reason to believe

that conducting a search of a broad collection of telephony metadata records will produce counterterrorism information—and that it is necessary to collect a large volume of data in order to employ the analytic tools needed to identify that information—the standard of relevance under Section 215 is satisfied, particularly in light of the strict limitations on the use of the data collected and the extensive oversight of the program.

As noted above, two decisions of the FISA Court that have recently been declassified by the Government and released publicly by the Court explain why the collection of telephony metadata in bulk is constitutional and is authorized under the statute. These opinions reflect the independent conclusions of two federal judges serving on the FISA Court that the Government's request for the production of call detail records under Section 215 meets the relevance standard and all other statutory requirements. Moreover, these opinions conclude that because the Government seeks only the production of telephony metadata, and not the content of communications, there are no Fourth Amendment impediments to the collection. Indeed, 15 separate judges of the FISA Court have held on 35 occasions that Section 215 authorizes the collection of telephony metadata in bulk in support of counterterrorism investigations. Last week, a district court in a criminal case in California also held that the collection of telephony metadata in bulk under Section 215 is consistent with the Fourth Amendment.

We appreciate that privacy concerns persist about the telephony metadata collection program, even considering the limited data the Government receives, the stringent constraints set by the FISA Court on how it is used, and the aforementioned legal rulings that have consistently upheld its legality. But we hope you will weigh those concerns against the increased risks to national security if this capability were terminated with no equivalent program that addresses

what the 9/11 Commission pointed out as a critical gap in the ability of the intelligence community to detect and "connect the dots" for foreign terror plots against our homeland. This program fills a significant gap in our ability to identify terrorist communications and, together with other authorities, can help us identify and disrupt terrorist plots, thus fulfilling the vision of the 9/11 Commission, which implored the Government to undertake mechanisms and collaboration which would prevent the recurrence of another 9/11.

We look forward to answering any questions you might have about these important intelligence collection programs and related issues. We understand that there are a variety of views in the Congress and among the American people about these activities, and we look forward to discussing these issues with this Committee as new legislation concerning these activities is considered. We hope that, with the assistance of this Committee, we can ensure that these programs are on the strongest possible footing, from the perspective of both national security and privacy, so that they will continue to enjoy Congressional support in the future. Thank you.