Department of Justice

STATEMENT

OF

STEVEN G. BRADBURY
PRINCIPAL DEPUTY ASSISTANT ATTORNEY GENERAL
OFFICE OF LEGAL COUNSEL
DEPARTMENT OF JUSTICE

BEFORE THE
SUBCOMMITTEE ON THE CONSTITUTION,
CIVIL RIGHTS, AND CIVIL LIBERTIES
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

CONCERNING
THE TERRORIST SURVEILLANCE PROGRAM AND
THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)

PRESENTED ON
JUNE 7, 2007

STATEMENT

OF

STEVEN G. BRADBURY
PRINCIPAL DEPUTY ASSISTANT ATTORNEY GENERAL
OFFICE OF LEGAL COUNSEL
DEPARTMENT OF JUSTICE

BEFORE THE
SUBCOMMITTEE ON THE CONSTITUTION,
CIVIL RIGHTS, AND CIVIL LIBERTIES
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

CONCERNING
THE TERRORIST SURVEILLANCE PROGRAM AND
THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)

PRESENTED ON
JUNE 7, 2007

Thank you, Chairman Nadler, Ranking Member Franks, and Members of the Subcommittee. I appreciate the opportunity to appear here today to discuss the President's constitutional authority to conduct electronic surveillance and how this authority relates to the Terrorist Surveillance Program and the Foreign Intelligence Surveillance Act ("FISA").

It has been almost six years since the attacks of September 11, 2001, the single deadliest set of foreign attacks on U.S. soil in our Nation's history. Nevertheless, we continue to confront a determined and deadly enemy that is fully committed to launching additional catastrophic attacks against and within the United States. Al Qaeda continues to demonstrate its ability to execute mass attacks as evidenced by, among other things, bombings in Bali, Madrid, London, and Iraq. We and our allies also have narrowly

averted additional attacks, some of which are public knowledge and others of which must remain classified.

In the wake of the attacks of September 11th, the President authorized the Terrorist Surveillance Program in order to establish an early-warning system to detect and prevent further terrorist attacks against the United States. As described by the President, under that Program the NSA targeted for interception international communications into and out of the United States where there was probable cause to believe that at least one party to the communication was a member or agent of al Qaeda or an associated terrorist organization. Highly trained intelligence professionals made the initial decision to target communications for interception, subject to rigorous oversight by attorneys and officials at the NSA. The Terrorist Surveillance Program was subject to unprecedented scrutiny by the NSA itself, as well as oversight by other parts of the Executive Branch, including the Department of Justice. In addition, the Program required reauthorization by the President every 45 days to ensure that it was still necessary and that it complied with the Constitution. Key Members of Congress were briefed on the Program from its inception, and it was subsequently briefed to the full membership of both intelligence committees.

In the spring of 2005—well before the first press accounts disclosing the existence of the Terrorist Surveillance Program—the Administration began exploring options for seeking authorization for the Program from the Foreign Intelligence Surveillance Court ("FISC"). Any court authorization had to ensure that the Intelligence Community would be able to operate with the speed and agility necessary to protect the United States from al Qaeda and associated terrorist organizations—the very speed and agility that the Terrorist Surveillance Program afforded to the Intelligence Community.

On January 10, 2007, a judge of the FISC issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that at least one of the participants to the communication is a member or an agent of al Qaeda or an associated terrorist organization. The orders issued by the FISC are innovative and complex; it took considerable time and effort for the Government to develop a sound approach that could be proposed to, and approved by, the FISC. The Attorney General recently explained that as a result of these orders, any electronic surveillance that was occurring as part of the Terrorist Surveillance Program is now subject to the approval of the FISC. Under these circumstances, the President determined not to reauthorize the Terrorist Surveillance Program when the last authorization expired. Accordingly, the Program is no longer operational.

Nevertheless, I wish to emphasize that the President had ample authority to authorize the Terrorist Surveillance Program under acts of Congress and the Constitution. As explained in greater detail in the Department of Justice's *Legal Authorities Supporting the Activities of the National Security Agency Described by the President* (Jan. 19, 2006) ("*Legal Authorities*"), a copy of which I ask be placed in the record for this hearing, the Authorization for the Use of Military Force ("Force Resolution"), Pub. L. No. 107-40, 115 Stat. 224 (Sept. 18, 2001), authorizes the President to "use all necessary and appropriate force" against those persons, organizations, and nations responsible for the September 11th attacks. A majority of the Supreme Court concluded in *Hamdi v. Rumsfeld* that with these words, Congress authorized the President to undertake all "fundamental and accepted . . . incident[s] to war." 542 U.S. 507, 518 (2004) (plurality opinion); *id.* at 587 (Thomas, J., dissenting). Intercepting the communications of the foreign enemies of the United States has been a fundamental element of warfare since the

Founding. *See Legal Authorities* at 14-17. Therefore, the Force Resolution, as construed by the Supreme Court in *Hamdi* and confirmed by history and tradition, authorized the Executive Branch to operate the Terrorist Surveillance Program. *See Hamdi*, 542 U.S. at 518 (plurality opinion) (Force Resolution satisfies statutory bar on detention of American citizens "except pursuant to an Act of Congress"); *id*. at 587 (Thomas, J., dissenting).

That is so notwithstanding the so-called "exclusive means" provision in section 201(b) of FISA, 18 U.S.C. § 2511(2)(f). The Force Resolution is a "statute" authorizing the conduct of "electronic surveillance" under 50 U.S.C. § 1809(a)(1). *See Legal Authorities* at 10-27. Assuming solely for the purposes of this hearing that the Terrorist Surveillance Program involved "electronic surveillance" as that term is narrowly defined in FISA, the exclusive means provision of FISA did not prohibit the Terrorist Surveillance Program for the reasons carefully stated in greater detail in the Department's *Legal Authorities*. *See id.* at 20-23.

Furthermore, it is well established that the President has constitutional authority to direct the use of electronic surveillance for the purpose of collecting foreign intelligence information without prior judicial approval, even during times of peace. *See, e.g.*, *United States v. Truong Dinh Hung*, 629 F.2d 908, 913-17 (4th Cir. 1980); *United States v. Butenko*, 494 F.2d 593, 602-06 (3d Cir. 1974) (en banc); *United States v. Brown*, 484 F.2d 418, 425-27 (5th Cir. 1973); *United States v. bin Laden*, 126 F. Supp. 2d 264, 271-77 (S.D.N.Y. 2000). Accordingly, the Foreign Intelligence Surveillance Court of Review, the very court Congress established to hear appeals from decisions of the FISC, noted that "all the other courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information." *In re Sealed Case*, 310 F.3d 717, 742 (2002). The Court of Review, therefore, "took for granted that the President does have that constitutional authority." *Id*.

The conclusion that the President has constitutional authority to conduct electronic surveillance without prior judicial approval is even stronger when undertaken to prevent further attacks against and within the United States, *see, e.g.*, *The Prize Cases*, 67 U.S. (2 Black) 635, 668 (1863) ("If a war be made by invasion of a foreign nation, the President is not only authorized but bound to resist force by force. He does not initiate the war, but is bound to accept the challenge without waiting for any special legislative authority."); *Campbell v. Clinton*, 203 F.3d 19, 27 (D.C. Cir. 2000) (noting that "the *Prize Cases* . . . stand for the proposition that the President has independent authority to repel aggressive acts by third parties even without specific congressional authorization") (Silberman, J., concurring), and it is stronger still in the context of an ongoing congressionally authorized armed conflict, *see Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 637 (1952) (Jackson, J., concurring); *Legal Authorities* at 11. Indeed, in the Force Resolution itself, Congress expressly recognized that "the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States." Force Resolution pmbl.

At a minimum, interpreting FISA to prohibit the President from authorizing foreign intelligence surveillance against a diffuse network of foreign terrorist enemies—who already have successfully attacked the United States and who repeatedly have avowed their intention to do so again—without prior judicial approval from the FISC would raise a serious question about the constitutionality of FISA. *See Legal Authorities* at 28-35. FISA must be interpreted, "if fairly possible," to avoid raising these constitutional concerns. *INS v. St. Cyr*, 533 U.S. 289, 299-300 (2001) (citations omitted); *see* William N. Eskridge, Jr., DYNAMIC STATUTORY INTERPRETATION 325 (1994) (describing "[s]uper-strong rule against congressional interference with the President's authority over foreign affairs and national security."). As we have explained, FISA is

best interpreted as allowing the Force Resolution to authorize electronic surveillance outside FISA's express procedures. This interpretation is more than "fairly possible."

Justice Jackson explained more than 50 years ago that separation of powers questions—at least those that actually arise in the real world—rarely admit of simple and unambiguous answers. *See Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 634-35 (1952) (Jackson, J., concurring). Nevertheless, we believe that even if interpreting FISA to allow the Force Resolution to authorize the Program were not "fairly possible," the Program was a lawful exercise of the President's authority under Article II of the Constitution. The Constitution establishes a zone of constitutional authority for the President to direct the exercise of military force against declared foreign enemies. *See Legal Authorities* at 9-10, 30-34. That power includes the authority to direct the collection of signals intelligence from our enemies in order to detect and prevent further attacks against the Nation. *See id.* at 14-17. Acting pursuant to that authority, the President determined that the Terrorist Surveillance Program was necessary to defend the United States against a subsequent catastrophic terrorist attack. *Id.* at 4-5.

A statute, such as FISA, cannot unduly restrict the President's constitutional authority as Commander in Chief to direct the collection of signals intelligence from the Nation's enemies during an ongoing armed conflict. The Supreme Court stated clearly in *Hamdan v. Rumsfeld* that "Congress [cannot intrude] upon the proper authority of the President . . . . Congress cannot direct the conduct of campaigns . . . ." 126 S. Ct. 2749, 2773 (2006) (quoting *Ex Parte Milligan*, 71 U.S. (4 Wall.) 2, 139-40 (1866) (Chase, C.J., concurring in judgment)); *see Legal Authorities* at 10 (the President "has certain powers and duties with which Congress cannot interfere") (quoting *Training of British Flying Students in the United States*, 40 Op. Att'y Gen. 58, 61 (1941) (Attorney General Robert

H. Jackson)); *see also, e.g.*, *Morrison v. Olson*, 487 U.S. 654, 691 (1988) (Congress may not "impede the President's ability to perform his constitutional duty").

In any event, the Terrorist Surveillance Program has not been reauthorized for several months, and any electronic surveillance that was occurring as part of the Program is now subject to the approval of the FISC. It is now imperative that Congress and the Executive Branch shift their focus away from former intelligence programs and cooperate to close critical gaps in our intelligence capabilities under FISA while ensuring proper protections for the civil liberties of U.S. persons.

FISA has been and continues to serve as the foundation for conducting electronic surveillance of foreign powers and agents of foreign powers in the United States. Although FISA is extremely important, it can and must be improved. The most serious problems with the statute stem from the fact that Congress defined the term "electronic surveillance" in a way that depends upon communications technology and practices as they existed in 1978. In 1978, almost all local calls were carried by wire and almost all transoceanic communications into and out of the United States were radio communications carried by satellite. Congress intentionally kept the latter category of communications largely outside the scope of FISA's coverage, consistent with FISA's primary focus of protecting the privacy of U.S. persons in the United States. Congress used the technological means by which communications were transmitted *at that time* as a proxy for the types and locations of targets to which the procedures and safeguards of FISA would apply.

This technology-dependent approach has had dramatic but unintended consequences, sweeping within the scope of FISA a wide range of communications intelligence activities that Congress intended to exclude from the scope of FISA. Since 1978, we have seen a fundamental transformation in the means by which we

communicate. Congress did not anticipate—nor could it have foreseen—the technological revolution that would bring us global high-speed fiber-optic networks, wireless networks, and the Internet. Sheer fortuity in the development and deployment of new communications technologies, rather than a considered judgment by Congress, has resulted in a considerable expansion of the reach of FISA to involve the FISC in approving the conduct of electronic surveillance of foreign persons overseas.

This unintended expansion of FISA's scope has hampered our intelligence capabilities and has caused the Intelligence Community, the Department of Justice, and the FISC to expend precious resources obtaining court approval to conduct intelligence activities directed at foreign persons overseas. The Director of National Intelligence, J. Michael McConnell, testified just last month that due to the outdated structure governing foreign intelligence surveillance, "[w]e are actually missing a significant portion of what we should be getting" from our enemies. Furthermore, resources that could be spent to protect the privacy of U.S. persons in the United States must be diverted to address applications for surveillance of foreign persons located overseas.

To rectify these problems, the Administration has proposed comprehensive amendments to FISA that would make the statute technology neutral, enhance the Government's authority to secure assistance from private entities in conducting lawful foreign intelligence surveillance activities, and streamline the application and approval process before the FISC. The Administration's proposal would revise the definition of "electronic surveillance," such that FISA's scope would turn upon the subject of the surveillance and the subject's location (inside the United States or abroad), rather than substantively irrelevant criteria, such as the means by which a communication is transmitted or the location where the Government intercepts the communication. A technology-neutral statute would prevent the unintended expansion of FISA and would

provide an enduring and stable framework for the Intelligence Community to conduct foreign intelligence surveillance activities notwithstanding future revolutions in telecommunications technologies.

Privacy and security are not mutually exclusive: By modernizing FISA, we can both provide the Intelligence Community with an enduring, agile, and efficient means of collecting critical foreign intelligence information and strengthen the privacy protections for U.S. persons in the United States. Reinstating FISA's original carve-out for certain foreign intelligence activities conducted against foreign persons overseas would provide the Intelligence Community with the speed and agility necessary to detect and prevent terrorist attacks mounted by a diffuse and flexible network of foreign terrorist organizations. In combination with other proposed amendments to FISA, redefining "electronic surveillance" also would help to restore the focus of FISA on protecting the privacy of U.S. persons in the United States. And it would enable the FISC and the Executive Branch to allocate scarce resources to those applications for the conduct of electronic surveillance that directly implicate the core concern of FISA: protecting the privacy of U.S. persons in the United States.

* * *

Again, Mr. Chairman, thank you for the opportunity to appear today to discuss these important issues. Given the determined and deadly adversary that we continue to face, it is important that Congress and the Executive Branch cooperate to protect the Nation from further terrorist attacks while preserving the civil liberties of all Americans. We look forward to working with Congress to meet those objectives.

# # #