

Subject: FW: TPs, Long Letter, & Short Letter
From: "Kelley, William K."
Date: 12/21/05, 4:14 PM
To: "Kavanaugh, Brett M."
CC: "Miers, Harriet"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 15 11:27:13 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: FW: TPs, Long Letter, & Short Letter
From: "Kavanaugh, Brett M."
Date: 12/21/05, 4:18 PM
To: "Staff Secretary"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 15 11:27:14 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: NSA Staffing comment
From: "Kelley, William K."
Date: 12/21/05, 7:29 PM
To: "Kavanaugh, Brett M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 15 11:27:16 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: New Version of NSA Talkers
From: "Kelley, William K."
Date: 12/21/05, 8:43 PM
To: "Kavanaugh, Brett M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 15 11:27:17 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: NSA Setting the record straight

From: "McDonald, Matthew T."

Date: 12/21/05, 8:57 PM

To: "McClellan, Scott", "Wallace, Nicolle", "Kavanaugh, Brett M.", "Davis, Michele A."

CC: "Sherzer, David", "Carleton, Nathan L.", "Pounder, Joseph S."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 15 11:27:20 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: FW: NSA Setting the record straight
From: "Kavanaugh, Brett M."
Date: 12/21/05, 9:31 PM
To: "Kelley, William K.", "Miers, Harriet"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 15 11:27:21 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: NSA Setting the record straight
From: "Miers, Harriet"
Date: 12/21/05, 9:42 PM
To: "Kavanaugh, Brett M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 15 11:27:22 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: FW: NSA Setting the record straight
From: "Kavanaugh, Brett M."
Date: 12/21/05, 9:48 PM
To: "McDonald, Matthew T."
CC: "Sherzer, David"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 15 11:27:23 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: FW: NSA Setting the record straight
From: "Sherzer, David"
Date: 12/21/05, 9:51 PM
To: "Kavanaugh, Brett M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 15 11:27:25 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: NSA Setting the record straight

From: "Wallace, Nicolle"

Date: 12/21/05, 10:20 PM

To: "McDonald, Matthew T.", "McClellan, Scott", "Kavanaugh, Brett M.", "Davis, Michele A."

CC: "Sherzer, David", "Carleton, Nathan L.", "Pounder, Joseph S."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 15 11:22:34 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: FW: NSA Setting the record straight
From: "Kavanaugh, Brett M."
Date: 12/21/05, 10:24 PM
To: "Wallace, Nicolle"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 15 11:22:36 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: NSA Setting the record straight

From: "McDonald, Matthew T."

Date: 12/21/05, 10:28 PM

To: "Wallace, Nicolle", "McClellan, Scott", "Kavanaugh, Brett M.", "Davis, Michele A.", "Kelley, William K.", "Miers, Harriet"

CC: "Sherzer, David", "Carleton, Nathan L.", "Pounder, Joseph S."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 15 11:22:38 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: NSA Setting the record straight
From: "Kavanaugh, Brett M."
Date: 12/21/05, 10:55 PM
To: "McDonald, Matthew T."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 15 11:22:41 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

From: "Kelley, William K."
Date: 12/21/05, 11:00 PM
To: "Kavanaugh, Brett M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 15 11:22:41 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

b(6),P6,P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Here were talkers ...

Subject: Here were talkers ...
From: "Kavanaugh, Brett M."
Date: 12/22/05, 12:05 AM
To: "Miers, Harriet"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Thu Apr 04 15:59:46 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: Fw: Final letter and talkers
From: "Kavanaugh, Brett M."
Date: 12/22/05, 2:51 AM
To: "Miers, Harriet", "Kelley, William K."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Dec 10 11:07:06 EST 2018

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0242-F

Additional Information:

Subject: FW: NSA legal authority talking points

From: "Kelley, William K."

Date: 12/22/05, 10:06 PM

To: "Wallace, Nicolle", "Rove, Karl C.", "Bartlett, Dan", "Kavanaugh, Brett M.", "McClellan, Scott", "Wehner, Peter H."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Thu Apr 04 16:28:33 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: NSA Setting the record straight

From: "McDonald, Matthew T."

Date: 1/4/06, 4:36 PM

To: "McDonald, Matthew T.", "Wallace, Nicolle", "McClellan, Scott", "Kavanaugh, Brett M.", "Davis, Michele A.", "Kelley, William K.", "Miers, Harriet"

CC: "Sherzer, David", "Carleton, Nathan L.", "Pounder, Joseph S."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 01 12:42:01 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: Re: NSA Setting the record straight

From: "Wallace, Nicolle"

Date: 1/4/06, 4:50 PM

To: "McDonald, Matthew T.", "McClellan, Scott", "Kavanaugh, Brett M.", "Davis, Michele A.", "Kelley, William K.", "Miers, Harriet"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 01 12:42:02 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: NSA Setting the record straight
From: "Sherzer, David"
Date: 1/4/06, 4:54 PM
To: "McDonald, Matthew T."
CC: "Kavanaugh, Brett M.", "Sherzer, David"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 01 12:42:03 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: Re: NSA Setting the record straight

From: "Wallace, Nicolle"

Date: 1/4/06, 4:56 PM

To: "McDonald, Matthew T.", "McClellan, Scott", "Kavanaugh, Brett M.", "Davis, Michele A.", "Kelley, William K.", "Miers, Harriet"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 01 12:42:04 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: NSA Setting the record straight

From: "McDonald, Matthew T."

Date: 1/4/06, 5:41 PM

To: "Wallace, Nicolle", "McClellan, Scott", "Kavanaugh, Brett M.", "Davis, Michele A.", "Kelley, William K.", "Miers, Harriet"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 01 12:42:06 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: Re: NSA Setting the record straight

From: "Kelley, William K."

Date: 1/4/06, 5:49 PM

To: "McDonald, Matthew T.", "Wallace, Nicolle", "McClellan, Scott", "Kavanaugh, Brett M.", "Davis, Michele A.", "Miers, Harriet"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 01 12:42:07 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: NSA Setting the record straight

From: "Miers, Harriet"

Date: 1/4/06, 6:02 PM

To: "Kelley, William K.", "McDonald, Matthew T.", "Wallace, Nicolle", "McClellan, Scott", "Kavanaugh, Brett M.", "Davis, Michele A."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 01 12:42:09 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: NSA Setting the record straight

From: "McDonald, Matthew T."

Date: 1/4/06, 6:08 PM

To: "Miers, Harriet", "Kelley, William K.", "Wallace, Nicolle", "McClellan, Scott", "Kavanaugh, Brett M.", "Davis, Michele A."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 01 12:42:10 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: NSA Setting the record straight

From: "Miers, Harriet"

Date: 1/4/06, 6:15 PM

To: "McDonald, Matthew T.", "Kelley, William K.", "Wallace, Nicolle", "McClellan, Scott", "Kavanaugh, Brett M.", "Davis, Michele A."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 01 12:42:11 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: FINAL
From: "McDonald, Matthew T."
Date: 1/4/06, 6:15 PM
To: "Kavanaugh, Brett M.", "Sherzer, David"

— Attachments: —

1.4.06 STRS NSA.doc

99.5 KB

Setting The Record Straight:

Critics Launch Attacks Against Program To Detect And Prevent Terrorist Attacks

"Critics have stepped up their attacks on the President for authorizing the National Security Agency to listen to international communications of known al Qaeda members or affiliated terrorists during a time of war. The American people expect their leaders to stay a step ahead of the enemy, and the National Security Agency authorization is a critical tool in the War on Terror that saves lives and protects civil liberties at the same time."

- Scott McClellan, White House Press Secretary

Setting The Record Straight On Separate NSA Activities To Safeguard Americans.

Representative Nancy Pelosi (D-CA) Expresses Concern That The NSA Was Conducting Surveillance Without Presidential Authority In The Aftermath Of 9/11. "During your appearance before the committee on October 1, you indicated that you had been operating since the September 11 attacks with an expansive view of your authorities with respect to the conduct of electronic surveillance under the Foreign Intelligence Surveillance Act and related statutes, orders, regulations, and guidelines. ... Therefore, I am concerned whether, and to what extent, the National Security Agency has received specific presidential authorization for the operations you are conducting. Until I understand better the legal analysis regarding the sufficiency of the authority which underlies your decision on the appropriate way to proceed on this matter, I will continue to be concerned." (Rep. Nancy Pelosi, Letter To Lieutenant General Michael V. Hayden, 10/11/01)

But These Were Separate NSA Activities Based On Previously Granted Authority.

- **General Hayden Was Briefing On The NSA's Electronic Surveillance Activities, Not The Program Authorized By The President.** "An intelligence official close to Hayden said that his appearance on Oct. 1, 2001, before the House committee had been to discuss Executive Order 12333, and not the new NSA program. The order, signed by President Ronald Reagan in 1981, gave guidance and specific instructions about the intelligence activities that the U.S. government could engage in." (Dafna Linzer, "Secret Surveillance May Have Occurred Before Authorization," *The Washington Post*, 1/4/06)
- **These NSA Actions Had Been Authorized Since 1981.** "Bush administration officials said on Tuesday that General Hayden, now the country's No. 2 intelligence official, had acted on the authority previously granted to the N.S.A., relying on an intelligence directive known as Executive Order 12333, issued by President Ronald Reagan in 1981. That order set guidelines for the collection of intelligence, including by the N.S.A. 'He had authority under E.O. 12333 that had been given to him, and he briefed Congress on what he did under those authorities,' said Judith A. Emmel, a spokeswoman for the Office of the Director of National Intelligence. 'Beyond that, we can't get into details of what was done.'" (Eric Lichtblau And Scott Shane, "Files Say Agency Initiated Growth of Spying Effort," *The New York Times*, 1/4/06)

Setting The Record Straight On The Terrorist Ties Of Intercepted Communications.

Senator Dick Durbin (D-IL) Says The National Security Agency (NSA) Is Eavesdropping On American Citizens With No "Indication Of Wrongdoing." SEN. DURBIN: "And in passing the Patriot Act, we gave the government new authority, but we didn't give the National Security Agency the authority to spy on American citizens without any indication of wrongdoing." (CBS' "Early Show," 12/17/05)

But The NSA Authorization Is Solely For Intercepting Communications Of Suspected Al Qaeda Members Or Related Terrorist Groups.

- **Ranking Democrat On The House Intelligence Committee Representative Jane Harman (D-CA) Calls The NSA Program "Essential" To Targeting Al Qaeda.** "As the Ranking Democrat on the House Intelligence Committee, I have been briefed since 2003 on a highly classified NSA foreign collection program that targeted Al Qaeda. I believe the program is essential to US national security and that its disclosure has damaged critical intelligence capabilities." (Rep. Jane Harman, Harman Statement On NSA Electronic Surveillance Program, Press Release, 12/21/05)
- **The Program Targets Suspected "Al Qaeda Communications."** DEPUTY DIRECTOR OF NATIONAL INTELLIGENCE GENERAL MICHAEL HAYDEN: "Again, I make the point, what we are talking about here are communications we have every reason to believe are al Qaeda communications, one end of which is in the United States. And I don't think any of us would want any inefficiencies in our coverage of those kinds of communications, above all. And that's what this program allows us to do – it allows us to be as agile as operationally required to cover these targets." (The White House, Press Briefing, 12/19/05)
- **The Government Has "A Reasonable Basis To Conclude That One Party To The Communication" Is Affiliated With Al Qaeda.** ATTORNEY GENERAL ALBERTO GONZALES: "Another very important point to remember is that we have to have a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda. We view these authorities as authorities to confront the enemy in which the United States is at war with – and that is al Qaeda and those who are supporting or affiliated with al Qaeda. What we're trying to do is learn of communications, back and forth, from within the United States to overseas with members of al Qaeda. And that's what this program is about." (The White House, Press Briefing, 12/19/05)

Setting The Record Straight On The Scope Of The Program.

Senator Robert Byrd (D-WV) Says The NSA Is Conducting Domestic Surveillance Of Calls. "He has rationalized the use of domestic, civilian surveillance with a flimsy claim that he has such authority because we are at war." (Sen. Byrd, "No President Is Above The Law," Press Release, 12/19/05)

But The NSA Authorization Is Solely For Intercepting International Calls.

- **One Party On The Call Has To Be Outside The United States.** ATTORNEY GENERAL GONZALES: "The President has authorized a program to engage in electronic surveillance of a particular kind, and this would be the intercepts of contents of communications where one of the – one party to the communication is outside the United States. And this is a very important point –

people are running around saying that the United States is somehow spying on American citizens calling their neighbors. Very, very important to understand that one party to the communication has to be outside the United States." (The White House, Press Briefing, 12/19/05)

Setting The Record Straight On The Use Of The FISA Court.

Senator Joe Biden (D-DE) Says The Administration Should Be Using The FISA Court. "There is nothing the president needed to do to protect Americans that could not have been done through FISA. Since 1979, the FISA court has received some 19,000 requests and approved all but five of them. The administration's assertion that it needed to bypass the court is out of bounds." (Sen. Joseph Biden, Op-Ed, "No President Is Above Our Constitution," *The Miami Herald*, 1/1/06)

But The Program Provides The Speed And Agility Needed To Prosecute The War On Terror.

- **The Government Continues To Use The FISA Court But Must Preserve The Flexibility To Act With Speed In All Circumstances.** ATTORNEY GENERAL ALBERTO GONZALES: "Well, we continue to go to the FISA court and obtain orders. It is a very important tool that we continue to utilize. ... The operators out at NSA tell me that we don't have the speed and the agility that we need, in all circumstances, to deal with this new kind of enemy. You have to remember that FISA was passed by the Congress in 1978. There have been tremendous advances in technology ... since then." (The White House, Press Briefing, 12/19/05)
- **Because Of Its Speed, The NSA Program Has Provided Crucial Information Otherwise Not Available.** GENERAL HAYDEN: "I can say unequivocally, all right, that we have got information through this program that would not otherwise have been available." QUESTION: "Through the court? Because of the speed that you got it?" GENERAL HAYDEN: "Yes, because of the speed, because of the procedures, because of the processes and requirements set up in the FISA process, I can say unequivocally that we have used this program in lieu of that and this program has been successful." (The White House, Press Briefing, 12/19/05)
- **Former Clinton Administration Associate Attorney General Writes That "FISA Does Not Anticipate A Post-Sept. 11 Situation."** "The administration has offered the further defense that FISA's reference to surveillance 'authorized by statute' is satisfied by congressional passage of the post-Sept. 11 resolution giving the president authority to 'use all necessary and appropriate force' to prevent those responsible for Sept. 11 from carrying out further attacks. The administration argues that obtaining intelligence is a necessary and expected component of any military or other use of force to prevent enemy action. But even if the NSA activity is 'electronic surveillance' and the Sept. 11 resolution is not 'statutory authorization' within the meaning of FISA, the act still cannot, in the words of the 2002 Court of Review decision, 'encroach upon the president's constitutional power.' FISA does not anticipate a post-Sept. 11 situation. What was needed after Sept. 11, according to the president, was surveillance beyond what could be authorized under that kind of individualized case-by-case judgment. It is hard to imagine the Supreme Court second-guessing that presidential judgment." (John Schmidt, Op-Ed, "President Had Legal Authority To OK Taps," *The Chicago Tribune*, 12/21/05)

Subject: RE: NSA Setting the record straight

From: "Miers, Harriet"

Date: 1/4/06, 6:16 PM

To: "McDonald, Matthew T.", "Kelley, William K.", "Wallace, Nicolle", "McClellan, Scott", "Kavanaugh, Brett M.", "Davis, Michele A."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 01 12:42:13 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: NSA Setting the record straight

From: "McDonald, Matthew T."

Date: 1/4/06, 6:19 PM

To: "Miers, Harriet", "Kelley, William K.", "Wallace, Nicole", "McClellan, Scott", "Kavanaugh, Brett M.", "Davis, Michele A."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Tue Apr 02 15:14:44 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: NSA Setting the record straight

From: "McDonald, Matthew T."

Date: 1/4/06, 6:53 PM

To: "Miers, Harriet", "Kelley, William K.", "Wallace, Nicole", "McClellan, Scott", "Kavanaugh, Brett M.", "Davis, Michele A."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Tue Apr 02 15:14:46 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: FINAL: NSA Setting the record straight

From: "McDonald, Matthew T."

Date: 1/4/06, 7:28 PM

To: "Miers, Harriet", "Kelley, William K.", "Wallace, Nicolle", "McClellan, Scott", "Kavanaugh, Brett M.", "Davis, Michele A."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Tue Apr 02 15:14:47 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: FINAL: NSA Setting the record straight

From: "McClellan, Scott"

Date: 1/4/06, 7:56 PM

To: "McDonald, Matthew T.", "Miers, Harriet", "Kelley, William K.", "Wallace, Nicolle", "Kavanaugh, Brett M.", "Davis, Michele A."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Tue Apr 02 15:14:48 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: FINAL: NSA Setting the record straight

From: "McDonald, Matthew T."

Date: 1/4/06, 7:58 PM

To: "McClellan, Scott", "Miers, Harriet", "Kelley, William K.", "Wallace, Nicolle", "Kavanaugh, Brett M.", "Davis, Michele A."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Tue Apr 02 15:14:49 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: FINAL: NSA Setting the record straight

From: "McDonald, Matthew T."

Date: 1/4/06, 8:13 PM

To: "Kavanaugh, Brett M.", "Miers, Harriet", "Kelley, William K.", "Wallace, Nicolle", "McClellan, Scott", "Davis, Michele A."

CC: "Sherzer, David"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Tue Apr 02 15:14:51 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: NSA Setting the record straight

From: "Kelley, William K."

Date: 1/4/06, 8:43 PM

To: "McDonald, Matthew T.", "Miers, Harriet", "Wallace, Nicolle", "McClellan, Scott", "Kavanaugh, Brett M.", "Davis, Michele A."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Tue Apr 02 15:14:52 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: FW: DOJ white paper on NSA activities
From: "Gerry, Brett C."
Date: 1/19/06, 1:13 PM
To: "Kavanaugh, Brett M."

Here's the final white paper.

— Attachments: —

White Paper on NSA Legal Authorities.pdf

216 KB



U.S. Department of Justice

Washington, D.C. 20530

January 19, 2006

LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT

As the President has explained, since shortly after the attacks of September 11, 2001, he has authorized the National Security Agency (“NSA”) to intercept international communications into and out of the United States of persons linked to al Qaeda or related terrorist organizations. The purpose of these intercepts is to establish an early warning system to detect and prevent another catastrophic terrorist attack on the United States. This paper addresses, in an unclassified form, the legal basis for the NSA activities described by the President (“NSA activities”).

SUMMARY

On September 11, 2001, the al Qaeda terrorist network launched the deadliest foreign attack on American soil in history. Al Qaeda’s leadership repeatedly has pledged to attack the United States again at a time of its choosing, and these terrorist organizations continue to pose a grave threat to the United States. In response to the September 11th attacks and the continuing threat, the President, with broad congressional approval, has acted to protect the Nation from another terrorist attack. In the immediate aftermath of September 11th, the President promised that “[w]e will direct every resource at our command—every means of diplomacy, every tool of intelligence, every tool of law enforcement, every financial influence, and every weapon of war—to the destruction of and to the defeat of the global terrorist network.” President Bush Address to a Joint Session of Congress (Sept. 20, 2001). The NSA activities are an indispensable aspect of this defense of the Nation. By targeting the international communications into and out of the United States of persons reasonably believed to be linked to al Qaeda, these activities provide the United States with an early warning system to help avert the next attack. For the following reasons, the NSA activities are lawful and consistent with civil liberties.

The NSA activities are supported by the President’s well-recognized inherent constitutional authority as Commander in Chief and sole organ for the Nation in foreign affairs to conduct warrantless surveillance of enemy forces for intelligence purposes to detect and disrupt armed attacks on the United States. The President has the chief responsibility under the Constitution to protect America from attack, and the Constitution gives the President the authority necessary to fulfill that solemn responsibility. The President has made clear that he will exercise all authority available to him, consistent with the Constitution, to protect the people of the United States.

In the specific context of the current armed conflict with al Qaeda and related terrorist organizations, Congress by statute has confirmed and supplemented the President's recognized authority under Article II of the Constitution to conduct such warrantless surveillance to prevent further catastrophic attacks on the homeland. In its first legislative response to the terrorist attacks of September 11th, Congress authorized the President to "use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks" of September 11th in order to prevent "any future acts of international terrorism against the United States." Authorization for Use of Military Force, Pub. L. No. 107-40, § 2(a), 115 Stat. 224, 224 (Sept. 18, 2001) (reported as a note to 50 U.S.C.A. § 1541) ("AUMF"). History conclusively demonstrates that warrantless communications intelligence targeted at the enemy in time of armed conflict is a traditional and fundamental incident of the use of military force authorized by the AUMF. The Supreme Court's interpretation of the AUMF in *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004), confirms that Congress in the AUMF gave its express approval to the military conflict against al Qaeda and its allies and thereby to the President's use of all traditional and accepted incidents of force in this current military conflict—including warrantless electronic surveillance to intercept enemy communications both at home and abroad. This understanding of the AUMF demonstrates Congress's support for the President's authority to protect the Nation and, at the same time, adheres to Justice O'Connor's admonition that "a state of war is not a blank check for the President," *Hamdi*, 542 U.S. at 536 (plurality opinion), particularly in view of the narrow scope of the NSA activities.

The AUMF places the President at the zenith of his powers in authorizing the NSA activities. Under the tripartite framework set forth by Justice Jackson in *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635-38 (1952) (Jackson, J., concurring), Presidential authority is analyzed to determine whether the President is acting in accordance with congressional authorization (category I), whether he acts in the absence of a grant or denial of authority by Congress (category II), or whether he uses his own authority under the Constitution to take actions incompatible with congressional measures (category III). Because of the broad authorization provided in the AUMF, the President's action here falls within category I of Justice Jackson's framework. Accordingly, the President's power in authorizing the NSA activities is at its height because he acted "pursuant to an express or implied authorization of Congress," and his power "includes all that he possesses in his own right plus all that Congress can delegate." *Id.* at 635.

The NSA activities are consistent with the preexisting statutory framework generally applicable to the interception of communications in the United States—the Foreign Intelligence Surveillance Act ("FISA"), as amended, 50 U.S.C. §§ 1801-1862 (2000 & Supp. II 2002), and relevant related provisions in chapter 119 of title 18.¹ Although FISA generally requires judicial approval of electronic surveillance, FISA also contemplates that Congress may authorize such surveillance by a statute other than FISA. *See* 50 U.S.C. § 1809(a) (prohibiting any person from intentionally "engag[ing] . . . in electronic surveillance under color of law except as authorized

¹ Chapter 119 of title 18, which was enacted by Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, 18 U.S.C. §§ 2510-2521 (2000 & West Supp. 2005), is often referred to as "Title III."

by statute”). The AUMF, as construed by the Supreme Court in *Hamdi* and as confirmed by the history and tradition of armed conflict, is just such a statute. Accordingly, electronic surveillance conducted by the President pursuant to the AUMF, including the NSA activities, is fully consistent with FISA and falls within category I of Justice Jackson’s framework.

Even if there were ambiguity about whether FISA, read together with the AUMF, permits the President to authorize the NSA activities, the canon of constitutional avoidance requires reading these statutes in harmony to overcome any restrictions in FISA and Title III, at least as they might otherwise apply to the congressionally authorized armed conflict with al Qaeda. Indeed, were FISA and Title III interpreted to impede the President’s ability to use the traditional tool of electronic surveillance to detect and prevent future attacks by a declared enemy that has already struck at the homeland and is engaged in ongoing operations against the United States, the constitutionality of FISA, as applied to that situation, would be called into very serious doubt. In fact, if this difficult constitutional question had to be addressed, FISA would be unconstitutional as applied to this narrow context. Importantly, the FISA Court of Review itself recognized just three years ago that the President retains constitutional authority to conduct foreign surveillance apart from the FISA framework, and the President is certainly entitled, at a minimum, to rely on that judicial interpretation of the Constitution and FISA.

Finally, the NSA activities fully comply with the requirements of the Fourth Amendment. The interception of communications described by the President falls within a well-established exception to the warrant requirement and satisfies the Fourth Amendment’s fundamental requirement of reasonableness. The NSA activities are thus constitutionally permissible and fully protective of civil liberties.

BACKGROUND

A. THE ATTACKS OF SEPTEMBER 11, 2001

On September 11, 2001, the al Qaeda terrorist network launched a set of coordinated attacks along the East Coast of the United States. Four commercial jetliners, each carefully selected to be fully loaded with fuel for a transcontinental flight, were hijacked by al Qaeda operatives. Two of the jetliners were targeted at the Nation’s financial center in New York and were deliberately flown into the Twin Towers of the World Trade Center. The third was targeted at the headquarters of the Nation’s Armed Forces, the Pentagon. The fourth was apparently headed toward Washington, D.C., when passengers struggled with the hijackers and the plane crashed in Shanksville, Pennsylvania. The intended target of this fourth jetliner was evidently the White House or the Capitol, strongly suggesting that its intended mission was to strike a decapitation blow on the Government of the United States—to kill the President, the Vice President, or Members of Congress. The attacks of September 11th resulted in approximately 3,000 deaths—the highest single-day death toll from hostile foreign attacks in the Nation’s history. These attacks shut down air travel in the United States, disrupted the Nation’s financial markets and government operations, and caused billions of dollars in damage to the economy.

On September 14, 2001, the President declared a national emergency “by reason of the terrorist attacks at the World Trade Center, New York, New York, and the Pentagon, and the continuing and immediate threat of further attacks on the United States.” Proclamation No. 7463, 66 Fed. Reg. 48,199 (Sept. 14, 2001). The same day, Congress passed a joint resolution authorizing the President “to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks” of September 11th, which the President signed on September 18th. AUMF § 2(a). Congress also expressly acknowledged that the attacks rendered it “necessary and appropriate” for the United States to exercise its right “to protect United States citizens both at home and abroad,” and in particular recognized that “the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States.” *Id.* pmb1. Congress emphasized that the attacks “continue to pose an unusual and extraordinary threat to the national security and foreign policy of the United States.” *Id.* The United States also launched a large-scale military response, both at home and abroad. In the United States, combat air patrols were immediately established over major metropolitan areas and were maintained 24 hours a day until April 2002. The United States also immediately began plans for a military response directed at al Qaeda’s base of operations in Afghanistan. Acting under his constitutional authority as Commander in Chief, and with the support of Congress, the President dispatched forces to Afghanistan and, with the assistance of the Northern Alliance, toppled the Taliban regime.

As the President made explicit in his Military Order of November 13, 2001, authorizing the use of military commissions to try terrorists, the attacks of September 11th “created a state of armed conflict.” Military Order § 1(a), 66 Fed. Reg. 57,833 (Nov. 13, 2001). Indeed, shortly after the attacks, NATO—for the first time in its 46-year history—invoked article 5 of the North Atlantic Treaty, which provides that an “armed attack against one or more of [the parties] shall be considered an attack against them all.” North Atlantic Treaty, Apr. 4, 1949, art. 5, 63 Stat. 2241, 2244, 34 U.N.T.S. 243, 246; *see also* Statement by NATO Secretary General Lord Robertson (Oct. 2, 2001), *available at* <http://www.nato.int/docu/speech/2001/s011002a.htm> (“[I]t has now been determined that the attack against the United States on 11 September was directed from abroad and shall therefore be regarded as an action covered by Article 5 of the Washington Treaty . . .”). The President also determined in his Military Order that al Qaeda and related terrorists organizations “possess both the capability and the intention to undertake further terrorist attacks against the United States that, if not detected and prevented, will cause mass deaths, mass injuries, and massive destruction of property, and may place at risk the continuity of the operations of the United States Government,” and concluded that “an extraordinary emergency exists for national defense purposes.” Military Order, § 1(c), (g), 66 Fed. Reg. at 57,833-34.

B. THE NSA ACTIVITIES

Against this unfolding background of events in the fall of 2001, there was substantial concern that al Qaeda and its allies were preparing to carry out another attack within the United States. Al Qaeda had demonstrated its ability to introduce agents into the United States undetected and to perpetrate devastating attacks, and it was suspected that additional agents were

likely already in position within the Nation's borders. As the President has explained, unlike a conventional enemy, al Qaeda has infiltrated "our cities and communities and communicated from here in America to plot and plan with bin Laden's lieutenants in Afghanistan, Pakistan and elsewhere." Press Conference of President Bush (Dec. 19, 2005), *available at* <http://www.whitehouse.gov/news/releases/2005/12/20051219-2.html> ("President's Press Conference"). To this day, finding al Qaeda sleeper agents in the United States remains one of the paramount concerns in the War on Terror. As the President has explained, "[t]he terrorists want to strike America again, and they hope to inflict even more damage than they did on September the 11th." *Id.*

The President has acknowledged that, to counter this threat, he has authorized the NSA to intercept international communications into and out of the United States of persons linked to al Qaeda or related terrorist organizations. The same day, the Attorney General elaborated and explained that in order to intercept a communication, there must be "a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda." Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence, *available at* <http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html> (Dec. 19, 2005) (statement of Attorney General Gonzales). The purpose of these intercepts is to establish an early warning system to detect and prevent another catastrophic terrorist attack on the United States. The President has stated that the NSA activities "ha[ve] been effective in disrupting the enemy, while safeguarding our civil liberties." President's Press Conference.

The President has explained that the NSA activities are "critical" to the national security of the United States. *Id.* Confronting al Qaeda "is not simply a matter of [domestic] law enforcement"—we must defend the country against an enemy that declared war against the United States. *Id.* To "effectively detect enemies hiding in our midst and prevent them from striking us again . . . we must be able to act fast and to detect conversations [made by individuals linked to al Qaeda] so we can prevent new attacks." *Id.* The President pointed out that "a two-minute phone conversation between somebody linked to al Qaeda here and an operative overseas could lead directly to the loss of thousands of lives." *Id.* The NSA activities are intended to help "connect the dots" between potential terrorists. *Id.* In addition, the Nation is facing "a different era, a different war . . . people are changing phone numbers . . . and they're moving quick[ly]." *Id.* As the President explained, the NSA activities "enable[] us to move faster and quicker. And that's important. We've got to be fast on our feet, quick to detect and prevent." *Id.* "This is an enemy that is quick and it's lethal. And sometimes we have to move very, very quickly." *Id.* FISA, by contrast, is better suited "for long-term monitoring." *Id.*

As the President has explained, the NSA activities are "carefully reviewed approximately every 45 days to ensure that [they are] being used properly." *Id.* These activities are reviewed for legality by the Department of Justice and are monitored by the General Counsel and Inspector General of the NSA to ensure that civil liberties are being protected. *Id.* Leaders in Congress from both parties have been briefed more than a dozen times on the NSA activities.

C. THE CONTINUING THREAT POSED BY AL QAEDA

Before the September 11th attacks, al Qaeda had promised to attack the United States. In 1998, Osama bin Laden declared a “religious” war against the United States and urged that it was the moral obligation of all Muslims to kill U.S. civilians and military personnel. *See* Statement of Osama bin Laden, Ayman al-Zawahiri, et al., *Fatwah Urging Jihad Against Americans*, published in Al-Quds al-’Arabi (Feb. 23, 1998) (“To kill the Americans and their allies—civilians and military—is an individual duty for every Muslim who can do it in any country in which it is possible to do it, in order to liberate the al-Aqsa Mosque and the holy mosque from their grip, and in order for their armies to move out of all the lands of Islam, defeated and unable to threaten any Muslim.”). Al Qaeda carried out those threats with a vengeance; they attacked the U.S.S. Cole in Yemen, the United States Embassy in Nairobi, and finally the United States itself in the September 11th attacks.

It is clear that al Qaeda is not content with the damage it wrought on September 11th. As recently as December 7, 2005, Ayman al-Zawahiri professed that al Qaeda “is spreading, growing, and becoming stronger,” and that al Qaeda is “waging a great historic battle in Iraq, Afghanistan, Palestine, and even in the Crusaders’ own homes.” Ayman al-Zawahiri, videotape released on Al-Jazeera television network (Dec. 7, 2005). Indeed, since September 11th, al Qaeda leaders have repeatedly promised to deliver another, even more devastating attack on America. *See, e.g.*, Osama bin Laden, videotape released on Al-Jazeera television network (Oct. 24, 2004) (warning United States citizens of further attacks and asserting that “your security is in your own hands”); Osama bin Laden, videotape released on Al-Jazeera television network (Oct. 18, 2003) (“We, God willing, will continue to fight you and will continue martyrdom operations inside and outside the United States”); Ayman Al-Zawahiri, videotape released on the Al-Jazeera television network (Oct. 9, 2002) (“I promise you [addressing the ‘citizens of the United States’] that the Islamic youth are preparing for you what will fill your hearts with horror”). Given that al Qaeda’s leaders have repeatedly made good on their threats and that al Qaeda has demonstrated its ability to insert foreign agents into the United States to execute attacks, it is clear that the threat continues. Indeed, since September 11th, al Qaeda has staged several large-scale attacks around the world, including in Indonesia, Madrid, and London, killing hundreds of innocent people.

ANALYSIS

I. THE PRESIDENT HAS INHERENT CONSTITUTIONAL AUTHORITY TO ORDER WARRANTLESS FOREIGN INTELLIGENCE SURVEILLANCE

As Congress expressly recognized in the AUMF, “the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States,” AUMF pmb., especially in the context of the current conflict. Article II of the Constitution vests in the President all executive power of the United States, including the power to act as Commander in Chief of the Armed Forces, *see* U.S. Const. art. II, § 2, and authority over the conduct of the Nation’s foreign affairs. As the Supreme Court has explained, “[t]he President is the sole organ of the nation in its external relations, and its sole representative with

foreign nations.” *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 319 (1936) (internal quotation marks and citations omitted). In this way, the Constitution grants the President inherent power to protect the Nation from foreign attack, *see, e.g., The Prize Cases*, 67 U.S. (2 Black) 635, 668 (1863), and to protect national security information, *see, e.g., Department of the Navy v. Egan*, 484 U.S. 518, 527 (1988).

To carry out these responsibilities, the President must have authority to gather information necessary for the execution of his office. The Founders, after all, intended the federal Government to be clothed with all authority necessary to protect the Nation. *See, e.g., The Federalist* No. 23, at 147 (Alexander Hamilton) (Jacob E. Cooke ed. 1961) (explaining that the federal Government will be “clothed with all the powers requisite to the complete execution of its trust”); *id.* No. 41, at 269 (James Madison) (“Security against foreign danger is one of the primitive objects of civil society The powers requisite for attaining it must be effectually confided to the federal councils.”). Because of the structural advantages of the Executive Branch, the Founders also intended that the President would have the primary responsibility and necessary authority as Commander in Chief and Chief Executive to protect the Nation and to conduct the Nation’s foreign affairs. *See, e.g., The Federalist* No. 70, at 471-72 (Alexander Hamilton); *see also Johnson v. Eisentrager*, 339 U.S. 763, 788 (1950) (“this [constitutional] grant of war power includes all that is necessary and proper for carrying these powers into execution”) (citation omitted). Thus, it has been long recognized that the President has the authority to use secretive means to collect intelligence necessary for the conduct of foreign affairs and military campaigns. *See, e.g., Chicago & S. Air Lines v. Waterman S.S. Corp.*, 333 U.S. 103, 111 (1948) (“The President, both as Commander-in-Chief and as the Nation’s organ for foreign affairs, has available intelligence services whose reports are not and ought not to be published to the world.”); *Curtiss-Wright*, 299 U.S. at 320 (“He has his confidential sources of information. He has his agents in the form of diplomatic, consular and other officials.”); *Totten v. United States*, 92 U.S. 105, 106 (1876) (President “was undoubtedly authorized during the war, as commander-in-chief . . . to employ secret agents to enter the rebel lines and obtain information respecting the strength, resources, and movements of the enemy”).

In reliance on these principles, a consistent understanding has developed that the President has inherent constitutional authority to conduct warrantless searches and surveillance within the United States for foreign intelligence purposes. Wiretaps for such purposes thus have been authorized by Presidents at least since the administration of Franklin Roosevelt in 1940. *See, e.g., United States v. United States District Court*, 444 F.2d 651, 669-71 (6th Cir. 1971) (reproducing as an appendix memoranda from Presidents Roosevelt, Truman, and Johnson). In a Memorandum to Attorney General Jackson, President Roosevelt wrote on May 21, 1940:

You are, therefore, authorized and directed in such cases as you may approve, after investigation of the need in each case, to authorize the necessary investigation agents that they are at liberty to secure information by listening devices directed to the conversation or other communications of persons suspected of subversive activities against the Government of the United States, including suspected spies. You are requested furthermore to limit these investigations so conducted to a minimum and limit them insofar as

possible to aliens.

Id. at 670 (appendix A). President Truman approved a memorandum drafted by Attorney General Tom Clark in which the Attorney General advised that “it is as necessary as it was in 1940 to take the investigative measures” authorized by President Roosevelt to conduct electronic surveillance “in cases vitally affecting the domestic security.” *Id.* Indeed, while FISA was being debated during the Carter Administration, Attorney General Griffin Bell testified that “the current bill recognizes no inherent power of the President to conduct electronic surveillance, and I want to interpolate here to say that *this does not take away the power [of] the President under the Constitution.*” Foreign Intelligence Electronic Surveillance Act of 1978: Hearings on H.R. 5764, H.R. 9745, H.R. 7308, and H.R. 5632 Before the Subcomm. on Legislation of the House Comm. on Intelligence, 95th Cong., 2d Sess. 15 (1978) (emphasis added); *see also Katz v. United States*, 389 U.S. 347, 363 (1967) (White, J., concurring) (“Wiretapping to protect the security of the Nation has been authorized by successive Presidents.”); *cf.* Amending the Foreign Intelligence Surveillance Act: Hearings Before the House Permanent Select Comm. on Intelligence, 103d Cong. 2d Sess. 61 (1994) (statement of Deputy Attorney General Jamie S. Gorelick) (“[T]he Department of Justice believes, and the case law supports, that the President has inherent authority to conduct warrantless physical searches for foreign intelligence purposes . . .”).

The courts uniformly have approved this longstanding Executive Branch practice. Indeed, every federal appellate court to rule on the question has concluded that, even in peacetime, the President has inherent constitutional authority, consistent with the Fourth Amendment, to conduct searches for foreign intelligence purposes without securing a judicial warrant. *See In re Sealed Case*, 310 F.3d 717, 742 (Foreign Intel. Surv. Ct. of Rev. 2002) (“[A]ll 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 *We take for granted that the President does have that authority and, assuming that is so, FISA could not encroach on the President’s constitutional power.*”) (emphasis added); *accord, e.g., United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980); *United States v. Butenko*, 494 F.2d 593 (3d Cir. 1974) (en banc); *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973). *But cf. Zweibon v. Mitchell*, 516 F.2d 594 (D.C. Cir. 1975) (en banc) (dictum in plurality opinion suggesting that a warrant would be required even in a foreign intelligence investigation).

In *United States v. United States District Court*, 407 U.S. 297 (1972) (the “*Keith*” case), the Supreme Court concluded that the Fourth Amendment’s warrant requirement applies to investigations of wholly *domestic* threats to security—such as domestic political violence and other crimes. But the Court in the *Keith* case made clear that it was not addressing the President’s authority to conduct *foreign* intelligence surveillance without a warrant and that it was expressly reserving that question: “[T]he instant case requires no judgment on the scope of the President’s surveillance power with respect to the activities of foreign powers, within or without this country.” *Id.* at 308; *see also id.* at 321-22 & n.20 (“We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents.”). That *Keith* does not apply in the context of protecting against a foreign attack has been confirmed by the lower courts. After *Keith*, each of the three courts of appeals

that have squarely considered the question have concluded—expressly taking the Supreme Court’s decision into account—that the President has inherent authority to conduct warrantless surveillance in the foreign intelligence context. *See, e.g., Truong Dinh Hung*, 629 F.2d at 913-14; *Butenko*, 494 F.2d at 603; *Brown*, 484 F.2d 425-26.

From a constitutional standpoint, foreign intelligence surveillance such as the NSA activities differs fundamentally from the domestic security surveillance at issue in *Keith*. As the Fourth Circuit observed, the President has uniquely strong constitutional powers in matters pertaining to foreign affairs and national security. “Perhaps most crucially, the executive branch not only has superior expertise in the area of foreign intelligence, it is also constitutionally designated as the pre-eminent authority in foreign affairs.” *Truong*, 629 F.2d at 914; *see id.* at 913 (noting that “the needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would . . . unduly frustrate the President in carrying out his foreign affairs responsibilities”); *cf. Haig v. Agee*, 453 U.S. 280, 292 (1981) (“Matters intimately related to foreign policy and national security are rarely proper subjects for judicial intervention.”).²

The present circumstances that support recognition of the President’s inherent constitutional authority to conduct the NSA activities are considerably stronger than were the circumstances at issue in the earlier courts of appeals cases that recognized this power. All of the cases described above addressed inherent executive authority under the foreign affairs power to conduct surveillance in a peacetime context. The courts in these cases therefore had no occasion even to consider the fundamental authority of the President, as Commander in Chief, to gather intelligence in the context of an ongoing armed conflict in which the United States already had suffered massive civilian casualties and in which the intelligence gathering efforts at issue were specifically designed to thwart further armed attacks. Indeed, intelligence gathering is particularly important in the current conflict, in which the enemy attacks largely through clandestine activities and which, as Congress recognized, “pose[s] an unusual and extraordinary threat,” AUMF pmb1.

Among the President’s most basic constitutional duties is the duty to protect the Nation from armed attack. The Constitution gives him all necessary authority to fulfill that responsibility. The courts thus have long acknowledged the President’s inherent authority to take action to protect Americans abroad, *see, e.g., Durand v. Hollins*, 8 F. Cas. 111, 112 (C.C.S.D.N.Y. 1860) (No. 4186), and to protect the Nation from attack, *see, e.g., The Prize Cases*, 67 U.S. at 668. *See generally Ex parte Quirin*, 317 U.S. 1, 28 (1942) (recognizing that

² *Keith* made clear that one of the significant concerns driving the Court’s conclusion in the domestic security context was the inevitable connection between perceived threats to domestic security and political dissent. As the Court explained: “Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect ‘domestic security.’” *Keith*, 407 U.S. at 314; *see also id.* at 320 (“Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent.”). Surveillance of domestic groups raises a First Amendment concern that generally is not present when the subjects of the surveillance are foreign powers or their agents.

the President has authority under the Constitution “to direct the performance of those functions which may constitutionally be performed by the military arm of the nation in time of war,” including “important incident[s] to the conduct of war,” such as “the adoption of measures by the military command . . . to repel and defeat the enemy”). As the Supreme Court emphasized in the *Prize Cases*, if the Nation is invaded, the President is “bound to resist force by force”; “[h]e must determine what degree of force the crisis demands” and need not await congressional sanction to do so. *The Prize Cases*, 67 U.S. at 670; *see also Campbell v. Clinton*, 203 F.3d 19, 27 (D.C. Cir. 2000) (Silberman, J., concurring) (“[T]he *Prize Cases* . . . stand for the proposition that the President has independent authority to repel aggressive acts by third parties even without specific congressional authorization, and courts may not review the level of force selected.”); *id.* at 40 (Tatel, J., concurring) (“[T]he President, as commander in chief, possesses emergency authority to use military force to defend the nation from attack without obtaining prior congressional approval.”). Indeed, “in virtue of his rank as head of the forces, [the President] has certain powers and duties with which Congress cannot interfere.” *Training of British Flying Students in the United States*, 40 Op. Att’y Gen. 58, 61 (1941) (Attorney General Robert H. Jackson) (internal quotation marks omitted). In exercising his constitutional powers, the President has wide discretion, consistent with the Constitution, over the methods of gathering intelligence about the Nation’s enemies in a time of armed conflict.

II. THE AUMF CONFIRMS AND SUPPLEMENTS THE PRESIDENT’S INHERENT POWER TO USE WARRANTLESS SURVEILLANCE AGAINST THE ENEMY IN THE CURRENT ARMED CONFLICT

In the Authorization for Use of Military Force enacted in the wake of September 11th, Congress confirms and supplements the President’s constitutional authority to protect the Nation, including through electronic surveillance, in the context of the current post-September 11th armed conflict with al Qaeda and its allies. The broad language of the AUMF affords the President, at a minimum, discretion to employ the traditional incidents of the use of military force. The history of the President’s use of warrantless surveillance during armed conflicts demonstrates that the NSA surveillance described by the President is a fundamental incident of the use of military force that is necessarily included in the AUMF.

A. THE TEXT AND PURPOSE OF THE AUMF AUTHORIZE THE NSA ACTIVITIES

On September 14, 2001, in its first legislative response to the attacks of September 11th, Congress gave its express approval to the President’s military campaign against al Qaeda and, in the process, confirmed the well-accepted understanding of the President’s Article II powers. *See* AUMF § 2(a).³ In the preamble to the AUMF, Congress stated that “the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States,” AUMF pmbl., and thereby acknowledged the President’s inherent constitutional authority to defend the United States. This clause “constitutes an extraordinarily

³ America’s military response began before the attacks of September 11th had been completed. *See The 9/11 Commission Report 20* (2004). Combat air patrols were established and authorized “to engage inbound aircraft if they could verify that the aircraft was hijacked.” *Id.* at 42.

sweeping recognition of independent presidential *constitutional* power to employ the war power to combat terrorism.” Michael Stokes Paulsen, *Youngstown Goes to War*, 19 Const. Comment. 215, 252 (2002). This striking recognition of presidential authority cannot be discounted as the product of excitement in the immediate aftermath of September 11th, for the same terms were repeated by Congress more than a year later in the Authorization for Use of Military Force Against Iraq Resolution of 2002. Pub. L. No. 107-243, pmb., 116 Stat. 1498, 1500 (Oct. 16, 2002) (“[T]he President has authority under the Constitution to take action in order to deter and prevent acts of international terrorism against the United States . . .”). In the context of the conflict with al Qaeda and related terrorist organizations, therefore, Congress has acknowledged a broad executive authority to “deter and prevent” further attacks against the United States.

The AUMF passed by Congress on September 14, 2001, does not lend itself to a narrow reading. Its expansive language authorizes the President “to use *all necessary and appropriate force* against those nations, organizations, or persons *he determines* planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001.” AUMF § 2(a) (emphases added). In the field of foreign affairs, and particularly that of war powers and national security, congressional enactments are to be broadly construed where they indicate support for authority long asserted and exercised by the Executive Branch. *See, e.g., Haig v. Agee*, 453 U.S. 280, 293-303 (1981); *United States ex rel. Knauff v. Shaughnessy*, 338 U.S. 537, 543-45 (1950); *cf. Loving v. United States*, 517 U.S. 748, 772 (1996) (noting that the usual “limitations on delegation [of congressional powers] do not apply” to authorizations linked to the Commander in Chief power); *Dames & Moore v. Regan*, 453 U.S. 654, 678-82 (1981) (even where there is no express statutory authorization for executive action, legislation in related field may be construed to indicate congressional acquiescence in that action). Although Congress’s war powers under Article I, Section 8 of the Constitution empower Congress to legislate regarding the raising, regulation, and material support of the Armed Forces and related matters, rather than the prosecution of military campaigns, the AUMF indicates Congress’s endorsement of the President’s use of his constitutional war powers. This authorization transforms the struggle against al Qaeda and related terrorist organizations from what Justice Jackson called “a zone of twilight,” in which the President and the Congress may have concurrent powers whose “distribution is uncertain,” *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 637 (1952) (Jackson, J., concurring), into a situation in which the President’s authority is at its maximum because “it includes all that he possesses in his own right plus all that Congress can delegate,” *id.* at 635. With regard to these fundamental tools of warfare—and, as demonstrated below, warrantless electronic surveillance against the declared enemy is one such tool—the AUMF places the President’s authority at its zenith under *Youngstown*.

It is also clear that the AUMF confirms and supports the President’s use of those traditional incidents of military force against the enemy, wherever they may be—on United States soil or abroad. The nature of the September 11th attacks—launched on United States soil by foreign agents secreted in the United States—necessitates such authority, and the text of the AUMF confirms it. The operative terms of the AUMF state that the President is authorized to use force “in order to prevent any future acts of international terrorism against the United States,” *id.*, an objective which, given the recent attacks within the Nation’s borders and the continuing use of air defense throughout the country at the time Congress acted, undoubtedly

contemplated the possibility of military action within the United States. The preamble, moreover, recites that the United States should exercise its rights “to protect United States citizens both *at home* and abroad.” *Id.* pmb1. (emphasis added). To take action against those linked to the September 11th attacks involves taking action against individuals within the United States. The United States had been attacked on its own soil—not by aircraft launched from carriers several hundred miles away, but by enemy agents who had resided in the United States for months. A crucial responsibility of the President—charged by the AUMF and the Constitution—was and is to identify and attack those enemies, especially if they were in the United States, ready to strike against the Nation.

The text of the AUMF demonstrates in an additional way that Congress authorized the President to conduct warrantless electronic surveillance against the enemy. The terms of the AUMF not only authorized the President to “use all necessary and appropriate force” against those responsible for the September 11th attacks; it also authorized the President to “determine[]” the persons or groups responsible for those attacks and to take all actions necessary to prevent further attacks. AUMF § 2(a) (“the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons *he determines* planned, authorized, committed, or aided the terrorist attacks that occurred on September 11th, 2001, or harbored such organizations or persons”) (emphasis added). Of vital importance to the use of force against the enemy is locating the enemy and identifying its plans of attack. And of vital importance to identifying the enemy and detecting possible future plots was the authority to intercept communications to or from the United States of persons with links to al Qaeda or related terrorist organizations. Given that the agents who carried out the initial attacks resided in the United States and had successfully blended into American society and disguised their identities and intentions until they were ready to strike, the necessity of using the most effective intelligence gathering tools against such an enemy, including electronic surveillance, was patent. Indeed, Congress recognized that the enemy in this conflict poses an “unusual and extraordinary threat.” AUMF pmb1.

The Supreme Court’s interpretation of the scope of the AUMF in *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004), strongly supports this reading of the AUMF. In *Hamdi*, five members of the Court found that the AUMF authorized the detention of an American within the United States, notwithstanding a statute that prohibits the detention of U.S. citizens “except pursuant to an Act of Congress,” 18 U.S.C. § 4001(a). *See Hamdi*, 542 U.S. at 519 (plurality opinion); *id.* at 587 (Thomas, J., dissenting). Drawing on historical materials and “longstanding law-of-war principles,” *id.* at 518-21, a plurality of the Court concluded that detention of combatants who fought against the United States as part of an organization “known to have supported” al Qaeda “is so fundamental and accepted an incident to war as to be an exercise of the ‘necessary and appropriate force’ Congress has authorized the President to use.” *Id.* at 518; *see also id.* at 587 (Thomas, J., dissenting) (agreeing with the plurality that the joint resolution authorized the President to “detain those arrayed against our troops”); *accord Quirin*, 317 U.S. at 26-29, 38 (recognizing the President’s authority to capture and try agents of the enemy in the United States even if they had never “entered the theatre or zone of active military operations”). Thus, even though the AUMF does not say anything expressly about detention, the Court nevertheless found that it satisfied section 4001(a)’s requirement that detention be congressionally authorized.

The conclusion of five Justices in *Hamdi* that the AUMF incorporates fundamental “incidents” of the use of military force makes clear that the absence of any specific reference to signals intelligence activities in the resolution is immaterial. *See Hamdi*, 542 U.S. at 519 (“[I]t is of no moment that the AUMF does not use specific language of detention.”) (plurality opinion). Indeed, given the circumstances in which the AUMF was adopted, it is hardly surprising that Congress chose to speak about the President’s authority in general terms. The purpose of the AUMF was for Congress to sanction and support the military response to the devastating terrorist attacks that had occurred just three days earlier. Congress evidently thought it neither necessary nor appropriate to attempt to catalog every specific aspect of the use of the forces it was authorizing and every potential preexisting statutory limitation on the Executive Branch. Rather than engage in that difficult and impractical exercise, Congress authorized the President, in general but intentionally broad terms, to use the traditional and fundamental incidents of war and to determine how best to identify and engage the enemy in the current armed conflict. Congress’s judgment to proceed in this manner was unassailable, for, as the Supreme Court has recognized, even in normal times involving no major national security crisis, “Congress cannot anticipate and legislate with regard to every possible action the President may find it necessary to take.” *Dames & Moore*, 453 U.S. at 678. Indeed, Congress often has enacted authorizations to use military force using general authorizing language that does not purport to catalogue in detail the specific powers the President may employ. The need for Congress to speak broadly in recognizing and augmenting the President’s core constitutional powers over foreign affairs and military campaigns is of course significantly heightened in times of national emergency. *See Zemel v. Rusk*, 381 U.S. 1, 17 (1965) (“[B]ecause of the changeable and explosive nature of contemporary international relations . . . Congress—in giving the Executive authority over matters of foreign affairs—must of necessity paint with a brush broader than that it customarily wields in domestic areas.”).

Hamdi thus establishes the proposition that the AUMF “clearly and unmistakably” authorizes the President to take actions against al Qaeda and related organizations that amount to “fundamental incident[s] of waging war.” *Hamdi*, 542 U.S. at 519 (plurality opinion); *see also id.* at 587 (Thomas, J., dissenting). In other words, “[t]he clear inference is that the AUMF authorizes what the laws of war permit.” Curtis A. Bradley & Jack L. Goldsmith, *Congressional Authorization and the War on Terrorism*, 118 Harv. L. Rev. 2048, 2092 (2005) (emphasis added). Congress is presumed to be aware of the Supreme Court’s precedents. Indeed, Congress recently enacted legislation in response to the Court’s decision in *Rasul v. Bush*, 542 U.S. 466 (2004)—which was issued the same day as the *Hamdi* decision—removing habeas corpus jurisdiction over claims filed on behalf of confined enemy combatants held at Guantanamo Bay. Congress, however, has not expressed any disapproval of the Supreme Court’s commonsense and plain-meaning interpretation of the AUMF in *Hamdi*.⁴

⁴ This understanding of the AUMF is consistent with Justice O’Connor’s admonition that “a state of war is not a blank check for the President,” *Hamdi*, 542 U.S. at 536 (plurality opinion). In addition to constituting a fundamental and accepted incident of the use of military force, the NSA activities are consistent with the law of armed conflict principle that the use of force be necessary and proportional. *See* Dieter Fleck, *The Handbook of Humanitarian Law in Armed Conflicts* 115 (1995). The NSA activities are proportional because they are minimally invasive and narrow in scope, targeting only the international communications of persons reasonably believed to be linked to al Qaeda, and are designed to protect the Nation from a devastating attack.

B. WARRANTLESS ELECTRONIC SURVEILLANCE AIMED AT INTERCEPTING ENEMY COMMUNICATIONS HAS LONG BEEN RECOGNIZED AS A FUNDAMENTAL INCIDENT OF THE USE OF MILITARY FORCE

The history of warfare—including the consistent practice of Presidents since the earliest days of the Republic—demonstrates that warrantless intelligence surveillance against the enemy is a fundamental incident of the use of military force, and this history confirms the statutory authority provided by the AUMF. Electronic surveillance is a fundamental tool of war that must be included in any natural reading of the AUMF’s authorization to use “all necessary and appropriate force.”

As one author has explained:

It is *essential* in warfare for a belligerent to be as fully informed as possible about the enemy—his strength, his weaknesses, measures taken by him and measures contemplated by him. This applies not only to military matters, but . . . anything which bears on and is material to his ability to wage the war in which he is engaged. *The laws of war recognize and sanction this aspect of warfare.*

Morris Greenspan, *The Modern Law of Land Warfare* 325 (1959) (emphases added); *see also* Memorandum for Members of the House Permanent Select Comm. on Intel., from Jeffrey H. Smith, *Re: Legal Authorities Regarding Warrantless Surveillance of U.S. Persons* 6 (Jan. 3, 2006) (“Certainly, the collection of intelligence is understood to be necessary to the execution of the war.”). Similarly, article 24 of the Hague Regulations of 1907 expressly states that “the employment of measures necessary for obtaining information about the enemy and the country [is] considered permissible.” *See also* L. Oppenheim, *International Law* vol. II § 159 (7th ed. 1952) (“War cannot be waged without all kinds of information, about the forces and the intentions of the enemy To obtain the necessary information, it has always been considered lawful to employ spies”); Joseph R. Baker & Henry G. Crocker, *The Laws of Land Warfare* 197 (1919) (“Every belligerent has a right . . . to discover the signals of the enemy and . . . to seek to procure information regarding the enemy through the aid of secret agents.”); *cf.* J.M. Spaight, *War Rights on Land* 205 (1911) (“[E]very nation employs spies; were a nation so quixotic as to refrain from doing so, it might as well sheathe its sword for ever. . . . Spies . . . are indispensably necessary to a general; and, other things being equal, that commander will be victorious who has the best secret service.”) (internal quotation marks omitted).

In accordance with these well-established principles, the Supreme Court has consistently recognized the President’s authority to conduct intelligence activities. *See, e.g., Totten v. United States*, 92 U.S. 105, 106 (1876) (recognizing President’s authority to hire spies); *Tenet v. Doe*, 544 U.S. 1 (2005) (reaffirming *Totten* and counseling against judicial interference with such matters); *see also Chicago & S. Air Lines v. Waterman S.S. Corp.*, 333 U.S. 103, 111 (1948) (“The President, both as Commander-in-Chief and as the Nation’s organ for foreign affairs, has available intelligence services whose reports neither are not and ought not to be published to the world.”); *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 320 (1936) (The President “has his confidential sources of information. He has his agents in the form of diplomatic,

consular, and other officials.”). Chief Justice John Marshall even described the gathering of intelligence as a military duty. *See Tatum v. Laird*, 444 F.2d 947, 952-53 (D.C. Cir. 1971) (“As Chief Justice John Marshall said of Washington, ‘A general must be governed by his intelligence and must regulate his measures by his information. It is his duty to obtain correct information’”) (quoting Foreword, U.S. Army Basic Field Manual, Vol. X, circa 1938), *rev’d on other grounds*, 408 U.S. 1 (1972).

The United States, furthermore, has a long history of wartime surveillance—a history that can be traced to George Washington, who “was a master of military espionage” and “made frequent and effective use of secret intelligence in the second half of the eighteenth century.” Rhodri Jeffreys-Jones, *Cloak and Dollar: A History of American Secret Intelligence* 11 (2002); *see generally id.* at 11-23 (recounting Washington’s use of intelligence); *see also Haig v. Agee*, 471 U.S. 159, 172 n.16 (1981) (quoting General Washington’s letter to an agent embarking upon an intelligence mission in 1777: “The necessity of procuring good intelligence, is apparent and need not be further urged.”). As President in 1790, Washington obtained from Congress a “secret fund” to deal with foreign dangers and to be spent at his discretion. Jeffreys-Jones, *supra*, at 22. The fund, which remained in use until the creation of the Central Intelligence Agency in the mid-twentieth century and gained “longstanding acceptance within our constitutional structure,” *Halperin v. CIA*, 629 F.2d 144, 158-59 (D.C. Cir. 1980), was used “for all purposes to which a secret service fund should or could be applied for the public benefit,” including “for persons sent publicly and secretly to search for important information, political or commercial,” *id.* at 159 (quoting Statement of Senator John Forsyth, Cong. Debates 295 (Feb. 25, 1831)). *See also Totten*, 92 U.S. at 107 (refusing to examine payments from this fund lest the publicity make a “secret service” “impossible”).

The interception of communications, in particular, has long been accepted as a fundamental method for conducting wartime surveillance. *See, e.g., Greenspan, supra*, at 326 (accepted and customary means for gathering intelligence “include air reconnaissance and photography; ground reconnaissance; observation of enemy positions; *interception of enemy messages, wireless and other*; examination of captured documents; . . . and interrogation of prisoners and civilian inhabitants”) (emphasis added). Indeed, since its independence, the United States has intercepted communications for wartime intelligence purposes and, if necessary, has done so within its own borders. During the Revolutionary War, for example, George Washington received and used to his advantage reports from American intelligence agents on British military strength, British strategic intentions, and British estimates of American strength. *See Jeffreys-Jones, supra*, at 13. One source of Washington’s intelligence was intercepted British mail. *See Central Intelligence Agency, Intelligence in the War of Independence* 31, 32 (1997). In fact, Washington himself proposed that one of his Generals “contrive a means of opening [British letters] without breaking the seals, take copies of the contents, and then let them go on.” *Id.* at 32 (“From that point on, Washington was privy to British intelligence pouches between New York and Canada.”); *see generally* Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities (the “Church Committee”), S. Rep. No. 94-755, at Book VI, 9-17 (Apr. 23, 1976) (describing Washington’s intelligence activities).

More specifically, warrantless electronic surveillance of wartime communications has been conducted in the United States since electronic communications have existed, *i.e.*, since at least the Civil War, when “[t]elegraph wiretapping was common, and an important intelligence source for both sides.” G.J.A. O’Toole, *The Encyclopedia of American Intelligence and Espionage* 498 (1988). Confederate General J.E.B. Stuart even “had his own personal wiretapper travel along with him in the field” to intercept military telegraphic communications. Samuel Dash, et al., *The Eavesdroppers* 23 (1971); *see also* O’Toole, *supra*, at 121, 385-88, 496-98 (discussing Civil War surveillance methods such as wiretaps, reconnaissance balloons, semaphore interception, and cryptanalysis). Similarly, there was extensive use of electronic surveillance during the Spanish-American War. *See* Bruce W. Bidwell, *History of the Military Intelligence Division, Department of the Army General Staff: 1775-1941*, at 62 (1986). When an American expeditionary force crossed into northern Mexico to confront the forces of Pancho Villa in 1916, the Army “frequently intercepted messages of the regime in Mexico City or the forces contesting its rule.” David Alvarez, *Secret Messages* 6-7 (2000). Shortly after Congress declared war on Germany in World War I, President Wilson (citing only his constitutional powers and the joint resolution declaring war) ordered the censorship of messages sent outside the United States via submarine cables, telegraph, and telephone lines. *See* Exec. Order No. 2604 (Apr. 28, 1917). During that war, wireless telegraphy “enabled each belligerent to tap the messages of the enemy.” Bidwell, *supra*, at 165 (quoting statement of Col. W. Nicolai, former head of the Secret Service of the High Command of the German Army, *in* W. Nicolai, *The German Secret Service* 21 (1924)).

As noted in Part I, on May 21, 1940, President Roosevelt authorized warrantless electronic surveillance of persons suspected of subversive activities, including spying, against the United States. In addition, on December 8, 1941, the day after the attack on Pearl Harbor, President Roosevelt gave the Director of the FBI “temporary powers to direct all news censorship and to *control all other telecommunications traffic* in and out of the United States.” Jack A. Gottschalk, “*Consistent with Security*”. . . . *A History of American Military Press Censorship*, 5 Comm. & L. 35, 39 (1983) (emphasis added). *See* Memorandum for the Secretaries of War, Navy, State, and Treasury, the Postmaster General, and the Federal Communications Commission from Franklin D. Roosevelt (Dec. 8, 1941). President Roosevelt soon supplanted that temporary regime by establishing an office for conducting such electronic surveillance in accordance with the War Powers Act of 1941. *See* Pub. L. No. 77-354, § 303, 55 Stat. 838, 840-41 (Dec. 18, 1941); Gottschalk, 5 Comm. & L. at 40. The President’s order gave the Government of the United States access to “communications by mail, cable, radio, or other means of transmission passing between the United States and any foreign country.” *Id.* *See also* Exec. Order No. 8985, § 1, 6 Fed. Reg. 6625, 6625 (Dec. 19, 1941). In addition, the United States systematically listened surreptitiously to electronic communications as part of the war effort. *See* Dash, *Eavesdroppers* at 30. During World War II, signals intelligence assisted in, among other things, the destruction of the German U-boat fleet by the Allied naval forces, *see id.* at 27, and the war against Japan, *see* O’Toole, *supra*, at 32, 323-24. In general, signals intelligence “helped to shorten the war by perhaps two years, reduce the loss of life, and make inevitable an eventual Allied victory.” Carl Boyd, *American Command of the Sea Through Carriers, Codes, and the Silent Service: World War II and Beyond* 27 (1995); *see also* Alvarez, *supra*, at 1 (“There can be little doubt that signals intelligence contributed significantly to the

military defeat of the Axis.”). Significantly, not only was wiretapping in World War II used “extensively by military intelligence and secret service personnel in combat areas abroad,” but also “by the FBI and secret service in this country.” *Dash, supra*, at 30.

In light of the long history of prior wartime practice, the NSA activities fit squarely within the sweeping terms of the AUMF. The use of signals intelligence to identify and pinpoint the enemy is a traditional component of wartime military operations—or, to use the terminology of *Hamdi*, a “fundamental and accepted . . . incident to war,” 542 U.S. at 518 (plurality opinion)—employed to defeat the enemy and to prevent enemy attacks in the United States. Here, as in other conflicts, the enemy may use public communications networks, and some of the enemy may already be in the United States. Although those factors may be present in this conflict to a greater degree than in the past, neither is novel. Certainly, both factors were well known at the time Congress enacted the AUMF. Wartime interception of international communications made by the enemy thus should be understood, no less than the wartime detention at issue in *Hamdi*, as one of the basic methods of engaging and defeating the enemy that Congress authorized in approving “*all* necessary and appropriate force” that the President would need to defend the Nation. AUMF § 2(a) (emphasis added).

* * *

Accordingly, the President has the authority to conduct warrantless electronic surveillance against the declared enemy of the United States in a time of armed conflict. That authority derives from the Constitution, and is reinforced by the text and purpose of the AUMF, the nature of the threat posed by al Qaeda that Congress authorized the President to repel, and the long-established understanding that electronic surveillance is a fundamental incident of the use of military force. The President’s power in authorizing the NSA activities is at its zenith because he has acted “pursuant to an express or implied authorization of Congress.” *Youngstown*, 343 U.S. at 635 (Jackson, J., concurring).

III. THE NSA ACTIVITIES ARE CONSISTENT WITH THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

The President’s exercise of his constitutional authority to conduct warrantless wartime electronic surveillance of the enemy, as confirmed and supplemented by statute in the AUMF, is fully consistent with the requirements of the Foreign Intelligence Surveillance Act (“FISA”).⁵ FISA is a critically important tool in the War on Terror. The United States makes full use of the authorities available under FISA to gather foreign intelligence information, including authorities to intercept communications, conduct physical searches, and install and use pen registers and trap and trace devices. While FISA establishes certain procedures that must be followed for these authorities to be used (procedures that usually involve applying for and obtaining an order from a special court), FISA also expressly contemplates that a later legislative enactment could

⁵ To avoid revealing details about the operation of the program, it is assumed for purposes of this paper that the activities described by the President constitute “electronic surveillance,” as defined by FISA, 50 U.S.C. § 1801(f).

authorize electronic surveillance outside the procedures set forth in FISA itself. The AUMF constitutes precisely such an enactment. To the extent there is any ambiguity on this point, the canon of constitutional avoidance requires that such ambiguity be resolved in favor of the President's authority to conduct the communications intelligence activities he has described. Finally, if FISA could not be read to allow the President to authorize the NSA activities during the current congressionally authorized armed conflict with al Qaeda, FISA would be unconstitutional as applied in this narrow context.

A. THE REQUIREMENTS OF FISA

FISA was enacted in 1978 to regulate “electronic surveillance,” particularly when conducted to obtain “foreign intelligence information,” as those terms are defined in section 101 of FISA, 50 U.S.C. § 1801. As a general matter, the statute requires that the Attorney General approve an application for an order from a special court composed of Article III judges and created by FISA—the Foreign Intelligence Surveillance Court (“FISC”). *See* 50 U.S.C. §§ 1803-1804. The application must demonstrate, among other things, that there is probable cause to believe that the target is a foreign power or an agent of a foreign power. *See id.* § 1805(a)(3)(A). It must also contain a certification from the Assistant to the President for National Security Affairs or an officer of the United States appointed by the President with the advice and consent of the Senate and having responsibilities in the area of national security or defense that the information sought is foreign intelligence information and cannot reasonably be obtained by normal investigative means. *See id.* § 1804(a)(7). FISA further requires the Government to state the means that it proposes to use to obtain the information and the basis for its belief that the facilities at which the surveillance will be directed are being used or are about to be used by a foreign power or an agent of a foreign power. *See id.* § 1804(a)(4), (a)(8).

FISA was the first congressional measure that sought to impose restrictions on the Executive Branch's authority to engage in electronic surveillance for foreign intelligence purposes, an authority that, as noted above, had been repeatedly recognized by the federal courts. *See* Americo R. Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. Penn. L. Rev. 793, 810 (1989) (stating that the “status of the President's inherent authority” to conduct surveillance “formed the core of subsequent legislative deliberations” leading to the enactment of FISA). To that end, FISA modified a provision in Title III that previously had disclaimed any intent to have laws governing wiretapping interfere with the President's constitutional authority to gather foreign intelligence. Prior to the passage of FISA, section 2511(3) of title 18 had stated that “[n]othing contained in this chapter or in section 605 of the Communications Act of 1934 . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities.” 18 U.S.C. § 2511(3) (1970). FISA replaced that provision with an important, though more limited, preservation of authority for the President. *See* Pub. L. No. 95-511, § 201(b), (c), 92 Stat. 1783, 1797 (1978), codified at 18 U.S.C. § 2511(2)(f) (West Supp. 2005) (carving out from statutory regulation only the acquisition of intelligence information from “international or foreign communications” and

“foreign intelligence activities . . . involving a foreign electronic communications system” as long as they are accomplished “utilizing a means other than electronic surveillance as defined in section 101” of FISA). Congress also defined “electronic surveillance,” 50 U.S.C. § 1801(f), carefully and somewhat narrowly.⁶

In addition, Congress addressed, to some degree, the manner in which FISA might apply after a formal declaration of war by expressly allowing warrantless surveillance for a period of fifteen days following such a declaration. Section 111 of FISA allows the President to “authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by the Congress.” 50 U.S.C. § 1811.

The legislative history of FISA shows that Congress understood it was legislating on fragile constitutional ground and was pressing or even exceeding constitutional limits in regulating the President’s authority in the field of foreign intelligence. The final House Conference Report, for example, recognized that the statute’s restrictions might well impermissibly infringe on the President’s constitutional powers. That report includes the extraordinary acknowledgment that “[t]he conferees agree that the establishment by this act of exclusive means by which the President may conduct electronic surveillance does not foreclose a different decision by the Supreme Court.” H.R. Conf. Rep. No. 95-1720, at 35, *reprinted in* 1978 U.S.C.C.A.N. 4048, 4064. But, invoking Justice Jackson’s concurrence in the *Steel Seizure* case, the Conference Report explained that Congress intended in FISA to exert whatever power Congress constitutionally had over the subject matter to restrict foreign intelligence surveillance and to leave the President solely with whatever inherent constitutional authority he might be able to invoke against Congress’s express wishes. *Id.* The Report thus explains that “[t]he intent of the conferees is to apply the standard set forth in Justice Jackson’s concurring opinion in the *Steel Seizure* Case: ‘When a President takes measures incompatible with the express or implied

⁶ FISA’s legislative history reveals that these provisions were intended to exclude certain intelligence activities conducted by the National Security Agency from the coverage of FISA. According to the report of the Senate Judiciary Committee on FISA, “this provision [referencing what became the first part of section 2511(2)(f)] is designed to make clear that the legislation does not deal with international signals intelligence activities as currently engaged in by the National Security Agency and electronic surveillance conducted outside the United States.” S. Rep. No. 95-604, at 64 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3965. The legislative history also makes clear that the definition of “electronic surveillance” was crafted for the same reason. *See id.* at 33-34, 1978 U.S.C.C.A.N. at 3934-36. FISA thereby “adopts the view expressed by the Attorney General during the hearings that enacting statutory controls to regulate the National Security Agency and the surveillance of Americans abroad raises problems best left to separate legislation.” *Id.* at 64, 1978 U.S.C.C.A.N. at 3965. Such legislation placing limitations on traditional NSA activities was drafted, but never passed. *See* National Intelligence Reorganization and Reform Act of 1978: Hearings Before the Senate Select Committee on Intelligence, 95th Cong., 2d Sess. 999-1007 (1978) (text of unenacted legislation). And Congress understood that the NSA surveillance that it intended categorically to exclude from FISA could include the monitoring of international communications into or out of the United States of U.S. citizens. The report specifically referred to the Church Committee report for its description of the NSA’s activities, S. Rep. No. 95-604, at 64 n.63, 1978 U.S.C.C.A.N. at 3965-66 n.63, which stated that “the NSA intercepts messages passing over international lines of communication, some of which have one terminal within the United States. Traveling over these lines of communication, especially those with one terminal in the United States, are messages of Americans” S. Rep. 94-755, at Book II, 308 (1976). Congress’s understanding in the legislative history of FISA that such communications could be intercepted outside FISA procedures is notable.

will of Congress, his power is at the lowest ebb, for then he can rely only upon his own constitutional power minus any constitutional power of Congress over the matter.” *Id.* (quoting *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 637 (1952) (Jackson, J., concurring)); *see also* S. Rep. No. 95-604, at 64, *reprinted in* 1978 U.S.C.C.A.N. at 3966 (same); *see generally* Elizabeth B. Bazen et al., Congressional Research Service, *Re: Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information* 28-29 (Jan. 5, 2006). It is significant, however, that Congress did not decide conclusively to continue to push the boundaries of its constitutional authority in wartime. Instead, Congress reserved the question of the appropriate procedures to regulate electronic surveillance in time of war, and established a fifteen-day period during which the President would be permitted to engage in electronic surveillance without complying with FISA’s express procedures and during which Congress would have the opportunity to revisit the issue. *See* 50 U.S.C. § 1811; H.R. Conf. Rep. No. 95-1720, at 34, *reprinted in* 1978 U.S.C.C.A.N. at 4063 (noting that the purpose of the fifteen-day period following a declaration of war in section 111 of FISA was to “allow time for consideration of any amendment to this act that may be appropriate during a wartime emergency”).

B. FISA CONTEMPLATES AND ALLOWS SURVEILLANCE AUTHORIZED “BY STATUTE”

Congress did not attempt through FISA to prohibit the Executive Branch from using electronic surveillance. Instead, Congress acted to bring the exercise of that power under more stringent congressional control. *See, e.g.*, H. Conf. Rep. No. 95-1720, at 32, *reprinted in* 1978 U.S.C.C.A.N. 4048, 4064. Congress therefore enacted a regime intended to supplant the President’s reliance on his own constitutional authority. Consistent with this overriding purpose of bringing the use of electronic surveillance under *congressional* control and with the commonsense notion that the Congress that enacted FISA could not bind future Congresses, FISA expressly contemplates that the Executive Branch may conduct electronic surveillance outside FISA’s express procedures if and when a subsequent statute authorizes such surveillance.

Thus, section 109 of FISA prohibits any person from intentionally “engag[ing] . . . in electronic surveillance under color of law *except as authorized by statute.*” 50 U.S.C. § 1809(a)(1) (emphasis added). Because FISA’s prohibitory provision broadly exempts surveillance “authorized by statute,” the provision demonstrates that Congress did not attempt to regulate through FISA electronic surveillance authorized by Congress through a subsequent enactment. The use of the term “statute” here is significant because it strongly suggests that *any* subsequent authorizing statute, not merely one that amends FISA itself, could legitimately authorize surveillance outside FISA’s standard procedural requirements. *Compare* 18 U.S.C. § 2511(1) (“Except as otherwise specifically provided *in this chapter* any person who—(a) intentionally intercepts . . . any wire, oral, or electronic communication[] . . . shall be punished . . .”) (emphasis added); *id.* § 2511(2)(e) (providing a defense to liability to individuals “conduct[ing] electronic surveillance, . . . as authorized by *that Act [FISA]*”) (emphasis added). In enacting FISA, therefore, Congress contemplated the possibility that the President might be permitted to conduct electronic surveillance pursuant to a later-enacted statute that did not

incorporate all of the procedural requirements set forth in FISA or that did not expressly amend FISA itself.

To be sure, the scope of this exception is rendered less clear by the conforming amendments that FISA made to chapter 119 of title 18—the portion of the criminal code that provides the mechanism for obtaining wiretaps for law enforcement purposes. Before FISA was enacted, chapter 119 made it a criminal offense for any person to intercept a communication except as specifically provided in that chapter. *See* 18 U.S.C. § 2511(1)(a), (4)(a). Section 201(b) of FISA amended that chapter to provide an exception from criminal liability for activities conducted pursuant to FISA. Specifically, FISA added 18 U.S.C. § 2511(2)(e), which provides that it is not unlawful for “an officer, employee, or agent of the United States . . . to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.” *Id.* § 2511(2)(e). Similarly, section 201(b) of FISA amended chapter 119 to provide that “procedures in this chapter [or chapter 121 (addressing access to stored wire and electronic communications and customer records)] and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.” *Id.* § 2511(2)(f) (West Supp. 2005).⁷

The amendments that section 201(b) of FISA made to title 18 are fully consistent, however, with the conclusion that FISA contemplates that a subsequent statute could authorize electronic surveillance outside FISA’s express procedural requirements. Section 2511(2)(e) of title 18, which provides that it is “not unlawful” for an officer of the United States to conduct electronic surveillance “as authorized by” FISA, is best understood as a safe-harbor provision. Because of section 109, the protection offered by section 2511(2)(e) for surveillance “authorized by” FISA extends to surveillance that is authorized by any other statute and therefore excepted from the prohibition of section 109. In any event, the purpose of section 2511(2)(e) is merely to make explicit what would already have been implicit—that those authorized by statute to engage in particular surveillance do not act unlawfully when they conduct such surveillance. Thus, even if that provision had not been enacted, an officer conducting surveillance authorized by statute (whether FISA or some other law) could not reasonably have been thought to be violating Title III. Similarly, section 2511(2)(e) cannot be read to require a result that would be manifestly unreasonable—exposing a federal officer to criminal liability for engaging in surveillance authorized by statute, merely because the authorizing statute happens not to be FISA itself.

Nor could 18 U.S.C. § 2511(2)(f), which provides that the “procedures in this chapter . . . and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance . . . may be conducted,” have been intended to trump the commonsense approach of section 109 and preclude a subsequent Congress from authorizing the President to engage in electronic surveillance through a statute other than FISA, using procedures other than those outlined in FISA or chapter 119 of title 18. The legislative history of section 2511(2)(f) clearly indicates an intent to prevent the President from engaging in surveillance except as

⁷ The bracketed portion was added in 1986 amendments to section 2511(2)(f). *See* Pub. L. No. 99-508 § 101(b)(3), 100 Stat. 1848, 1850.

authorized by Congress, *see* H.R. Conf. Rep. No. 95-1720, at 32, *reprinted in* 1978 U.S.C.C.A.N. 4048, 4064, which explains why section 2511(2)(f) set forth all then-existing statutory restrictions on electronic surveillance. Section 2511(2)(f)'s reference to "exclusive means" reflected the state of statutory authority for electronic surveillance in 1978 and cautioned the President not to engage in electronic surveillance outside congressionally sanctioned parameters. It is implausible to think that, in attempting to limit the *President's* authority, Congress also limited its own future authority by barring subsequent Congresses from authorizing the Executive to engage in surveillance in ways not specifically enumerated in FISA or chapter 119, or by requiring a subsequent Congress specifically to amend FISA and section 2511(2)(f). There would be a serious question as to whether the Ninety-Fifth Congress could have so tied the hands of its successors. *See, e.g., Fletcher v. Peck*, 10 U.S. (6 Cranch) 87, 135 (1810) (noting that "one legislature cannot abridge the powers of a succeeding legislature"); *Reichelderfer v. Quinn*, 287 U.S. 315, 318 (1932) ("[T]he will of a particular Congress . . . does not impose itself upon those to follow in succeeding years"); *Lockhart v. United States*, 126 S. Ct. 699, 703 (2005) (Scalia, J., concurring) (collecting precedent); 1 W. Blackstone, *Commentaries on the Laws of England* 90 (1765) ("Acts of parliament derogatory from the power of subsequent parliaments bind not"). In the absence of a clear statement to the contrary, it cannot be presumed that Congress attempted to abnegate its own authority in such a way.

Far from a clear statement of congressional intent to bind itself, there are indications that section 2511(2)(f) cannot be interpreted as requiring that *all* electronic surveillance and domestic interception be conducted under FISA's enumerated procedures or those of chapter 119 of title 18 until and unless those provisions are repealed or amended. Even when section 2511(2)(f) was enacted (and no subsequent authorizing statute existed), it could not reasonably be read to preclude all electronic surveillance conducted outside the procedures of FISA or chapter 119 of title 18. In 1978, use of a pen register or trap and trace device constituted electronic surveillance as defined by FISA. *See* 50 U.S.C. §§ 1801(f), (n). Title I of FISA provided procedures for obtaining court authorization for the use of pen registers to obtain foreign intelligence information. But the Supreme Court had, just prior to the enactment of FISA, held that chapter 119 of title 18 did not govern the use of pen registers. *See United States v. New York Tel. Co.*, 434 U.S. 159, 165-68 (1977). Thus, if section 2511(2)(f) were to be read to permit of no exceptions, the use of pen registers for purposes other than to collect foreign intelligence information would have been unlawful because such use would not have been authorized by the "exclusive" procedures of section 2511(2)(f), *i.e.*, FISA and chapter 119. But no court has held that pen registers could not be authorized outside the foreign intelligence context. Indeed, FISA appears to have recognized this issue by providing a defense to liability for any official who engages in electronic surveillance under a search warrant or court order. *See* 50 U.S.C. § 1809(b). (The practice when FISA was enacted was for law enforcement officers to obtain search warrants under the Federal Rules of Criminal Procedure authorizing the installation and use of pen registers. *See S. 1667, A Bill to Amend Title 18, United States Code, with Respect to the Interception of Certain Communications, Other Forms of Surveillance, and for Other Purposes: Hearing Before the Subcomm. On Patents, Copyrights and Trademarks of the Senate*

Comm. on the Judiciary, 99th Cong. 57 (1985) (prepared statement of James Knapp, Deputy Assistant Attorney General, Criminal Division)).⁸

In addition, section 2511(2)(a)(ii) authorizes telecommunications providers to assist officers of the Government engaged in electronic surveillance when the Attorney General certifies that “no warrant or court order is required by law [and] that all statutory requirements have been met.” 18 U.S.C. § 2511(2)(a)(ii).⁹ If the Attorney General can certify, in good faith, that the requirements of a subsequent statute authorizing electronic surveillance are met, service providers are affirmatively and expressly authorized to assist the Government. Although FISA does allow the Government to proceed without a court order in several situations, *see* 50 U.S.C. § 1805(f) (emergencies); *id.* § 1802 (certain communications between foreign governments), this provision specifically lists only Title III’s emergency provision but speaks generally to Attorney General certification. That reference to Attorney General certification is consistent with the historical practice in which Presidents have delegated to the Attorney General authority to approve warrantless surveillance for foreign intelligence purposes. *See, e.g., United States v. United States District Court*, 444 F.2d 651, 669-71 (6th Cir. 1971) (reproducing as an appendix memoranda from Presidents Roosevelt, Truman, and Johnson). Section 2511(2)(a)(ii) thus suggests that telecommunications providers can be authorized to assist with warrantless electronic surveillance when such surveillance is authorized by law outside FISA.

In sum, by expressly and broadly excepting from its prohibition electronic surveillance undertaken “as authorized by statute,” section 109 of FISA permits an exception to the “procedures” of FISA referred to in 18 U.S.C. § 2511(2)(f) where authorized by another statute, even if the other authorizing statute does not specifically amend section 2511(2)(f).

C. THE AUMF IS A “STATUTE” AUTHORIZING SURVEILLANCE OUTSIDE THE CONFINES OF FISA

The AUMF qualifies as a “statute” authorizing electronic surveillance within the meaning of section 109 of FISA.

First, because the term “statute” historically has been given broad meaning, the phrase “authorized by statute” in section 109 of FISA must be read to include joint resolutions such as

⁸ Alternatively, section 109(b) may be read to constitute a “procedure” in FISA or to incorporate procedures from sources other than FISA (such as the Federal Rules of Criminal Procedure or state court procedures), and in that way to satisfy section 2511(2)(f). But if section 109(b)’s defense can be so read, section 109(a) should also be read to constitute a procedure or incorporate procedures not expressly enumerated in FISA.

⁹ Section 2511(2)(a)(ii) states:

Notwithstanding any other law, providers of wire or electronic communication service, . . . are authorized by law to provide information, facilities, or technical assistance to persons authorized by law to intercept . . . communications or to conduct electronic surveillance, as defined [by FISA], if such provider . . . has been provided with . . . a certification in writing by [specified persons proceeding under Title III’s emergency provision] or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specific assistance is required.

the AUMF. See *American Fed'n of Labor v. Watson*, 327 U. S. 582, 592-93 (1946) (finding the term “statute” as used in 28 U.S.C. § 380 to mean “a compendious summary of various enactments, by whatever method they may be adopted, to which a State gives her sanction”); Black’s Law Dictionary 1410 (6th ed. 1990) (defining “statute” broadly to include any “formal written enactment of a legislative body,” and stating that the term is used “to designate the legislatively created laws in contradistinction to court decided or unwritten laws”). It is thus of no significance to this analysis that the AUMF was enacted as a joint resolution rather than a bill. See, e.g., *Ann Arbor R.R. Co. v. United States*, 281 U.S. 658, 666 (1930) (joint resolutions are to be construed by applying “the rules applicable to legislation in general”); *United States ex rel. Levey v. Stockslager*, 129 U.S. 470, 475 (1889) (joint resolution had “all the characteristics and effects” of statute that it suspended); *Padilla ex rel. Newman v. Bush*, 233 F. Supp. 2d 564, 598 (S.D.N.Y. 2002) (in analyzing the AUMF, finding that there is “no relevant constitutional difference between a bill and a joint resolution”), *rev’d sub nom. on other grounds, Rumsfeld v. Padilla*, 352 F.3d 695 (2d Cir. 2003), *rev’d*, 542 U.S. 426 (2004); see also Letter for the Hon. John Conyers, Jr., U.S. House of Representatives, from Prof. Laurence H. Tribe at 3 (Jan. 6, 2006) (term “statute” in section 109 of FISA “of course encompasses a joint resolution presented to and signed by the President”).

Second, the longstanding history of communications intelligence as a fundamental incident of the use of force and the Supreme Court’s decision in *Hamdi v. Rumsfeld* strongly suggest that the AUMF satisfies the requirement of section 109 of FISA for statutory authorization of electronic surveillance. As explained above, it is not necessary to demarcate the outer limits of the AUMF to conclude that it encompasses electronic surveillance targeted at the enemy. Just as a majority of the Court concluded in *Hamdi* that the AUMF authorizes detention of U.S. citizens who are enemy combatants without expressly mentioning the President’s long-recognized power to detain, so too does it authorize the use of electronic surveillance without specifically mentioning the President’s equally long-recognized power to engage in communications intelligence targeted at the enemy. And just as the AUMF satisfies the requirement in 18 U.S.C. § 4001(a) that no U.S. citizen be detained “except pursuant to an Act of Congress,” so too does it satisfy section 109’s requirement for statutory authorization of electronic surveillance.¹⁰ In authorizing the President’s use of force in response to the September 11th attacks, Congress did not need to comb through the United States Code looking for those restrictions that it had placed on national security operations during times of peace and designate with specificity each traditional tool of military force that it sought to authorize the President to use. There is no historical precedent for such a requirement: authorizations to use

¹⁰ It might be argued that Congress dealt more comprehensively with electronic surveillance in FISA than it did with detention in 18 U.S.C. § 4001(a). Thus, although Congress prohibited detention “except pursuant to an Act of Congress,” it combined the analogous prohibition in FISA (section 109(a)) with section 2511(2)(f)’s exclusivity provision. See Letter to the Hon. Bill Frist, Majority Leader, U.S. Senate, from Professor Curtis A. Bradley *et al.* at 5 n.6 (Jan. 9, 2006) (noting that section 4001(a) does not “attempt[] to create an exclusive mechanism for detention”). On closer examination, however, it is evident that Congress has regulated detention far more meticulously than these arguments suggest. Detention is the topic of much of the Criminal Code, as well as a variety of other statutes, including those providing for civil commitment of the mentally ill and confinement of alien terrorists. The existence of these statutes and accompanying extensive procedural safeguards, combined with the substantial constitutional issues inherent in detention, see, e.g., *Hamdi*, 542 U.S. at 574-75 (Scalia, J., dissenting), refute any such argument.

military force traditionally have been couched in general language. Indeed, prior administrations have interpreted joint resolutions declaring war and authorizing the use of military force to authorize expansive collection of communications into and out of the United States.¹¹

Moreover, crucial to the Framers' decision to vest the President with primary constitutional authority to defend the Nation from foreign attack is the fact that the Executive can act quickly, decisively, and flexibly as needed. For Congress to have a role in that process, it must be able to act with similar speed, either to lend its support to, or to signal its disagreement with, proposed military action. Yet the need for prompt decisionmaking in the wake of a devastating attack on the United States is fundamentally inconsistent with the notion that to do so Congress must legislate at a level of detail more in keeping with a peacetime budget reconciliation bill. In emergency situations, Congress must be able to use broad language that effectively sanctions the President's use of the core incidents of military force. That is precisely what Congress did when it passed the AUMF on September 14, 2001—just three days after the deadly attacks on America. The Capitol had been evacuated on September 11th, and Congress was meeting in scattered locations. As an account emerged of who might be responsible for these attacks, Congress acted quickly to authorize the President to use “all necessary and appropriate force” against the enemy that he determines was involved in the September 11th attacks. Under these circumstances, it would be unreasonable and wholly impractical to demand that Congress specifically amend FISA in order to assist the President in defending the Nation. Such specificity would also have been self-defeating because it would have apprised our adversaries of some of our most sensitive methods of intelligence gathering.¹²

Section 111 of FISA, 50 U.S.C. § 1811, which authorizes the President, “[n]otwithstanding any other law,” to conduct “electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by Congress,” does not require a different reading of the AUMF. *See also id.* § 1844 (same provision for pen registers); *id.* § 1829 (same provision for physical searches). Section 111 cannot reasonably be read as Congress's final word on electronic surveillance during wartime, thus permanently limiting the President in all

¹¹ As noted above, in intercepting communications, President Wilson relied on his constitutional authority and the joint resolution declaring war and authorizing the use of military force, which, as relevant here, provided “that the President [is] authorized and directed to employ the entire naval and military forces of the United States and the resources of the Government to carry on war against the Imperial German Government; and to bring the conflict to a successful termination all of the resources of the country are hereby pledged by the Congress of the United States.” Joint Resolution of Apr. 6, 1917, ch. 1, 40 Stat. 1. The authorization did not explicitly mention interception of communications.

¹² Some have suggested that the Administration declined to seek a specific amendment to FISA allowing the NSA activities “because it was advised that Congress would reject such an amendment,” Letter to the Hon. Bill Frist, Majority Leader, U.S. Senate, from Professor Curtis A. Bradley *et al.* 4 & n.4 (Jan. 9, 2005), and they have quoted in support of that assertion the Attorney General's statement that certain Members of Congress advised the Administration that legislative relief “would be difficult, if not impossible.” *Id.* at 4 n.4. As the Attorney General subsequently indicated, however, the difficulty with such specific legislation was that it could not be enacted “without compromising the program.” *See* Remarks by Homeland Security Secretary Chertoff and Attorney General Gonzales on the USA PATRIOT Act (Dec. 21, 2005), *available at* <http://www.dhs.gov/dhspublic/display?content=5285>.

circumstances to a mere fifteen days of warrantless military intelligence gathering targeted at the enemy following a declaration of war. Rather, section 111 represents Congress's recognition that it would likely have to return to the subject and provide additional authorization to conduct warrantless electronic surveillance outside FISA during time of war. The Conference Report explicitly stated the conferees' "inten[t] that this [fifteen-day] period will allow time for consideration of any amendment to this act that may be appropriate during a wartime emergency." H.R. Conf. Rep. No. 95-1720, at 34, *reprinted in* 1978 U.S.C.C.A.N. at 4063. Congress enacted section 111 so that the President could conduct warrantless surveillance while Congress considered supplemental wartime legislation.

Nothing in the terms of section 111 disables Congress from authorizing such electronic surveillance as a traditional incident of war through a broad, conflict-specific authorization for the use of military force, such as the AUMF. Although the legislative history of section 111 indicates that in 1978 some Members of Congress believed that any such authorization would come in the form of a particularized amendment to FISA itself, section 111 does not require that result. Nor could the Ninety-Fifth Congress tie the hands of a subsequent Congress in this way, at least in the absence of far clearer statutory language expressly requiring that result. *See supra*, pp. 21-22; *compare, e.g.*, War Powers Resolution, § 8, 50 U.S.C. § 1547(a) ("Authority to introduce United States Armed Forces into hostilities . . . shall not be inferred . . . from any provision of law . . . unless such provision specifically authorizes [such] introduction . . . and states that it is intended to constitute specific statutory authorization within the meaning of this chapter."); 10 U.S.C. § 401 (stating that any other provision of law providing assistance to foreign countries to detect and clear landmines shall be subject to specific limitations and may be construed as superseding such limitations "only if, and to the extent that, such provision specifically refers to this section and specifically identifies the provision of this section that is to be considered superseded or otherwise inapplicable"). An interpretation of section 111 that would disable Congress from authorizing broader electronic surveillance in that form can be reconciled neither with the purposes of section 111 nor with the well-established proposition that "one legislature cannot abridge the powers of a succeeding legislature." *Fletcher v. Peck*, 10 U.S. (6 Cranch) at 135; *see supra* Part II.B. For these reasons, the better interpretation is that section 111 was not intended to, and did not, foreclose Congress from using the AUMF as the legal vehicle for supplementing the President's existing authority under FISA in the battle against al Qaeda.

The contrary interpretation of section 111 also ignores the important differences between a formal declaration of war and a resolution such as the AUMF. As a historical matter, a formal declaration of war was no longer than a sentence, and thus Congress would not expect a declaration of war to outline the extent to which Congress authorized the President to engage in various incidents of waging war. Authorizations for the use of military force, by contrast, are typically more detailed and are made for the *specific purpose* of reciting the manner in which Congress has authorized the President to act. Thus, Congress could reasonably expect that an authorization for the use of military force would address the issue of wartime surveillance, while a declaration of war would not. Here, the AUMF declares that the Nation faces "an unusual and extraordinary threat," acknowledges that "the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States," and

provides that the President is authorized “to use all necessary and appropriate force” against those “he determines” are linked to the September 11th attacks. AUMF pmb., § 2. This sweeping language goes far beyond the bare terms of a declaration of war. *Compare, e.g.*, Act of Apr. 25, 1898, ch. 189, 30 Stat. 364 (“First. That war be, and the same is hereby declared to exist . . . between the United States of America and the Kingdom of Spain.”).

Although legislation that has included a declaration of war has often also included an authorization of the President to use force, these provisions are separate and need not be combined in a single statute. *See, e.g., id.* (“Second. That the President of the United States be, and he hereby is, directed and empowered to use the entire land and naval forces of the United States, and to call into the actual service of the United States the militia of the several states, *to such extent as may be necessary to carry this Act into effect.*”) (emphasis added). Moreover, declarations of war have legal significance independent of any additional authorization of force that might follow. *See, e.g.*, Louis Henkin, *Foreign Affairs and the U.S. Constitution* 75 (2d ed. 1996) (explaining that a formal state of war has various legal effects, such as terminating diplomatic relations, and abrogating or suspending treaty obligations and international law rights and duties); *see also id.* at 370 n.65 (speculating that one reason to fight an undeclared war would be to “avoid the traditional consequences of declared war on relations with third nations or even . . . belligerents”).

In addition, section 111 does not cover the vast majority of modern military conflicts. The last declared war was World War II. Indeed, the most recent conflict prior to the passage of FISA, Vietnam, was fought without a formal declaration of war. In addition, the War Powers Resolution, enacted less than five years before FISA, clearly recognizes the distinctions between formal declarations of war and authorizations of force and demonstrates that, if Congress had wanted to include such authorizations in section 111, it knew how to do so. *See, e.g.*, 50 U.S.C. § 1544(b) (attempting to impose certain consequences 60 days after reporting the initiation of hostilities to Congress “unless the Congress . . . has declared war *or has enacted a specific authorization for such use*” of military force) (emphasis added). It is possible that, in enacting section 111, Congress intended to make no provision for even the temporary use of electronic surveillance without a court order for what had become the legal regime for most military conflicts. A better reading, however, is that Congress assumed that such a default provision would be unnecessary because, if it had acted through an authorization for the use of military force, the more detailed provisions of that authorization would resolve the extent to which Congress would attempt to authorize, or withhold authorization for, the use of electronic surveillance.¹³

¹³ Some have pointed to the specific amendments to FISA that Congress made shortly after September 11th in the USA PATRIOT Act, Pub. L. No. 107-56, §§ 204, 218, 115 Stat. 272, 281, 291 (2001), to argue that Congress did not contemplate electronic surveillance outside the parameters of FISA. *See* Memorandum for Members of the House Permanent Select Comm. on Intel. from Jeffrey H. Smith, *Re: Legal Authorities Regarding Warrantless Surveillance of U.S. Persons* 6-7 (Jan. 3, 2006). The USA PATRIOT Act amendments, however, do not justify giving the AUMF an unnaturally narrow reading. The USA PATRIOT Act amendments made important corrections in the general application of FISA; they were not intended to define the precise incidents of military force that would be available to the President in prosecuting the current armed conflict against al Qaeda and its allies. Many removed long-standing impediments to the effectiveness of FISA that had contributed to the

* * *

The broad text of the AUMF, the authoritative interpretation that the Supreme Court gave it in *Hamdi*, and the circumstances in which it was passed demonstrate that the AUMF is a statute authorizing electronic surveillance under section 109 of FISA. When the President authorizes electronic surveillance against the enemy pursuant to the AUMF, he is therefore acting at the height of his authority under *Youngstown*, 343 U.S. at 637 (Jackson, J., concurring).

D. THE CANON OF CONSTITUTIONAL AVOIDANCE REQUIRES RESOLVING IN FAVOR OF THE PRESIDENT'S AUTHORITY ANY AMBIGUITY ABOUT WHETHER FISA FORBIDS THE NSA ACTIVITIES

As explained above, the AUMF fully authorizes the NSA activities. Because FISA contemplates the possibility that subsequent statutes could authorize electronic surveillance without requiring FISA's standard procedures, the NSA activities are also consistent with FISA and related provisions in title 18. Nevertheless, some might argue that sections 109 and 111 of FISA, along with section 2511(2)(f)'s "exclusivity" provision and section 2511(2)(e)'s liability exception for officers engaged in FISA-authorized surveillance, are best read to suggest that FISA requires that subsequent authorizing legislation specifically amend FISA in order to free the Executive from FISA's enumerated procedures. As detailed above, this is not the better reading of FISA. But even if these provisions were ambiguous, any doubt as to whether the AUMF and FISA should be understood to allow the President to make tactical military decisions to authorize surveillance outside the parameters of FISA must be resolved to avoid the serious constitutional questions that a contrary interpretation would raise.

It is well established that the first task of any interpreter faced with a statute that may present an unconstitutional infringement on the powers of the President is to determine whether the statute may be construed to avoid the constitutional difficulty. "[I]f an otherwise acceptable

maintenance of an unnecessary "wall" between foreign intelligence gathering and criminal law enforcement; others were technical clarifications. See *In re Sealed Case*, 310 F.3d 717, 725-30 (Foreign Int. Surv. Ct. Rev. 2002). The "wall" had been identified as a significant problem hampering the Government's efficient use of foreign intelligence information well before the September 11th attacks and in contexts unrelated to terrorism. See, e.g., *Final Report of the Attorney General's Review Team on the Handling of the Los Alamos National Laboratory Investigation* 710, 729, 732 (May 2000); General Accounting Office, *FBI Intelligence Investigations: Coordination Within Justice on Counterintelligence Criminal Matters Is Limited* (GAO-01-780) 3, 31 (July 2001). Finally, it is worth noting that Justice Souter made a similar argument in *Hamdi* that the USA PATRIOT Act all but compelled a narrow reading of the AUMF. See 542 U.S. at 551 ("It is very difficult to believe that the same Congress that carefully circumscribed Executive power over alien terrorists on home soil [in the USA PATRIOT Act] would not have meant to require the Government to justify clearly its detention of an American citizen held on home soil incommunicado."). Only Justice Ginsburg joined this opinion, and the position was rejected by a majority of Justices.

Nor do later amendments to FISA undermine the conclusion that the AUMF authorizes electronic surveillance outside the procedures of FISA. Three months after the enactment of the AUMF, Congress enacted certain "technical amendments" to FISA which, *inter alia*, extended the time during which the Attorney General may issue an emergency authorization of electronic surveillance from 24 to 72 hours. See Intelligence Authorization Act for Fiscal Year 2002, Pub. L. No. 107-108, § 314, 115 Stat. 1394, 1402 (2001). These modifications to FISA do not in any way undermine Congress's previous authorization in the AUMF for the President to engage in electronic surveillance outside the parameters of FISA in the specific context of the armed conflict with al Qaeda.

construction of a statute would raise serious constitutional problems, and where an alternative interpretation of the statute is ‘fairly possible,’ we are obligated to construe the statute to avoid such problems.” *INS v. St. Cyr*, 533 U.S. 289, 299-300 (2001) (citations omitted); *Ashwander v. TVA*, 297 U.S. 288, 345-48 (1936) (Brandeis, J., concurring). Moreover, the canon of constitutional avoidance has particular importance in the realm of national security, where the President’s constitutional authority is at its highest. See *Department of the Navy v. Egan*, 484 U.S. 518, 527, 530 (1988); 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”). Thus, courts and the Executive Branch typically construe a general statute, even one that is written in unqualified terms, to be implicitly limited so as not to infringe on the President’s Commander in Chief powers.

Reading FISA to prohibit the NSA activities would raise two serious constitutional questions, both of which must be avoided if possible: (1) whether the signals intelligence collection the President determined was necessary to undertake is such a core exercise of Commander in Chief control over the Armed Forces during armed conflict that Congress cannot interfere with it at all and (2) whether the particular restrictions imposed by FISA are such that their application would impermissibly impede the President’s exercise of his constitutionally assigned duties as Commander in Chief. Constitutional avoidance principles require interpreting FISA, at least in the context of the military conflict authorized by the AUMF, to avoid these questions, if “fairly possible.” Even if Congress intended FISA to use the full extent of its constitutional authority to “occupy the field” of “electronic surveillance,” as FISA used that term, during peacetime, the legislative history indicates that Congress had not reached a definitive conclusion about its regulation during wartime. See H.R. Conf. Rep. No. 95-1720, at 34, *reprinted in* 1978 U.S.C.C.A.N. at 4063 (noting that the purpose of the fifteen-day period following a declaration of war in section 111 of FISA was to “allow time for consideration of any amendment to this act that may be appropriate during a wartime emergency”). Therefore, it is not clear that Congress, in fact, intended to test the limits of its constitutional authority in the context of wartime electronic surveillance.

Whether Congress may interfere with the President’s constitutional authority to collect foreign intelligence information through interception of communications reasonably believed to be linked to the enemy poses a difficult constitutional question. As explained in Part I, it had long been accepted at the time of FISA’s enactment that the President has inherent constitutional authority to conduct warrantless electronic surveillance for foreign intelligence purposes. Congress recognized at the time that the enactment of a statute purporting to eliminate the President’s ability, even during peacetime, to conduct warrantless electronic surveillance to collect foreign intelligence was near or perhaps beyond the limit of Congress’s Article I powers. The NSA activities, however, involve signals intelligence performed in the midst of a congressionally authorized armed conflict undertaken to prevent further hostile attacks on the United States. The NSA activities lie at the very core of the Commander in Chief power, especially in light of the AUMF’s explicit authorization for the President to take *all* necessary and appropriate military action to stop al Qaeda from striking again. The constitutional principles at stake here thus involve not merely the President’s well-established inherent

authority to conduct warrantless surveillance for foreign intelligence purposes during peacetime, but also the powers and duties expressly conferred on him as Commander in Chief by Article II.

Even outside the context of wartime surveillance of the enemy, the source and scope of Congress's power to restrict the President's inherent authority to conduct foreign intelligence surveillance is unclear. As explained above, the President's role as sole organ for the Nation in foreign affairs has long been recognized as carrying with it preeminent authority in the field of national security and foreign intelligence. The source of this authority traces to the Vesting Clause of Article II, which states that "[t]he executive Power shall be vested in a President of the United States of America." U.S. Const. art. II, § 1. The Vesting Clause "has long been held to confer on the President plenary authority to represent the United States and to pursue its interests outside the borders of the country, subject only to limits specifically set forth in the Constitution itself and to such statutory limitations as the Constitution permits Congress to impose by exercising one of its enumerated powers." *The President's Compliance with the "Timely Notification" Requirement of Section 501(b) of the National Security Act*, 10 Op. O.L.C. 159, 160-61 (1986) ("*Timely Notification Requirement Op.*").

Moreover, it is clear that some presidential authorities in this context are beyond Congress's ability to regulate. For example, as the Supreme Court explained in *Curtiss-Wright*, the President "*makes* treaties with the advice and consent of the Senate; but he alone negotiates. Into the field of negotiation the Senate cannot intrude; and Congress itself is powerless to invade it." 299 U.S. at 319. Similarly, President Washington established early in the history of the Republic the Executive's absolute authority to maintain the secrecy of negotiations with foreign powers, even against congressional efforts to secure information. *See id.* at 320-21. Recognizing presidential authority in this field, the Executive Branch has taken the position that "congressional legislation authorizing extraterritorial diplomatic and intelligence activities is superfluous, and . . . statutes infringing the President's inherent Article II authority would be unconstitutional." *Timely Notification Requirement Op.*, 10 Op. O.L.C. at 164.

There are certainly constitutional limits on Congress's ability to interfere with the President's power to conduct foreign intelligence searches, consistent with the Constitution, within the United States. As explained above, intelligence gathering is at the heart of executive functions. Since the time of the Founding it has been recognized that matters requiring secrecy—and intelligence in particular—are quintessentially executive functions. *See, e.g., The Federalist No. 64*, at 435 (John Jay) (Jacob E. Cooke ed. 1961) ("The convention have done well therefore in so disposing of the power of making treaties, that although the president must in forming them act by the advice and consent of the senate, yet he will be able to manage the business of intelligence in such manner as prudence may suggest."); *see also Timely Notification Requirement Op.*, 10 Op. O.L.C. at 165; *cf. New York Times Co. v. United States*, 403 U.S. 713, 729-30 (1971) (Stewart, J., concurring) ("[I]t is the constitutional duty of the Executive—as a matter of sovereign prerogative and not as a matter of law as the courts know law—through the promulgation and enforcement of executive regulations, to protect the confidentiality necessary to carry out its responsibilities in the field of international relations and national defense.").

Because Congress has rarely attempted to intrude in this area and because many of these questions are not susceptible to judicial review, there are few guideposts for determining exactly where the line defining the President's sphere of exclusive authority lies. Typically, if a statute is in danger of encroaching upon exclusive powers of the President, the courts apply the constitutional avoidance canon, if a construction avoiding the constitutional issue is "fairly possible." *See, e.g., Egan*, 484 U.S. at 527, 530. The only court that squarely has addressed the relative powers of Congress and the President in this field suggested that the balance tips decidedly in the President's favor. The Foreign Intelligence Surveillance Court of Review recently noted that all courts to have addressed the issue of the President's inherent authority 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 (Foreign Intel. Surv. Ct. of Rev. 2002). On the basis of that unbroken line of precedent, the court "[took] for granted that the President does have that authority," and concluded that, "assuming that is so, FISA could not encroach on the President's constitutional power." *Id.*¹⁴ Although the court did not provide extensive analysis, it is the only judicial statement on point, and it comes from the specialized appellate court created expressly to deal with foreign intelligence issues under FISA.

But the NSA activities are not simply exercises of the President's general foreign affairs powers. Rather, they are primarily an exercise of the President's authority as Commander in Chief during an armed conflict that Congress expressly has authorized the President to pursue. The NSA activities, moreover, have been undertaken specifically to prevent a renewed attack at the hands of an enemy that has already inflicted the single deadliest foreign attack in the Nation's history. The core of the Commander in Chief power is the authority to direct the Armed Forces in conducting a military campaign. Thus, the Supreme Court has made clear that the "President alone" is "constitutionally invested with the entire charge of hostile operations." *Hamilton v. Dillin*, 88 U.S. (21 Wall.) 73, 87 (1874); *The Federalist* No. 74, at 500 (Alexander Hamilton). "As commander-in-chief, [the President] is authorized to direct the movements of the naval and military forces placed by law at his command, and to employ them in the manner he may deem most effectual to harass and conquer and subdue the enemy." *Fleming v. Page*, 50 U.S. (9 How.) 603, 615 (1850). As Chief Justice Chase explained in 1866, although Congress has authority to legislate to support the prosecution of a war, Congress may not "*interfere[] with the command of the forces and the conduct of campaigns*. That power and duty belong to the President as commander-in-chief." *Ex parte Milligan*, 71 U.S. (4 Wall.) 2, 139 (1866) (Chase, C.J., concurring in judgment) (emphasis added).

The Executive Branch uniformly has construed the Commander in Chief and foreign affairs powers to grant the President authority that is beyond the ability of Congress to regulate. In 1860, Attorney General Black concluded that an act of Congress, if intended to constrain the President's discretion in assigning duties to an officer in the army, would be unconstitutional:

As commander-in-chief of the army it is your right to decide according to your

¹⁴ In the past, other courts have declined to express a view on that issue one way or the other. *See, e.g., Butenko*, 494 F.2d at 601 ("We do not intimate, at this time, any view whatsoever as the proper resolution of the possible clash of the constitutional powers of the President and Congress.").

own judgment what officer shall perform any particular duty, and as the supreme executive magistrate you have the power of appointment. Congress could not, if it would, take away from the President, or in anywise diminish the authority conferred upon him by the Constitution.

Memorial of Captain Meigs, 9 Op. Att’y Gen. 462, 468 (1860). Attorney General Black went on to explain that, in his view, the statute involved there could probably be read as simply providing “a recommendation” that the President could decline to follow at his discretion. *Id.* at 469-70.¹⁵

Supreme Court precedent does not support claims of congressional authority over core military decisions during armed conflicts. In particular, the two decisions of the Supreme Court that address a conflict between asserted wartime powers of the Commander in Chief and congressional legislation and that resolve the conflict in favor of Congress—*Little v. Barreme*, 6 U.S. (2 Cranch) 170 (1804), and *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952)—are both distinguishable from the situation presented by the NSA activities in the conflict with al Qaeda. Neither supports the constitutionality of the restrictions in FISA as applied here.

Barreme involved a suit brought to recover a ship seized by an officer of the U.S. Navy on the high seas during the so-called “Quasi War” with France in 1799. The seizure had been based upon the officer’s orders implementing an act of Congress suspending commerce between the United States and France and authorizing the seizure of American ships bound to a French port. The ship in question was suspected of sailing from a French port. The Supreme Court held that the orders given by the President could not authorize a seizure beyond the terms of the

¹⁵ Executive practice recognizes, consistent with the Constitution, some congressional control over the Executive’s decisions concerning the Armed Forces. *See, e.g.*, U.S. Const. art. I, § 8, cl. 12 (granting Congress power “to raise and support Armies”). But such examples have not involved congressional attempts to regulate the actual conduct of a military campaign, and there is no comparable textual support for such interference. For example, just before World War II, Attorney General Robert Jackson concluded that the Neutrality Act prohibited President Roosevelt from selling certain armed naval vessels and sending them to Great Britain. *See Acquisition of Naval and Air Bases in Exchange for Over-Age Destroyers*, 39 Op. Att’y Gen. 484, 496 (1940). Jackson’s apparent conclusion that Congress could control the President’s ability to transfer war material does not imply acceptance of direct congressional regulation of the Commander in Chief’s control of the means and methods of engaging the enemy in conflict. Similarly, in *Youngstown Sheet & Tube Co. v. Sawyer*, the Truman Administration readily conceded that, if Congress had prohibited the seizure of steel mills by statute, Congress’s action would have been controlling. *See* Brief for Petitioner at 150, *Youngstown*, 343 U.S. 579 (1952) (Nos. 744 and 745). This concession implies nothing concerning congressional control over the methods of engaging the enemy.

Likewise, the fact that the Executive Branch has, at times, sought congressional ratification after taking unilateral action in a wartime emergency does not reflect a concession that the Executive lacks authority in this area. A decision to seek congressional support can be prompted by many motivations, including a desire for political support. In modern times, several administrations have sought congressional authorization for the use of military force while preserving the ability to assert the unconstitutionality of the War Powers Resolution. *See, e.g.*, *Statement on Signing the Resolution Authorizing the Use of Military Force Against Iraq*, 1 Pub. Papers of George Bush 40 (1991) (“[M]y request for congressional support did not . . . constitute any change in the long-standing positions of the executive branch on either the President’s constitutional authority to use the Armed Forces to defend vital U.S. interests or the constitutionality of the War Powers Resolution.”). Moreover, many actions for which congressional support has been sought—such as President Lincoln’s action in raising an Army in 1861—quite likely fall primarily under Congress’s core Article I powers.

statute and therefore that the seizure of the ship not in fact bound *to* a French port was unlawful. *See* 6 U.S. at 177-78. Although some commentators have broadly characterized *Barreme* as standing for the proposition that Congress may restrict by statute the means by which the President can direct the Nation’s Armed Forces to carry on a war, the Court’s holding was limited in at least two significant ways. First, the operative section of the statute in question applied only to *American* merchant ships. *See id.* at 170 (quoting Act of February 9, 1799). Thus, the Court simply had no occasion to rule on whether, even in the limited and peculiar circumstances of the Quasi War, Congress could have placed some restriction on the orders the Commander in Chief could issue concerning direct engagements with enemy forces. Second, it is significant that the statute in *Barreme* was cast expressly, not as a limitation on the conduct of warfare by the President, but rather as regulation of a subject within the core of Congress’s enumerated powers under Article I—the regulation of foreign commerce. *See* U.S. Const., art. I, § 8, cl. 3. The basis of Congress’s authority to act was therefore clearer in *Barreme* than it is here.

Youngstown involved an effort by the President—in the face of a threatened work stoppage—to seize and to run steel mills. Congress had expressly considered the possibility of giving the President power to effect such a seizure during national emergencies. It rejected that option, however, instead providing different mechanisms for resolving labor disputes and mechanisms for seizing industries to ensure production vital to national defense.

For the Court, the connection between the seizure and the core Commander in Chief function of commanding the Armed Forces was too attenuated. The Court pointed out that the case did not involve authority over “day-to-day fighting in a theater of war.” *Id.* at 587. Instead, it involved a dramatic extension of the President’s authority over military operations to exercise control over an industry that was vital for producing equipment needed overseas. Justice Jackson’s concurring opinion also reveals a concern for what might be termed foreign-to-domestic presidential bootstrapping. The United States became involved in the Korean conflict through President Truman’s unilateral decision to commit troops to the defense of South Korea. The President then claimed authority, based upon this foreign conflict, to extend presidential control into vast sectors of the domestic economy. Justice Jackson expressed “alarm[]” at a theory under which “a President whose conduct of foreign affairs is so largely uncontrolled, and often even is unknown, can vastly enlarge his mastery over the internal affairs of the country by his own commitment of the Nation’s armed forces to some foreign venture.” *Id.* at 642.

Moreover, President Truman’s action extended the President’s authority into a field that the Constitution predominantly assigns to Congress. *See id.* at 588 (discussing Congress’s commerce power and noting that “[t]he Constitution does not subject this lawmaking power of Congress to presidential or military supervision or control”); *see also id.* at 643 (Jackson, J., concurring) (explaining that Congress is given express authority to ““raise and *support* Armies”” and ““to *provide* and *maintain* a Navy””) (quoting U.S. Const. art. I, § 8, cls. 12, 13). Thus, *Youngstown* involved an assertion of executive power that not only stretched far beyond the

President's core Commander in Chief functions, but that did so by intruding into areas where Congress had been given an express, and apparently dominant, role by the Constitution.¹⁶

The present situation differs dramatically. The exercise of executive authority involved in the NSA activities is not several steps removed from the actual conduct of a military campaign. As explained above, it is an essential part of the military campaign. Unlike the activities at issue in *Youngstown*, the NSA activities are directed at the enemy, and not at domestic activity that might incidentally aid the war effort. And assertion of executive authority here does not involve extending presidential power into areas reserved for Congress. Moreover, the theme that appeared most strongly in Justice Jackson's concurrence in *Youngstown*—the fear of presidential bootstrapping—does not apply in this context. Whereas President Truman had used his inherent constitutional authority to commit U.S. troops, here Congress expressly provided the President sweeping authority to use “all necessary and appropriate force” to protect the Nation from further attack. AUMF § 2(a). There is thus no bootstrapping concern.

Finally, *Youngstown* cannot be read to suggest that the President's authority for engaging the enemy is less extensive inside the United States than abroad. To the contrary, the extent of the President's Commander in Chief authority necessarily depends on where the enemy is found and where the battle is waged. In World War II, for example, the Supreme Court recognized that the President's authority as Commander in Chief, as supplemented by Congress, included the power to capture and try agents of the enemy in the United States, even if they never had “entered the theatre or zone of active military operations.” *Quirin*, 317 U.S. at 38.¹⁷ In the present conflict, unlike in the Korean War, the battlefield was brought to the United States in the most literal way, and the United States continues to face a threat of further attacks on its soil. In short, therefore, *Youngstown* does not support the view that Congress may constitutionally prohibit the President from authorizing the NSA activities.

The second serious constitutional question is whether the particular restrictions imposed by FISA would impermissibly hamper the President's exercise of his constitutionally assigned duties as Commander in Chief. The President has determined that the speed and agility required to carry out the NSA activities successfully could not have been achieved under FISA.¹⁸ Because the President also has determined that the NSA activities are necessary to the defense of

¹⁶ *Youngstown* does demonstrate that the mere fact that Executive action might be placed in Justice Jackson's category III does not obviate the need for further analysis. Justice Jackson's framework therefore recognizes that Congress might impermissibly interfere with the President's authority as Commander in Chief or to conduct the Nation's foreign affairs.

¹⁷ It had been recognized long before *Youngstown* that, in a large-scale conflict, the area of operations could readily extend to the continental United States, even when there are no major engagements of armed forces here. Thus, in the context of the trial of a German officer for spying in World War I, it was recognized that “[w]ith the progress made in obtaining ways and means for devastation and destruction, the territory of the United States was certainly within the field of active operations” during the war, particularly in the port of New York, and that a spy in the United States might easily have aided the “hostile operation” of U-boats off the coast. *United States ex rel. Wessels v. McDonald*, 265 F. 754, 764 (E.D.N.Y. 1920).

¹⁸ In order to avoid further compromising vital national security activities, a full explanation of the basis for the President's determination cannot be given in an unclassified document.

the United States from a subsequent terrorist attack in the armed conflict with al Qaeda, FISA would impermissibly interfere with the President's most solemn constitutional obligation—to defend the United States against foreign attack.

Indeed, if an interpretation of FISA that allows the President to conduct the NSA activities were not “fairly possible,” FISA would be unconstitutional as applied in the context of this congressionally authorized armed conflict. In that event, FISA would purport to *prohibit* the President from undertaking actions necessary to fulfill his constitutional obligation to protect the Nation from foreign attack in the context of a congressionally authorized armed conflict with an enemy that has already staged the most deadly foreign attack in our Nation's history. A statute may not “*impede* the President's ability to perform his constitutional duty,” *Morrison v. Olson*, 487 U.S. 654, 691 (1988) (emphasis added); *see also id.* at 696-97, particularly not the President's most solemn constitutional obligation—the defense of the Nation. *See also In re Sealed Case*, 310 F.3d at 742 (explaining that “FISA could not encroach on the President's constitutional power”).

Application of the avoidance canon would be especially appropriate here for several reasons beyond the acute constitutional crises that would otherwise result. First, as noted, Congress did not intend FISA to be the final word on electronic surveillance conducted during armed conflicts. Instead, Congress expected that it would revisit the subject in subsequent legislation. Whatever intent can be gleaned from FISA's text and legislative history to set forth a comprehensive scheme for regulating electronic surveillance during peacetime, that same intent simply does not extend to armed conflicts and declared wars.¹⁹ Second, FISA was enacted during the Cold War, not during active hostilities with an adversary whose mode of operation is to blend in with the civilian population until it is ready to strike. These changed circumstances have seriously altered the constitutional calculus, one that FISA's enactors had already recognized might suggest that the statute was unconstitutional. Third, certain technological changes have rendered FISA still more problematic. As discussed above, when FISA was enacted in 1978, Congress expressly declined to regulate through FISA certain signals intelligence activities conducted by the NSA. *See supra*, at pp. 18-19 & n.6.²⁰ These same factors weigh heavily in favor of concluding that FISA would be unconstitutional as applied to the current conflict if the canon of constitutional avoidance could not be used to head off a collision between the Branches.

¹⁹ FISA exempts the President from its procedures for fifteen days following a congressional declaration of war. *See* 50 U.S.C. § 1811. If an adversary succeeded in a decapitation strike, preventing Congress from declaring war or passing subsequent authorizing legislation, it seems clear that FISA could not constitutionally continue to apply in such circumstances.

²⁰ Since FISA's enactment in 1978, the means of transmitting communications has undergone extensive transformation. In particular, many communications that would have been carried by wire are now transmitted through the air, and many communications that would have been carried by radio signals (including by satellite transmissions) are now transmitted by fiber optic cables. It is such technological advancements that have broadened FISA's reach, not any particularized congressional judgment that the NSA's traditional activities in intercepting such international communications should be subject to FISA's procedures. A full explanation of these technological changes would require a discussion of classified information.

As explained above, FISA is best interpreted to allow a statute such as the AUMF to authorize electronic surveillance outside FISA's enumerated procedures. The strongest counterarguments to this conclusion are that various provisions in FISA and title 18, including section 111 of FISA and section 2511(2)(f) of title 18, together require that subsequent legislation must reference or amend FISA in order to authorize electronic surveillance outside FISA's procedures and that interpreting the AUMF as a statute authorizing electronic surveillance outside FISA procedures amounts to a disfavored repeal by implication. At the very least, however, interpreting FISA to allow a subsequent statute such as the AUMF to authorize electronic surveillance without following FISA's express procedures is "fairly possible," and that is all that is required for purposes of invoking constitutional avoidance. In the competition of competing canons, particularly in the context of an ongoing armed conflict, the constitutional avoidance canon carries much greater interpretative force.²¹

IV. THE NSA ACTIVITIES ARE CONSISTENT WITH THE FOURTH AMENDMENT

The Fourth Amendment prohibits "unreasonable searches and seizures" and directs that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and

²¹ If the text of FISA were clear that nothing other than an amendment to FISA could authorize additional electronic surveillance, the AUMF would impliedly repeal as much of FISA as would prevent the President from using "all necessary and appropriate force" in order to prevent al Qaeda and its allies from launching another terrorist attack against the United States. To be sure, repeals by implication are disfavored and are generally not found whenever two statutes are "capable of co-existence." *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1018 (1984). Under this standard, an implied repeal may be found where one statute would "unduly interfere with" the operation of another. *Radzanower v. Touche Ross & Co.*, 426 U.S. 148, 156 (1976). The President's determination that electronic surveillance of al Qaeda outside the confines of FISA was "necessary and appropriate" would create a clear conflict between the AUMF and FISA. FISA's restrictions on the use of electronic surveillance would preclude the President from doing what the AUMF specifically authorized him to do: use all "necessary and appropriate force" to prevent al Qaeda from carrying out future attacks against the United States. The ordinary restrictions in FISA cannot continue to apply if the AUMF is to have its full effect; those constraints would "unduly interfere" with the operation of the AUMF.

Contrary to the recent suggestion made by several law professors and former government officials, the ordinary presumption against implied repeals is overcome here. *Cf.* Letter to the Hon. Bill Frist, Majority Leader, U.S. Senate, from Professor Curtis A. Bradley et al. at 4 (Jan. 9, 2006). First, like other canons of statutory construction, the canon against implied repeals is simply a presumption that may be rebutted by other factors, including conflicting canons. *Connecticut National Bank v. Germain*, 503 U.S. 249, 253 (1992); *see also Chickasaw Nation v. United States*, 534 U.S. 84, 94 (2001); *Circuit City Stores, Inc. v. Adams*, 532 U.S. 105, 115 (2001). Indeed, the Supreme Court has declined to apply the ordinary presumption against implied repeals where other canons apply and suggest the opposite result. *See Montana v. Blackfeet Tribe of Indians*, 471 U.S. 759, 765-66 (1985). Moreover, *Blackfeet* suggests that where the presumption against implied repeals would conflict with other, more compelling interpretive imperatives, it simply does not apply at all. *See* 471 U.S. at 766. Here, in light of the constitutional avoidance canon, which imposes the overriding imperative to use the tools of statutory interpretation to avoid constitutional conflicts, the implied repeal canon either would not apply at all or would apply with significantly reduced force. Second, the AUMF was enacted during an acute national emergency, where the type of deliberation and detail normally required for application of the canon against implied repeals was neither practical nor warranted. As discussed above, in these circumstances, Congress cannot be expected to work through every potential implication of the U.S. Code and to define with particularity each of the traditional incidents of the use of force available to the President.

particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. The touchstone for review of government action under the Fourth Amendment is whether the search is “reasonable.” *See, e.g., Vernonia Sch. Dist. v. Acton*, 515 U.S. 646, 653 (1995).

As noted above, *see* Part I, all of the federal courts of appeals to have addressed the issue have affirmed the President’s inherent constitutional authority to collect foreign intelligence without a warrant. *See In re Sealed Case*, 310 F.3d at 742. Properly understood, foreign intelligence collection in general, and the NSA activities in particular, fit within the “special needs” exception to the warrant requirement of the Fourth Amendment. Accordingly, the mere fact that no warrant is secured prior to the surveillance at issue in the NSA activities does not suffice to render the activities unreasonable. Instead, reasonableness in this context must be assessed under a general balancing approach, “by assessing, on the one hand, the degree to which it intrudes upon an individual’s privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.” *United States v. Knights*, 534 U.S. 112, 118-19 (2001) (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)). The NSA activities are reasonable because the Government’s interest, defending the Nation from another foreign attack in time of armed conflict, outweighs the individual privacy interests at stake, and because they seek to intercept only international communications where one party is linked to al Qaeda or an affiliated terrorist organization.

A. THE WARRANT REQUIREMENT OF THE FOURTH AMENDMENT DOES NOT APPLY TO THE NSA ACTIVITIES

In “the criminal context,” the Fourth Amendment reasonableness requirement “usually requires a showing of probable cause” and a warrant. *Board of Educ. v. Earls*, 536 U.S. 822, 828 (2002). The requirement of a warrant supported by probable cause, however, is not universal. Rather, the Fourth Amendment’s “central requirement is one of reasonableness,” and the rules the Court has developed to implement that requirement “[s]ometimes . . . require warrants.” *Illinois v. McArthur*, 531 U.S. 326, 330 (2001); *see also, e.g., Earls*, 536 U.S. at 828 (noting that the probable cause standard “is peculiarly related to criminal investigations and may be unsuited to determining the reasonableness of administrative searches where the Government seeks to prevent the development of hazardous conditions”) (internal quotation marks omitted).

In particular, the Supreme Court repeatedly has made clear that in situations involving “special needs” that go beyond a routine interest in law enforcement, the warrant requirement is inapplicable. *See Vernonia*, 515 U.S. at 653 (there are circumstances “when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable”) (quoting *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987)); *see also McArthur*, 531 U.S. at 330 (“When faced with special law enforcement needs, diminished expectations of privacy, minimal intrusions, or the like, the Court has found that certain general, or individual, circumstances may render a warrantless search or seizure reasonable.”). It is difficult to encapsulate in a nutshell all of the different circumstances the Court has found to qualify as “special needs” justifying warrantless searches. But one application in which the Court has found the warrant requirement inapplicable is in circumstances in which the Government faces

an increased need to be able to react swiftly and flexibly, or when there are at stake interests in public safety beyond the interests in ordinary law enforcement. One important factor in establishing “special needs” is whether the Government is responding to an emergency that goes beyond the need for general crime control. *See In re Sealed Case*, 310 F.3d at 745-46.

Thus, the Court has permitted warrantless searches of property of students in public schools, *see New Jersey v. T.L.O.*, 469 U.S. 325, 340 (1985) (noting that warrant requirement would “unduly interfere with the maintenance of the swift and informal disciplinary procedures needed in the schools”), to screen athletes and students involved in extracurricular activities at public schools for drug use, *see Vernonia*, 515 U.S. at 654-55; *Earls*, 536 U.S. at 829-38, to conduct drug testing of railroad personnel involved in train accidents, *see Skinner v. Railway Labor Executives’ Ass’n*, 489 U.S. 602, 634 (1989), and to search probationers’ homes, *see Griffin*, 483 U.S. 868. Many special needs doctrine and related cases have upheld *suspicionless* searches or seizures. *See, e.g., Illinois v. Lidster*, 540 U.S. 419, 427 (2004) (implicitly relying on special needs doctrine to uphold use of automobile checkpoint to obtain information about recent hit-and-run accident); *Earls*, 536 U.S. at 829-38 (suspicionless drug testing of public school students involved in extracurricular activities); *Michigan Dep’t of State Police v. Sitz*, 496 U.S. 444, 449-55 (1990) (road block to check all motorists for signs of drunken driving); *United States v. Martinez-Fuerte*, 428 U.S. 543 (1976) (road block near the border to check vehicles for illegal immigrants); *cf. In re Sealed Case*, 310 F.3d at 745-46 (noting that suspicionless searches and seizures in one sense are a greater encroachment on privacy than electronic surveillance under FISA because they are not based on any particular suspicion, but “[o]n the other hand, wiretapping is a good deal more intrusive than an automobile stop accompanied by questioning”). To fall within the “special needs” exception to the warrant requirement, the purpose of the search must be distinguishable from ordinary general crime control. *See, e.g., Ferguson v. Charleston*, 532 U.S. 67 (2001); *City of Indianapolis v. Edmond*, 531 U.S. 32, 41 (2000).

Foreign intelligence collection, especially in the midst of an armed conflict in which the adversary has already launched catastrophic attacks within the United States, fits squarely within the area of “special needs, beyond the normal need for law enforcement” where the Fourth Amendment’s touchstone of reasonableness can be satisfied without resort to a warrant. *Vernonia*, 515 U.S. at 653. The Executive Branch has long maintained that collecting foreign intelligence is far removed from the ordinary criminal law enforcement action to which the warrant requirement is particularly suited. *See, e.g., Amending the Foreign Intelligence Surveillance Act: Hearings Before the House Permanent Select Comm. on Intelligence*, 103d Cong. 2d Sess. 62, 63 (1994) (statement of Deputy Attorney General Jamie S. Gorelick) (“[I]t is important to understand that the rules and methodology for criminal searches are inconsistent with the collection of foreign intelligence and would unduly frustrate the President in carrying out his foreign intelligence responsibilities. . . . [W]e believe that the warrant clause of the Fourth Amendment is inapplicable to such [foreign intelligence] searches.”); *see also In re Sealed Case*, 310 F.3d 745. The object of foreign intelligence collection is securing information necessary to protect the national security from the hostile designs of foreign powers like al Qaeda and affiliated terrorist organizations, including the possibility of another foreign attack on the United States. In foreign intelligence investigations, moreover, the targets of surveillance

often are agents of foreign powers, including international terrorist groups, who may be specially trained in concealing their activities and whose activities may be particularly difficult to detect. The Executive requires a greater degree of flexibility in this field to respond with speed and absolute secrecy to the ever-changing array of foreign threats faced by the Nation.²²

In particular, the NSA activities are undertaken to prevent further devastating attacks on our Nation, and they serve the highest government purpose through means other than traditional law enforcement.²³ The NSA activities are designed to enable the Government to act quickly and flexibly (and with secrecy) to find agents of al Qaeda and its affiliates—an international terrorist group which has already demonstrated a capability to infiltrate American communities without being detected—in time to disrupt future terrorist attacks against the United States. As explained by the Foreign Intelligence Surveillance Court of Review, the nature of the “emergency” posed by al Qaeda “takes the matter out of the realm of ordinary crime control.” *In re Sealed Case*, 310 F.3d at 746. Thus, under the “special needs” doctrine, no warrant is required by the Fourth Amendment for the NSA activities.

B. THE NSA ACTIVITIES ARE REASONABLE

As the Supreme Court has emphasized repeatedly, “[t]he touchstone of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined by assessing, on the one hand, the degree to which it intrudes upon an individual’s privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.” *Knights*, 534 U.S. at 118-19 (quotation marks omitted); *see also Earls*, 536 U.S. at 829. The Supreme Court has found a search reasonable when, under the totality of the circumstances, the importance of the governmental interests outweighs the nature and quality of the intrusion on the individual’s Fourth Amendment interests. *See Knights*, 534 U.S. at 118-22. Under the standard

²² Even in the domestic context, the Supreme Court has recognized that there may be significant distinctions between wiretapping for ordinary law enforcement purposes and domestic national security surveillance. *See United States v. United States District Court*, 407 U.S. 297, 322 (1972) (“*Keith*”) (explaining that “the focus of domestic [security] surveillance may be less precise than that directed against more conventional types of crime” because often “the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government’s preparedness for some possible future crisis or emergency”); *see also United States v. Duggan*, 743 F.2d 59, 72 (2d Cir. 1984) (reading *Keith* to recognize that “the governmental interests presented in national security investigations differ substantially from those presented in traditional criminal investigations”). Although the Court in *Keith* held that the Fourth Amendment’s warrant requirement does apply to investigations of purely *domestic* threats to national security—such as domestic terrorism, it suggested that Congress consider establishing a lower standard for such warrants than that set forth in Title III. *See id.* at 322-23 (advising that “different standards” from those applied to traditional law enforcement “may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of the Government for intelligence information and the protected rights of our citizens”). *Keith*’s emphasis on the need for flexibility applies with even greater force to surveillance directed at *foreign* threats to national security. *See* S. Rep. No. 95-701, at 16 (“Far more than in domestic security matters, foreign counterintelligence investigations are ‘long range’ and involve ‘the interrelation of various sources and types of information.’”) (quoting *Keith*, 407 U.S. at 322). And flexibility is particularly essential here, where the purpose of the NSA activities is to prevent another armed attack against the United States.

²³ This is not to say that traditional law enforcement has no role in protecting the Nation from attack. The NSA activities, however, are not directed at bringing criminals to justice but at detecting and preventing plots by a declared enemy of the United States to attack it again.

balancing of interests analysis used for gauging reasonableness, the NSA activities are consistent with the Fourth Amendment.

With respect to the individual privacy interests at stake, there can be no doubt that, as a general matter, interception of telephone communications implicates a significant privacy interest of the individual whose conversation is intercepted. The Supreme Court has made clear at least since *Katz v. United States*, 389 U.S. 347 (1967), that individuals have a substantial and constitutionally protected reasonable expectation of privacy that their telephone conversations will not be subject to governmental eavesdropping. Although the individual privacy interests at stake may be substantial, it is well recognized that a variety of governmental interests—including routine law enforcement and foreign-intelligence gathering—can overcome those interests.

On the other side of the scale here, the Government's interest in engaging in the NSA activities is the most compelling interest possible—securing the Nation from foreign attack in the midst of an armed conflict. One attack already has taken thousands of lives and placed the Nation in state of armed conflict. Defending the Nation from attack is perhaps the most important function of the federal Government—and one of the few express obligations of the federal Government enshrined in the Constitution. See U.S. Const. art. IV, § 4 (“The United States shall guarantee to every State in this Union a Republican Form of Government, *and shall protect each of them against Invasion . . .*”) (emphasis added); *The Prize Cases*, 67 U.S. (2 Black) 635, 668 (1863) (“If war be made by invasion of a foreign nation, the President is not only authorized but bound to resist force by force.”). As the Supreme Court has declared, “[i]t is ‘obvious and unarguable’ that no governmental interest is more compelling than the security of the Nation.” *Haig v. Agee*, 453 U.S. 280, 307 (1981).

The Government's overwhelming interest in detecting and thwarting further al Qaeda attacks is easily sufficient to make reasonable the intrusion into privacy involved in intercepting one-end foreign communications where there is “a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda.” Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence, *available at* <http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html> (Dec. 19, 2005) (statement of Attorney General Gonzales); *cf. Edmond*, 531 U.S. at 44 (noting that “the Fourth Amendment would almost certainly permit an appropriately tailored roadblock set up to thwart an imminent terrorist attack” because “[t]he exigencies created by th[at] scenario[] are far removed” from ordinary law enforcement). The United States has already suffered one attack that killed thousands, disrupted the Nation's financial center for days, and successfully struck at the command and control center for the Nation's military. And the President has stated that the NSA activities are “critical” to our national security. Press Conference of President Bush (Dec. 19, 2005). To this day, finding al Qaeda sleeper agents in the United States remains one of the preeminent concerns of the war on terrorism. As the President has explained, “[t]he terrorists want to strike America again, and they hope to inflict even more damage than they did on September 11th.” *Id.*

Of course, because the magnitude of the Government's interest here depends in part upon the threat posed by al Qaeda, it might be possible for the weight that interest carries in the balance to change over time. It is thus significant for the reasonableness of the NSA activities that the President has established a system under which he authorizes the surveillance only for a limited period, typically for 45 days. This process of reauthorization ensures a periodic review to evaluate whether the threat from al Qaeda remains sufficiently strong that the Government's interest in protecting the Nation and its citizens from foreign attack continues to outweigh the individual privacy interests at stake.

Finally, as part of the balancing of interests to evaluate Fourth Amendment reasonableness, it is significant that the NSA activities are limited to intercepting international communications where there is a reasonable basis to conclude that one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. This factor is relevant because the Supreme Court has indicated that in evaluating reasonableness, one should consider the "efficacy of [the] means for addressing the problem." *Vernonia*, 515 U.S. at 663; *see also Earls*, 536 U.S. at 834 ("Finally, this Court must consider the nature and immediacy of the government's concerns and the efficacy of the Policy in meeting them."). That consideration does not mean that reasonableness requires the "least intrusive" or most "narrowly tailored" means for obtaining information. To the contrary, the Supreme Court has repeatedly rejected such suggestions. *See, e.g., Earls*, 536 U.S. at 837 ("[T]his Court has repeatedly stated that reasonableness under the Fourth Amendment does not require employing the least intrusive means, because the logic of such elaborate less-restrictive-alternative arguments could raise insuperable barriers to the exercise of virtually all search-and-seizure powers.") (internal quotation marks omitted); *Vernonia*, 515 U.S. at 663 ("We have repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment."). Nevertheless, the Court has indicated that some consideration of the efficacy of the search being implemented—that is, some measure of fit between the search and the desired objective—is relevant to the reasonableness analysis. The NSA activities are targeted to intercept international communications of persons reasonably believed to be members or agents of al Qaeda or an affiliated terrorist organization, a limitation which further strongly supports the reasonableness of the searches.

In sum, the NSA activities are consistent with the Fourth Amendment because the warrant requirement does not apply in these circumstances, which involve both "special needs" beyond the need for ordinary law enforcement and the inherent authority of the President to conduct warrantless electronic surveillance to obtain foreign intelligence to protect our Nation from foreign armed attack. The touchstone of the Fourth Amendment is reasonableness, and the NSA activities are certainly reasonable, particularly taking into account the nature of the threat the Nation faces.

CONCLUSION

For the foregoing reasons, the President—in light of the broad authority to use military force in response to the attacks of September 11th and to prevent further catastrophic attack expressly conferred on the President by the Constitution and confirmed and supplemented by

Congress in the AUMF—has legal authority to authorize the NSA to conduct the signals intelligence activities he has described. Those activities are authorized by the Constitution and by statute, and they violate neither FISA nor the Fourth Amendment.

Subject: 1/23 Remarks on War on Terror #2 -- for Dan, Nicolle and Brett's review
From: "Drouin, Lindsey E."
Date: 1/19/06, 9:52 PM
To: "Violette, Aimee E.", "Burdick, Amanda K.", "Kavanaugh, Brett M."
CC: "Michel, Christopher G.", "Thiessen, Marc A.", "Drouin, Lindsey E.", "Carson, Melissa M.", "Fahy, Brian D.", "Merkley, Brendon A.", "Ward, Frank P."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Tue Apr 02 15:14:53 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5,P6,b(6)

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: FW: AP – Bush to visit intelligence agency that runs domestic spying program
From: "Kaplan, Joel"
Date: 1/20/06, 10:51 AM
To: "Kavanaugh, Brett M."

[Sweet.](#)

From: White House News Update [mailto:News.Update@WhiteHouse.Gov]
Sent: Friday, January 20, 2006 10:28 AM
To: Kaplan, Joel
Subject: AP - Bush to visit intelligence agency that runs domestic spying program

Bush to visit intelligence agency that runs domestic spying program

WASHINGTON (AP) The Bush administration is opening a campaign to push back against criticism of its domestic spying program, ahead of congressional hearings into whether President Bush has the legal authority to eavesdrop on Americans.

President Bush will visit the ultra-secret National Security Agency on Wednesday, underscoring his claim that he has the constitutional authority to let intelligence officials listen in on international phone calls of Americans with suspected ties to terrorists.

On Monday, Mike Hayden, deputy national intelligence director who headed the National Security Agency when the program began in October 2001, will speak on the issue at the National Press Club.

On Tuesday, Attorney General Alberto Gonzales is delivering a speech on the program in Washington.

You are currently subscribed to News Update (wires) as: Joel_D._Kaplan@omb.eop.gov.
To unsubscribe send a blank email to leave-whitehouse-news-wires-1000279K@list.whitehouse.gov

Subject: post-staffing remarks for Monday (war on terror)
From: "Drouin, Lindsey E."
Date: 1/20/06, 9:18 PM
To: "Kavanaugh, Brett M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Tue Apr 02 16:38:48 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5,P6,b(6)

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: Fw: 1/23 Remarks on War on Terror #6 -- for the President's review
From: "Kavanaugh, Brett M."
Date: 1/21/06, 3:27 AM
To: "Sherzer, David", "Slaughter, Kristen K."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Tue Apr 02 16:38:49 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5,P6,b(6)

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

From: "Deckard, Josh"
To: "Scott McClellan"

P6/b6

Subject: RE: Enzo

Received(Date): Mon, 5 Mar 2007 09:44:25 -0500

ouch! I was thinking, more like McClellan:

""During the visit, I'm the face of the administration," Ensenat said."

From: Scott McClellan [redacted] P6/b6

Sent: Monday, March 05, 2007 9:41 AM

[redacted] P6/b6

Subject: RE: ENZO

Kind of like Deckard:

In most of the official White House and State Department diplomatic pictures, Ensenat is off to the side or in the background. He was always on the edge of the limelight, but rarely in it.

From: Deckard, Josh [mailto:Josh_Deckard@who.eop.gov]

Sent: Monday, March 05, 2007 6:40 AM

[redacted] P6/b6

Subject: Enzo

-----Original Message-----

From: Weinstein, Jared B.

To: Recher, Jason; Hagin, Joseph W; Meyers, John M.; Beyer, Todd W.; Bennett, Melissa S.; Keller, Karen E.; Haines, Mary A.; Newton, Julia K.; Sherzer, David; Deckard, Josh; Draper, Eric; Morse, Paul L; Perino, Dana M.; Carroll, Carlton F.; Edwards, Chris

Sent: Mon Mar 05 06:01:53 2007

Subject: times-picayune: bush's chief of protocol bows out

<<@StoryAd?x>>

Bush's chief of protocol bows out

New Orleanian held key White House job
Friday, March 02, 2007
By Bill Walsh
Washington bureau

WASHINGTON -- Donald Ensenat, who recently left the job as U.S. chief of protocol, likes to tell people that the position dates to ancient Greece.

http://ads.nola.com/RealMedia/ads/click_nx.ads/www.nola.com/xml/story/N/NSDC/@StoryAd?x

The term "proto" meant first and "collon" meant glued, a reference to the written summaries Greek diplomats attached to the outside of their dispatches. In six years in the job, Ensenat gave the old term a new twist: More than any other protocol chief in memory, Ensenat was glued to the president's side.

"I think he was very respected in the diplomatic community because they knew how close he and the president were," said Tom Kuhn, a Yale University classmate and president of the leading electric company trade group, the Edison Electric Institute. "It enabled him to be very effective."

Bush has shown he highly prizes friendship and loyalty, and Ensenat, 60, a New Orleans native, rates high marks in each. The two met at Yale where they were fraternity brothers and lived together in a Texas apartment afterward. Bush's father appointed him as ambassador to the Kingdom of Brunei. Ensenat and the younger Bush have been friends for more than four decades.

When he left the job Feb. 16, "Enzo," as the president calls him, was the second-longest serving protocol chief behind Selwa "Lucky" Roosevelt, who held the position during President Reagan's two terms.

"Washington being what it is, I think I would hire a close friend in a job like that, too," said John Weinmann, a fellow New Orleanian who was chief of protocol in the first Bush administration.

Post is misunderstood

Ensenat, who held the rank of ambassador, said the post is widely misunderstood. He said it bears little resemblance to the 1984 comedy "Protocol," starring Goldie Hawn, who plays a comely blond waitress co-opted by the State Department in a scheme to persuade a Middle Eastern emir to allow a U.S. military base in his country.

In most of the official White House and State Department diplomatic pictures, Ensenat is off to the side or in the background. He was always on the edge of the limelight, but rarely in it.

Ensenat said that two-thirds of the job involved arranging the nuts and bolts of visits by foreign dignitaries from the moment their planes touch down through a meet-and-greet with Bush to the farewell handshake on the tarmac.

"During the visit, I'm the face of the administration," Ensenat said.

When Ensenat, a New Orleans lawyer, accepted the job, he had every reason to believe it would be relatively light duty. It was no secret that candidate Bush didn't travel much outside the United States and also wasn't much for formal entertaining.

Not long after Bush took office in 2001, the two found themselves standing next to each other awaiting the first meeting with Russian President Vladimir Putin in Slovenia. With the international press corps poised to record every moment, Bush leaned over to his former frat brother and whispered, "Enzo, this is a long way from DKE House, isn't it?"

9/11 changed all

No one could have predicted what an understatement that would be. Later that year, terrorists attacked the United States and threw diplomatic relations into overdrive. The ensuing five years would see a surge in diplomatic visits to the White House. Ensenat counted 2,172 in all, a record pace.

"9/11 changed everything," he said. "Terrorism jumped to the head of the agenda. There were increased visits. Security ramped up tremendously. The motorcades were bigger and the logistics were bigger."

Logistics are the core of the protocol chief's job. Besides shepherding foreign dignitaries through the White House, Ensenat was responsible for overseeing the details of Bush's foreign trips, a total of 30 to 80 countries, each with a three-month planning lead time.

Ensenat said he was part of the "traveling squad" of advisers that stuck close to the president. Among other things, it fell to Ensenat and his 60-person staff to make sure that everyone got introduced by the correct title and the right order according to their diplomatic rank.

"Everyone has a pecking order," he said. "It's useful in making sure no one gets their nose out of joint and there is no diversion from the business at hand."

By 2003, the outpouring of international empathy the United States enjoyed after 9/11 had morphed into angry protests across the globe against the imminent invasion of Iraq. Ensenat said he saw little change on the diplomatic front.

Even from the French, who led the opposition to the war?

"The French are a special case," Ensenat said diplomatically.

Odd gifts to president

Ensenat's diplomacy seems to be a character trait. Asked about the strangest gift Bush received from a foreign dignitary, Ensenat described a seashell portrait of the president, but declined to identify the gift giver. He also demurred in saying who gave Bush a rare breed of dog, a breach of international protocol that you don't give animals to heads of state. The dog was holed up at the National Security Agency for two days before being adopted.

Ultimately, after six years the demands of protocol wore thin. Ensenat said he was leaving because of the "great sacrifice" it has put on him and his family. His wife, Taylor, divided time between Washington and New Orleans, but the time apart took a toll. He used to tell people that he would be lucky if by the end of his term he wasn't divorced or broke.

As it turned out, he is neither. Back in New Orleans, he has gone into business with fellow Bush loyalist Joe Canizaro, a developer, banker and venture capitalist. Ensenat said he may open up a Washington lobbying office, too.

He also hopes to keep up with his old friend the president. It shouldn't be hard. The two are neighbors. Four years ago, Ensenat and Canizaro bought a 600-acre ranch about five miles from Crawford, Texas, where Bush makes his home.

.....

Subject: FW: Legislative Correspondence Report
From: "Kavanaugh, Brett M."
Date: 1/22/06, 7:43 PM
To: "Lee, Sujean S."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Tue Apr 02 16:38:49 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: Re: [Fwd: FW: DETAILED LEGAL ANALYSIS OF THE NSA ACTIVITIES DESCRIBED BY THE PRESIDENT]

From: [50 USC 3024 (m)(1)]

Date: 1/22/06, 9:35 PM

To: "McDonald, Matthew T.", "Miers, Harriet", "Kavanaugh, Brett M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Tue Apr 02 16:38:51 EDT 2019

Releasability: Withheld In Part

Reasons for Withholding:

b(3),P3

Notes:

50 USC 3024 (m)(1)

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: STRS Final
From: "McDonald, Matthew T."
Date: 1/22/06, 9:40 PM
To: "Miers, Harriet", "Gerry, Brett C.", [50 USC 3024 (m)(1)], "Kavanaugh, Brett M.", "Wallace, Nicole", "Bartlett, Dan", "McClellan, Scott"
CC: "Perino, Dana M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Tue Apr 02 16:38:51 EDT 2019

Releasability: Withheld In Part

Reasons for Withholding:

b(3),P3

Notes:

50 USC 3024 (m)(1)

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: [Fwd: FW: DETAILED LEGAL ANALYSIS OF THE NSA ACTIVITIES DESCRIBED BY THE PRESIDENT]

From: "McDonald, Matthew T."

Date: 1/22/06, 9:42 PM

To: [50 USC 3024 (m)(1)], "Miers, Harriet", "Kavanaugh, Brett M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Tue Apr 02 16:38:52 EDT 2019

Releasability: Withheld In Part

Reasons for Withholding:

b(3),P3

Notes:

50 USC 3024 (m)(1)

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: STRS Final
From: "Miers, Harriet"
Date: 1/22/06, 9:45 PM
To: "McDonald, Matthew T.", "Gerry, Brett C.", [50 USC 3024 (m)(1)], "Kavanaugh, Brett M.", "Wallace, Nicolle", "Bartlett, Dan", "McClellan, Scott"
CC: "Perino, Dana M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Tue Apr 02 16:38:53 EDT 2019

Releasability: Withheld In Part

Reasons for Withholding:

b(3),P3

Notes:

50 USC 3024 (m)(1)

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: Re: STRS Final
From: "McClellan, Scott"
Date: 1/22/06, 9:45 PM
To: "McDonald, Matthew T.", "Miers, Harriet", "Gerry, Brett C.", [50 USC 3024 (m)(1)], "Kavanaugh, Brett M.", "Wallace, Nicolle", "Bartlett, Dan"
CC: "Perino, Dana M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Tue Apr 02 16:38:53 EDT 2019

Releasability: Withheld In Part

Reasons for Withholding:

b(3),P3

Notes:

50 USC 3024 (m)(1)

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: Re: STRS Final
From: "Kavanaugh, Brett M."
Date: 1/22/06, 9:49 PM
To: "McDonald, Matthew T."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Tue Apr 02 16:38:54 EDT 2019

Releasability: Withheld In Part

Reasons for Withholding:

b(3),P3

Notes:

50 USC 3024 (m)(1)

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: STRS Final
From: "McDonald, Matthew T."
Date: 1/22/06, 9:49 PM
To: "Kavanaugh, Brett M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Tue Apr 02 16:38:55 EDT 2019

Releasability: Withheld In Part

Reasons for Withholding:

b(3),P3

Notes:

50 USC 3024 (m)(1)

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: Re: STRS Final
From: [50 USC 3024 (m)(1)]
Date: 1/22/06, 9:51 PM
To: "McDonald, Matthew T."
CC: "Miers, Harriet", "Gerry, Brett C.", "Kavanaugh, Brett M.", "Wallace, Nicolle", "Bartlett, Dan", "McClellan, Scott", "Perino, Dana M.", "Allen, Michael"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Tue Apr 02 16:38:56 EDT 2019

Releasability: Withheld In Part

Reasons for Withholding:

b(3),P3

Notes:

50 USC 3024 (m)(1)

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: STRS Final
From: "Miers, Harriet"
Date: 1/22/06, 9:55 PM
To: [50 USC 3024 (m)(1)], "McDonald, Matthew T."
CC: "Gerry, Brett C.", "Kavanaugh, Brett M.", "Wallace, Nicolle", "Bartlett, Dan", "McClellan, Scott", "Perino, Dana M.", "Allen, Michael"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Tue Apr 02 16:38:58 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5,b(3),P3

Notes:

50 USC 3024 (m)(1)

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: STRS Final
From: "McDonald, Matthew T."
Date: 1/22/06, 9:56 PM
To: "Miers, Harriet", [50 USC 3024 (m)(1)]
CC: "Gerry, Brett C.", "Kavanaugh, Brett M.", "Wallace, Nicolle", "Bartlett, Dan", "McClellan, Scott", "Perino, Dana M.", "Allen, Michael"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Tue Apr 02 16:38:59 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5,b(3),P3

Notes:

50 USC 3024 (m)(1)

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: Re: STRS Final
From: "McClellan, Scott"
Date: 1/22/06, 9:57 PM
To: [50 USC 3024 (m)(1)], "McDonald, Matthew T."
CC: "Miers, Harriet", "Gerry, Brett C.", "Kavanaugh, Brett M.", "Wallace, Nicolle", "Bartlett, Dan", "Perino, Dana M.", "Allen, Michael"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Tue Apr 02 16:39:00 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5,b(3),P3

Notes:

50 USC 3024 (m)(1)

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: Re: STRS Final
From: "Bartlett, Dan"
Date: 1/22/06, 9:58 PM
To: "McDonald, Matthew T.", "Miers, Harriet", [b3 50 USC 3024 (m)(1)]
CC: "Gerry, Brett C.", "Kavanaugh, Brett M.", "Wallace, Nicolle", "McClellan, Scott", "Perino, Dana M.", "Allen, Michael"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Wed Apr 03 15:40:09 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

b(3),P3,P5

Notes:

50 USC 3024 (m)(1)

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: [Fwd: Re: [Fwd: FW: DETAILED LEGAL ANALYSIS OF THE NSA ACTIVITIES DESCRIBED BY THE PRESIDENT]]

From: [b3 50 USC 3024 (m)(1)]

Date: 1/22/06, 9:59 PM

To: "Kavanaugh, Brett M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Wed Apr 03 15:40:10 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

b(3),P3,P5

Notes:

50 USC 3024 (m)(1)

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: STRS Final
From: "McDonald, Matthew T."
Date: 1/22/06, 10:00 PM
To: "McClellan, Scott", [b3 50 USC 3024 (m)(1)]
CC: "Miers, Harriet", "Gerry, Brett C.", "Kavanaugh, Brett M.", "Wallace, Nicolle", "Bartlett, Dan", "Perino, Dana M.", "Allen, Michael"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Wed Apr 03 15:40:11 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

b(3),P3,P5

Notes:

50 USC 3024 (m)(1)

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: Re: STRS Final
From: "Gerry, Brett C."
Date: 1/22/06, 10:07 PM
To: "Miers, Harriet", [b3 50 USC 3024 (m)(1)], "McDonald, Matthew T."
CC: "Kavanaugh, Brett M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Wed Apr 03 15:40:12 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

b(3),P3,P5

Notes:

50 USC 3024 (m)(1)

Case ID: gwb.2018-0258-F.3

Additional Information:

From: "Kavanaugh, Brett M."
To: "Haenle, Paul T."
Subject: final tp's for today
Received(Date): Mon, 23 Jan 2006 07:50:21 -0500
[KansasState23January2006#7.doc](#)

Talking Points on the Global War on Terror – Manhattan, Kansas
Monday, January 23, 2006
Draft #7

Kansas State University

- I am glad to be at K-State. Instead of Hail to the Chief, I was hoping I might get to hear “Wabash Cannonball.”¹
- I appreciate a school that takes its sports seriously. Your basketball team looked pretty good against the Jayhawks the other day.² My only request is that you take it easy when the Longhorns come to town.³
- I thank all the K-State students who came out today. It must have been tough to get you to skip class ... and it’s probably too early to head over to The Last Chance.⁴

Acknowledgments

- Mrs. Laura Bush (not present)
- Senator Pat Roberts (R-KS) (introduced you)
- Governor Kathleen Sebelius (D-KS)
- Senator Sam Brownback (R-KS)
- Congressman Jim Ryun (R-KS) (his district)
- Congressman Jerry Moran (R-KS)
- Congressman Dennis Moore (D-KS)
- Jon Wefald [WEE-fall], President, Kansas State University (event host)
- Dr. Charles Reagan, Chairman, Landon Lecture Series
- Edward Seaton, Chairman, Landon Lecture Series Patrons, and Editor-in-Chief and Publisher, *The Manhattan Mercury*
- Tom Herald, Faculty Senate President, Kansas State University
- Michael Burns, Student Body President, Kansas State University
- General Dick Myers, Former Chairman of the Joint Chiefs of Staff, and Foundation Professor of Military History and Leadership, Kansas State University
- General Jim Warner, Deputy Commandant of the U.S. Army Command and General Staff College, Fort Leavenworth
- Major General Dennis Hardy, Commanding General, 24th Infantry Division and Fort Riley

¹ The Kansas State fight song

² On January 14, Kansas State basketball beat archrival Kansas for the first time since 1994.

³ Kansas State hosts Texas on February 22.

⁴ The most popular bar on campus.

- Brigadier General Dana Pittard, Assistant Division Commander, 24th Infantry Division and Fort Riley
- All the members of the armed forces with us today, and especially to those recently returned from Iraq or Afghanistan

Landon Lecture Series

- Alf Landon was a soldier, an entrepreneur, a governor, a presidential candidate, and always a patriot. His integrity, decency, and conviction are a model for all who serve in public office.
- I hope you don't mind if I modify the format today. I was not a big fan of lectures back in college – I can't promise I went to every one I was supposed to ... I can't promise I stayed awake through every one I attended.
- Instead of a lecture, I want to share some thoughts on the job of the President, and what we are doing to build a safer country and a more peaceful world. Then I want to answer some questions.

Responsibilities ... Wartime Presidency

- Job of a President is to make decisions.
- Most solemn responsibility is to protect the American people.
- America is at war – came to our shores on September 11, 2001
 - Recent tapes are evidence that enemy is still active and plotting.

After September 11, we reshaped American foreign policy based on certain principles

- Nature of the enemy – followers of a radical ideology that exploits Islam to serve a violent, political vision: the establishment of a totalitarian empire that denies all freedom and extends from Spain to Indonesia
 - Use the tactics of terror in an attempt to spread this ideology – cannot be appeased ... must be confronted and defeated
- First: We are on the offense with every element of national power:
 - Military – take fight to the enemy
 - Intelligence – find out where enemy lurks, share information
 - Law enforcement – find enemies within our borders, prevent attacks
 - Diplomatic – leading powerful war on terror coalition
 - Financial – freezing terrorist assets and choking off support
- Second: Harbor a terrorist, equally as guilty as the terrorists
 - Afghanistan under the Taliban

- Third: Confront threats before they fully materialize
 - Saddam Hussein's Iraq
 - Sworn enemy of the United States ... firing at American military pilots ... open defiance of UN resolutions ... state sponsor of terror ... had pursued and used weapons of mass destruction
 - Tried to address diplomatically – went to the United Nations Security Council ... passed unanimous resolution to disclose and disarm ... gave Saddam a final ultimatum
 - Saddam defied the will of the world – now in prison and on trial ... America and the world are better off.
- Fourth: Change the conditions that give rise to tyranny and terror
 - Terrorists' vision – no free speech or women's rights or religious tolerance
 - Defeat the ideology with vision of freedom. Free nations are peaceful nations – spreading freedom in broader Middle East:
 - Afghanistan and Iraq have freely-elected governments
 - Elections in Lebanon and the Palestinian Territories

Central front in the war on terror is Iraq

- Words of bin Laden: “Third World War is raging” in Iraq ... will end in “victory and glory or misery and humiliation.”
- Our goal in Iraq is victory – achieved when:
 - Terrorists and Saddamists can no longer threaten Iraq's democracy
 - Iraqi Security Forces can provide for the safety of their own citizens
 - Iraq is not a safe haven for terrorists to plot attacks on America
- The enemy we face in Iraq: rejectionists, Saddamists, terrorists
- 3-part strategy for victory: political, security, economic ... adjust tactics
- Troop levels – As Iraqis stand up, we will stand down.
 - Reducing from 17 to 15 brigades by this spring
 - Bringing home 20,000 troops who were in Iraq largely to assist with security during December elections
 - Decisions based on conditions on the ground and advice of military leaders – not artificial timetables set by politicians
- Cannot lose on the battlefield – only lose if we lose our will. Will not happen on my watch.
- Democratic Iraq will lead to peace ... Japan after World War II, Koizumi

Also fighting the war here at home

- Created Department of Homeland Security
- Changed mission of the FBI to preventing terrorist attacks
- Created Director of National Intelligence and National Counterterrorism Center to better integrate intelligence and prevent attacks
- Trained 800,000 state and local first responders
- Strengthened security at airports, seaports, bridges, tunnels, other
- Improved security of food supply – thank scientists at K-State who dedicate their work to protecting our food supply from terrorist attack

Patriot Act

- Congress passed the Patriot Act with huge bipartisan majorities
- Allows law enforcement and intelligence to share more information
- Allows law enforcement officers to pursue terrorists with tools they already use against other criminals
- Includes safeguards to protect civil liberties
- Law enforcement has used Patriot Act to:
 - Break up terror cells in New York, Oregon, Virginia, and Florida
 - Prosecute terrorist operatives and supporters in California, Texas, New Jersey, Illinois, North Carolina, and Ohio
- Certain provisions scheduled to expire at the end of 2005.
- Majority in Senate and House support renewal – including Senators Roberts and Brownback.
- A minority of Senators blocked permanent renewal – Democratic Leader in Senate bragged that they had “killed the Patriot Act.”
- Congress agreed to temporarily extend the Patriot Act until February 3 – next Friday. If Congress does not act by then, our law enforcement officers will be without this vital law.
- We need this vital weapon to protect Americans – and we cannot afford to be without it for a single moment. The minority of Senators who are blocking the law should stop playing politics with national security. The Senate needs to renew the Patriot Act.

National Security Agency Program – Enemy Surveillance

- After September 11, I authorized the National Security Agency to intercept certain international terrorist communications.
- Lots of discussion, here are the facts:
 - Applies only to communications in which one person is reasonably suspected of links to al Qaida or related terrorist organizations.

- Applies only to international communications – one end of the communications must be outside the United States
- Includes strict review measures to protect civil liberties.
- Leaders in Congress have been briefed on the program more than a dozen times.
- General Hayden, America’s second-ranking intelligence official: Program has helped connect the dots – detect and prevent attacks in United States. Program has saved American lives.
- Some say NSA program is unlawful. Why they are wrong:
 - First, federal courts have consistently ruled that a President has authority under the Constitution to conduct foreign intelligence surveillance against our enemies.
 - Second, my predecessors as President have consistently cited and, as necessary used, the same constitutional authority I am using to conduct foreign intelligence surveillance against our enemies.
 - Third, the Supreme Court has ruled that the Authorization for the Use of Military Force passed by Congress in 2001 gave the President additional authority to use what it called the “fundamental incidents of waging war” against al-Qaida. Here is what that means in real English: Congress resolved that the President has the authority and responsibility to use all the traditional tools of war in the fight against terror – and that includes electronic surveillance against our enemies.
- The law is clear: I have the authority, both from the Constitution and from Congress, to undertake this vital program.
- Some may think, as a matter of policy, that it is a mistake for me to use that legal authority to listen to al Qaida terrorists when they contact people in the United States. That is a pre-September 11 mentality, and I strongly disagree.
- The American people expect me to protect them and their civil liberties – and that is precisely what we are doing. So I will continue to reauthorize this program for as long as our country faces a continuing threat from al-Qaida and related groups.

Conclusion

- Grateful that America has now gone four years and five months without a terrorist attack on our soil. Not for a lack of desire on the part of the terrorists – because of the courage of our military, law enforcement,

intelligence, and homeland security professionals. And because we have given them the tools and resources they need to protect us.

- Cannot let the fact that we have not been attacked lull us into illusion that threats have disappeared. They have not. Enemy is still active –London, Madrid, Bali, Beslan, and other places. Terrorists will do everything they can to strike us – and we must continue to do everything we can to stop them.
- The last sitting president to deliver a Landon Lecture was Ronald Reagan, in 1982. He spoke of what he called “awesome problems” facing America at the time – economic crisis, international tension, and the danger of nuclear war. Also spoke with confidence in our future: “We can and will prevail if we have the faith and the courage to believe in ourselves and in our ability to perform great deeds as we have throughout our history.”
- History has proven his confidence to be justified. Within a decade of President Reagan’s Landon Lecture, the Soviet Union was no more. And last October, the former leader of the Soviet Union came to Manhattan for a Landon Lecture of his own.
- In every age, the power of freedom has overcome challenges, because the will to live in freedom is a part of every soul. With the strength and idealism and resolve of the American people, I have no doubt that freedom will prevail in our age as well.
- Thank you for your warm welcome – happy to take some questions.

Drafted by: Chris Michel and Marc Thiessen, Office of Speechwriting

Office: 202/456-5860 and 202/456-2170

Cell:

P6/b6

talking points for K State (not sure how much he will follow these)

Subject: talking points for K State (not sure how much he will follow these)

From: "Kavanaugh, Brett M."

Date: 1/23/06, 12:13 PM

To: "McClellan, Scott", "Hervey, Tina"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Wed Apr 03 15:40:12 EDT 2019

Releasability: Withheld In Part

Reasons for Withholding:

b(6),P6

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: FW: 1/25 Statement at National Security Agency #2 – to be staffed out
From: "Burck, Bill"
Date: 1/23/06, 12:18 PM
To: "Kavanaugh, Brett M."

[Do you want this also staffed to AG, Defense, others?](#)

From: Drouin, Lindsey E.
Sent: Monday, January 23, 2006 12:11 PM
To: Houser, Molly M.; Staff Secretary
Subject: RE: 1/25 Statement at National Security Agency #2 - to be staffed out

[Thanks.](#)

From: Houser, Molly M.
Sent: Monday, January 23, 2006 12:11 PM
To: Staff Secretary
Cc: Drouin, Lindsey E.
Subject: FW: 1/25 Statement at National Security Agency #2 - to be staffed out

[I'll staff this.](#)

From: Drouin, Lindsey E.
Sent: Monday, January 23, 2006 12:01 PM
To: Staff Secretary
Cc: Michel, Christopher G.; Thiessen, Marc A.; Burdick, Amanda K.; Carson, Melissa M.; Drouin, Lindsey E.; Fahy, Brian D.; Gerson, Michael J.; Green, Anneke E.; Hughes, Taylor A.; Jordan, Elise; Klunk, Kate A.; Kropp, Emily L.; Martin, Catherine; McConnell, John P.; McGurn, William J.; Merkley, Brendon A.; Patel, Neil S.; Ralston, Susan B.; Violette, Aimee E.; Ward, Frank P.
Subject: 1/25 Statement at National Security Agency #2 - to be staffed out

Comments due back tomorrow at noon. Thanks!

Subject: Re: 1/25 Statement at National Security Agency #2 – to be staffed out
From: "Kavanaugh, Brett M."
Date: 1/23/06, 12:26 PM
To: "Burck, Bill"

I told lindsey to tell sherzer to send to hayden. We also should send to kyle sampson (for the ag) and steve bradbury at doj.

-----Original Message-----

From: Burck, Bill <William_A._Burck@who.eop.gov>
To: Kavanaugh, Brett M. <Brett_M._Kavanaugh@who.eop.gov>
Sent: Mon Jan 23 12:18:46 2006
Subject: FW: 1/25 Statement at National Security Agency #2 – to be staffed out

Do you want this also staffed to AG, Defense, others?

From: Drouin, Lindsey E.
Sent: Monday, January 23, 2006 12:11 PM
To: Houser, Molly M.; Staff Secretary
Subject: RE: 1/25 Statement at National Security Agency #2 – to be staffed out

Thanks.

From: Houser, Molly M.
Sent: Monday, January 23, 2006 12:11 PM
To: Staff Secretary
Cc: Drouin, Lindsey E.
Subject: FW: 1/25 Statement at National Security Agency #2 – to be staffed out

I'll staff this.

From: Drouin, Lindsey E.
Sent: Monday, January 23, 2006 12:01 PM
To: Staff Secretary
Cc: Michel, Christopher G.; Thiessen, Marc A.; Burdick, Amanda K.; Carson, Melissa M.; Drouin, Lindsey E.; Fahy, Brian D.; Gerson, Michael J.; Green, Anneke E.; Hughes, Taylor A.; Jordan, Elise; Klunk, Kate A.; Kropp, Emily L.; Martin, Catherine; McConnell, John P.; McGurn, William J.; Merkle, Brendon A.; Patel, Neil S.; Ralston, Susan B.; Violette, Aimee E.; Ward, Frank P.

Subject: 1/25 Statement at National Security Agency #2 – to be staffed out

Re: 1/25 Statement at National Security Agency #2 - to be staffed out

Comments due back tomorrow at noon. Thanks!

Subject: RE: 1/25 Statement at National Security Agency #2 - to be staffed out
From: "Burck, Bill"
Date: 1/23/06, 12:27 PM
To: "Kavanaugh, Brett M."

Will do

-----Original Message-----

From: Kavanaugh, Brett M.
Sent: Monday, January 23, 2006 12:26 PM
To: Burck, Bill
Subject: Re: 1/25 Statement at National Security Agency #2 - to be staffed out

I told lindsey to tell sherzer to send to hayden. We also should send to kyle sampson (for the ag) and steve bradbury at doj.

-----Original Message-----

From: Burck, Bill <William_A._Burck@who.eop.gov>
To: Kavanaugh, Brett M. <Brett_M._Kavanaugh@who.eop.gov>
Sent: Mon Jan 23 12:18:46 2006
Subject: FW: 1/25 Statement at National Security Agency #2 - to be staffed out

Do you want this also staffed to AG, Defense, others?

From: Drouin, Lindsey E.
Sent: Monday, January 23, 2006 12:11 PM
To: Houser, Molly M.; Staff Secretary
Subject: RE: 1/25 Statement at National Security Agency #2 - to be staffed out

Thanks.

From: Houser, Molly M.
Sent: Monday, January 23, 2006 12:11 PM
To: Staff Secretary
Cc: Drouin, Lindsey E.
Subject: FW: 1/25 Statement at National Security Agency #2 - to be staffed out

I'll staff this.

From: Drouin, Lindsey E.
Sent: Monday, January 23, 2006 12:01 PM
To: Staff Secretary

RE: 1/25 Statement at National Security Agency #2 - to be staffed out

Cc: Michel, Christopher G.; Thiessen, Marc A.; Burdick, Amanda K.; Carson, Melissa M.; Drouin, Lindsey E.; Fahy, Brian D.; Gerson, Michael J.; Green, Anneke E.; Hughes, Taylor A.; Jordan, Elise; Klunk, Kate A.; Kropp, Emily L.; Martin, Catherine; McConnell, John P.; McGurn, William J.; Merkley, Brendon A.; Patel, Neil S.; Ralston, Susan B.; Violette, Aimee E.; Ward, Frank P.

Subject: 1/25 Statement at National Security Agency #2 – to be staffed out

Comments due back tomorrow at noon. Thanks!

Subject: Re: 1/25 Statement at National Security Agency #2 - to be staffed out
From: "Kavanaugh, Brett M."
Date: 1/23/06, 12:29 PM
To: "Burck, Bill"

Gerry should have their email addresses.

-----Original Message-----

From: Burck, Bill <William_A_Burck@who.eop.gov>
To: Kavanaugh, Brett M. <Brett_M_Kavanaugh@who.eop.gov>
Sent: Mon Jan 23 12:27:44 2006
Subject: RE: 1/25 Statement at National Security Agency #2 - to be staffed out

Will do

-----Original Message-----

From: Kavanaugh, Brett M.
Sent: Monday, January 23, 2006 12:26 PM
To: Burck, Bill
Subject: Re: 1/25 Statement at National Security Agency #2 - to be staffed out

I told lindsey to tell sherzer to send to hayden. We also should send to kyle sampson (for the ag) and steve bradbury at doj.

-----Original Message-----

From: Burck, Bill <William_A_Burck@who.eop.gov>
To: Kavanaugh, Brett M. <Brett_M_Kavanaugh@who.eop.gov>
Sent: Mon Jan 23 12:18:46 2006
Subject: FW: 1/25 Statement at National Security Agency #2 - to be staffed out

Do you want this also staffed to AG, Defense, others?

From: Drouin, Lindsey E.
Sent: Monday, January 23, 2006 12:11 PM
To: Houser, Molly M.; Staff Secretary
Subject: RE: 1/25 Statement at National Security Agency #2 - to be staffed out

Thanks.

From: Houser, Molly M.
Sent: Monday, January 23, 2006 12:11 PM
To: Staff Secretary
Cc: Drouin, Lindsey E.
Subject: FW: 1/25 Statement at National Security Agency #2 - to be staffed out

Re: 1/25 Statement at National Security Agency #2 - to be staffed out

I'll staff this.

From: Drouin, Lindsey E.

Sent: Monday, January 23, 2006 12:01 PM

To: Staff Secretary

Cc: Michel, Christopher G.; Thiessen, Marc A.; Burdick, Amanda K.; Carson, Melissa M.; Drouin, Lindsey E.; Fahy, Brian D.; Gerson, Michael J.; Green, Anneke E.; Hughes, Taylor A.; Jordan, Elise; Klunk, Kate A.; Kropp, Emily L.; Martin, Catherine; McConnell, John P.; McGurn, William J.; Merkley, Brendon A.; Patel, Neil S.; Ralston, Susan B.; Violette, Aimee E.; Ward, Frank P.

Subject: 1/25 Statement at National Security Agency #2 - to be staffed out

Comments due back tomorrow at noon. Thanks!

Subject: final tp's for today
From: "Kavanaugh, Brett M."
Date: 1/23/06, 12:50 PM
To: "Haenle, Paul T."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Wed Apr 03 15:40:14 EDT 2019

Releasability: Withheld In Part

Reasons for Withholding:

b(6),P6

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: 1/25 Statement after NSA Visit #2 -- for Dan, Nicolle and Brett's review

From: "Drouin, Lindsey E."

Date: 1/23/06, 4:24 PM

To: "Burdick, Amanda K.", "Violette, Aimee E.", "Kavanaugh, Brett M."

CC: "Michel, Christopher G.", "Thiessen, Marc A.", "Carson, Melissa M.", "Fahy, Brian D.", "Merkley, Brendon A.", "Ward, Frank P."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Wed Apr 03 15:40:15 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

b(6),P5,P6

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: FW: Draft Presidential remarks for your review.
From: "Sherzer, David"
Date: 1/23/06, 9:29 PM
To: "Kavanaugh, Brett M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Wed Apr 03 15:40:16 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

b(6),P5,P6

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

From: "Carson, Melissa M."
To: [REDACTED] b3 50 USC 3024 (m)(1)
Cc: "Ward, Frank P."; "Merkley, Brendon A."; "Kavanaugh, Brett M."
Subject: RE: POTUS Remarks -- DNI
Received(Date): Tue, 24 Jan 2006 12:50:12 -0500

Thanks for the confirmation, Ben.

From: [REDACTED] b3 50 USC 3024 (m)(1)
Sent: Tuesday, January 24, 2006 12:41 PM
To: Carson, Melissa M.
Cc: Ward, Frank P.; Merkley, Brendon A.; Kavanaugh, Brett M.
Subject: Re: POTUS Remarks -- DNI

I have verified with General's assistant that it is accurate to state:

"Signals intelligence is vital to these efforts. Information gathered by the NSA has helped our courageous men and women serving in Afghanistan, Iraq and other fronts in the war on terror capture or kill dangerous terrorists."

that said, please ensure that speeches continue to go through the standard clearance process -- I don't want to create any confusion, however slight, about the process that has been worked out to clear national security statements and who is responsible for ultimately signing off on statements. I know that there is a very specific process in place.

Carson, Melissa M. wrote:

Ben,

Here is the paragraph for context. Staff Secretary would like you to verify the accuracy of the highlighted sentences.

Thanks,

Melissa

The National Security Agency is playing a critical role in the war on terror. We face determined enemies, who lurk in shadows and attack without warning. To secure our homeland, we must be able to learn the intentions of these enemies before they strike. Signals intelligence is vital to these efforts. Information gathered by the NSA has helped our courageous men and women serving in Afghanistan, Iraq and other fronts in the war on terror capture or kill dangerous terrorists. And it has also helped our law enforcement officials here at home stop attacks against the American people.

From: <Steve.Bradbury@usdoj.gov>
To: "Miers, Harriet", "Kavanaugh, Brett M.", <benjaap@dni.gov>, "Gerry, Brett C.", "Allen, Michael"
Cc: [REDACTED]

Subject: DOJ letters to nra

b3 50 USC 3024 (m)(1)
b3 50 USC 3605

Received(Date): Wed, 1 Mar 2006 09:32:34 -0500
[2.28.06.AG responses to 2.6.QFRs.pdf](#)
[2.28.06.response to Feinstein pre-hearing questions.pdf](#)
[Responses to Sen. Feinstein's Questions \(2 28 06\).pdf](#)

Attached are the letters and QFR responses on the TSP that DOJ sent to the Senate Judiciary Committee yesterday. There are numerous additional QFRs that we are working on, and we will circulate drafts of those responses shortly.



The Attorney General

Washington, D.C.

February 28, 2006

The Honorable Arlen Specter
Chairman, Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Chairman Specter:

I write to provide responses to several questions posed to me at the hearing on "Wartime Executive Power and the National Security Agency's Surveillance Authority," held Monday, February 6, 2006, before the Senate Committee on the Judiciary. I also write to clarify certain of my responses at the February 6th hearing.

Except when otherwise indicated, this letter will be confined to addressing questions relating to the specific NSA activities that have been publicly confirmed by the President. Those activities involve the interception by the NSA of the contents of communications in which one party is outside the United States where there are reasonable grounds to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization (hereinafter, the "Terrorist Surveillance Program").

Additional Information Requested by Senators at February 6th Hearing

Senator Leahy asked whether the President first authorized the Terrorist Surveillance Program after he signed the Authorization for Use of Military Force of September 18, 2001 ("Force Resolution") and before he signed the USA PATRIOT Act. 2/6/06 Unofficial Hearing Transcript ("Tr.") at 50. The President first authorized the Program in October 2001, before he signed the USA PATRIOT Act.

Senator Brownback asked for recommendations on improving the Foreign Intelligence Surveillance Act ("FISA"). Tr. at 180-81. The Administration believes that it is unnecessary to amend FISA to accommodate the Terrorist Surveillance Program. The Administration will, of course, work with Congress and evaluate any proposals for improving FISA.

Senator Feinstein asked whether the Government had informed the Supreme Court of the Terrorist Surveillance Program when it briefed and argued *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004). Tr. at 207. The question presented in *Hamdi* was whether the military had validly detained Yaser Esam Hamdi, a presumed American citizen who was captured in Afghanistan during the combat operations in late 2001, whom the military had concluded to be an enemy combatant who should be detained in

connection with ongoing hostilities. No challenge was made concerning electronic surveillance and the Terrorist Surveillance Program was not a part of the lower court proceedings. The Government therefore did not brief the Supreme Court regarding the Terrorist Surveillance Program.

Senator Feinstein asked whether “any President ever authorized warrantless surveillance in the face of a statute passed by Congress which prohibits that surveillance.” Tr. at 208. I recalled that President Franklin Roosevelt had authorized warrantless surveillance in the face of a contrary statute, but wanted to confirm this. To the extent that the question is premised on the understanding that the Terrorist Surveillance Program conflicts with any statute, we disagree with that premise. The Terrorist Surveillance Program is entirely consistent with FISA, as explained in some detail in my testimony and the Department’s January 19th paper. As for the conduct of past Presidents, President Roosevelt directed Attorney General Jackson “to authorize the necessary investigating agents that they are at liberty to secure information by listening devices directed to the conversation or other communications of persons suspected of subversive activities against the Government of the United States.” Memorandum from President Roosevelt (May 21, 1940), reproduced in *United States v. United States District Court*, 444 F.2d 651, 670 (6th Cir. 1971) (Appendix A). President Roosevelt authorized this activity notwithstanding the language of 47 U.S.C. § 605, a prohibition of the Communications Act of 1934, which, at the time, provided that “no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person.” President Roosevelt took this action, moreover, despite the fact that the Supreme Court had, just three years earlier, made clear that section 605 “include[s] within its sweep federal officers.” *Nardone v. United States*, 302 U.S. 379, 384 (1937). It should be noted that section 605 prohibited interception followed by divulging or publishing the contents of the communication. The Department of Justice took the view that interception without “divulg[ing] or publish[ing]” was not prohibited, and it interpreted “divulge” narrowly to allow dissemination within the Executive Branch.

Senator Feingold asked, “[D]o you know of any other President who has authorized warrantless wiretaps outside of FISA since 1978 when FISA was passed?” Tr. at 217. The laws of the United States, both before and after FISA’s enactment, have long permitted various forms of foreign intelligence surveillance, including the use of wiretaps, outside the procedures of FISA. If the question is limited to “electronic surveillance” as defined in FISA, however, we are unaware of any such authorizations.

Senator Feingold asked, “[A]re there other actions under the use of military force for Afghanistan resolution that without the inherent power would not be permitted because of the FISA statute? Are there any other programs like that?” Tr. at 224. I understand the Senator to be referring to the Force Resolution, which authorizes the President to “use all necessary and appropriate force against those nations, organizations, or persons” responsible for the attacks of September 11th in order to prevent further terrorist attacks on the United States, and which by its terms is not limited to action

against Afghanistan or any other particular nation. I am not in a position to provide information here concerning any other intelligence activities beyond the Terrorist Surveillance Program. Consistent with long-standing practice, the Executive Branch notifies Congress concerning the classified intelligence activities of the United States through appropriate briefing of the oversight committees and congressional leadership.

Senator Feingold noted that, on September 10, 2002, then-Associate Deputy Attorney General David S. Kris testified before the Senate Judiciary Committee. Senator Feingold quoted Mr. Kris's statement that "[w]e cannot monitor anyone today whom we could not have monitored this time last year," and he asked me to provide the names of individuals in the Department of Justice and the White House who reviewed and approved Mr. Kris's testimony. Tr. at 225-26. Mr. Kris's testimony was addressing the Government's appeal in 2002 of decisions of the Foreign Intelligence Surveillance Court to the Foreign Intelligence Surveillance Court of Review. In the course of that discussion, Mr. Kris explained the effects of the USA PATRIOT Act's amendments to FISA, and, in particular, the amendment to FISA requiring that a "significant purpose" of the surveillance be the collection of foreign intelligence information. Mr. Kris explained that that amendment "will not and cannot change who the government may monitor." Mr. Kris emphasized that under FISA as amended, the Government still needed to show that there is probable cause that the target of the surveillance is an agent of a foreign power and that the surveillance has at least a significant foreign intelligence purpose. In context, it is apparent that Mr. Kris was addressing only the effects of the USA PATRIOT Act's amendments to FISA. In any event, his statements are also accurate with respect to the President's Terrorist Surveillance Program, because the Program involves the interception of communications only when there is probable cause ("reasonable grounds to believe") that at least one party to the communication is an agent of a foreign power (al Qaeda or an affiliated terrorist organization). Please note that it is Department of Justice policy not to identify the individual officials who reviewed and approved particular testimony.

Senators Biden and Schumer asked whether the legal analysis underlying the Terrorist Surveillance Program would extend to the interception of purely domestic calls. Tr. at 80-82, 233-34. The Department believes that the Force Resolution's authorization of "all necessary and appropriate force," which the Supreme Court in *Hamdi* interpreted to include the fundamental and accepted incidents of the use of military force, clearly encompasses the narrowly focused Terrorist Surveillance Program. The Program targets only communications in which one party is outside the United States and there are reasonable grounds to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. The Program is narrower than the wartime surveillances authorized by President Woodrow Wilson (*all* telephone, telegraph, and cable communications into and out of the United States) and President Franklin Roosevelt ("*all . . . telecommunications traffic* in and out of the United States"), based on their constitutional authority and general force-authorization resolutions like the Force Resolution. The Terrorist Surveillance Program fits comfortably within this historical precedent and tradition. The legal analysis set forth in the Department's January 19th paper does not address the interception of purely domestic communications.

The Department believes that the interception of the contents of domestic communications would present a different question from the interception of international communications, and the Department would need to analyze that question in light of all current circumstances before any such interception would be authorized.

Senator Schumer asked me whether the Force Resolution would support physical searches within the United States without complying with FISA procedures. Tr. at 159. The Terrorist Surveillance Program does not involve physical searches. Although FISA's physical search subchapter contains a provision analogous to section 109 of FISA, *see* 50 U.S.C. § 1827(a)(1) (prohibiting physical searches within the United States for foreign intelligence "except as authorized by statute"), physical searches conducted for foreign intelligence purposes present issues different from those discussed in the Department's January 19th paper addressing the legal basis for the Terrorist Surveillance Program. Thus, we would need to consider that issue specifically before taking a position.

Senator Schumer asked, "Have there been any abuses of the NSA surveillance program? Have there been any investigations arising from concerns about abuse of the NSA program? Has there been any disciplinary action taken against any official for abuses of the program?" Tr. at 237-38. Although no complex program like the Terrorist Surveillance Program can ever be free from inadvertent mistakes, the Program is the subject of intense oversight both within the NSA and outside that agency to ensure that any compliance issues are identified and resolved promptly on recognition. Procedures are in place, based on the guidelines I approved under Executive Order 12333, to protect the privacy of U.S. persons. NSA's Office of General Counsel has informed us that the oversight process conducted both by that office and by the NSA Inspector General has uncovered no abuses of the Terrorist Surveillance Program, and, accordingly, that no disciplinary action has been needed or taken because of abuses of the Program.

Clarification of Certain Responses

I would also like to clarify certain aspects of my responses to questions posed at the February 6th hearing.

First, as I emphasized in my opening statement, in all of my testimony at the hearing I addressed—with limited exceptions—only the legal underpinnings of the Terrorist Surveillance Program, as defined above. I did not and could not address operational aspects of the Program or any other classified intelligence activities. So, for example, when I testified in response to questions from Senator Leahy, "Sir, I have tried to outline for you and the Committee what the President has authorized, and that is all that he has authorized," Tr. at 53, I was confining my remarks to the Terrorist Surveillance Program as described by the President, the legality of which was the subject of the February 6th hearing.

Second, in response to questions from Senator Biden as to why the President's authorization of the Terrorist Surveillance Program does not provide for the interception of domestic communications within the United States of persons associated with al

Qaeda, I stated, “That analysis, quite frankly, had not been conducted.” Tr. at 82. In response to similar questions from Senator Kyl and Senator Schumer, I stated, “The legal analysis as to whether or not that kind of [domestic] surveillance—we haven’t done that kind of analysis because, of course, the President—that is not what the President has authorized,” Tr. at 92, and “I have said that I do not believe that we have done the analysis on that.” Tr. at 160. These statements may give the misimpression that the Department’s legal analysis has been static over time. Since I was testifying only as to the legal basis of the activity confirmed by the President, I was referring only to the legal analysis of the Department set out in the January 19th paper, which addressed that activity and therefore, of course, does not address the interception of purely domestic communications. However, I did not mean to suggest that no analysis beyond the January 19th paper had ever been conducted by the Department. The Department believes that the interception of the contents of domestic communications presents a different question from the interception of international communications, and the Department’s analysis of that question would always need to take account of all current circumstances before any such interception would be authorized.

Third, at one point in my afternoon testimony, in response to a question from Senator Feinstein, I stated, “I am not prepared at this juncture to say absolutely that if the AUMF argument does not work here, that FISA is unconstitutional as applied. I am not saying that.” Tr. at 209. As set forth in the January 19th paper, the Department believes that FISA is best read to allow a statute such as the Force Resolution to authorize electronic surveillance outside FISA procedures and, in any case, that the canon of constitutional avoidance requires adopting that interpretation. It is natural to approach the question whether FISA might be unconstitutional as applied in certain circumstances with extreme caution. But if an interpretation of FISA that allows the President to conduct the NSA activities were not “fairly possible,” and if FISA were read to impede the President’s ability to undertake actions necessary to fulfill his constitutional obligation to protect the Nation from foreign attack in the context of a congressionally authorized armed conflict against an enemy that has already staged the most deadly foreign attack in our Nation’s history, there would be serious doubt about the constitutionality of FISA as so applied. A statute may not “impede the President’s ability to perform his constitutional duty,” *Morrison v. Olson*, 487 U.S. 654, 691 (1988) (emphasis added); see also *id.* at 696-97, particularly not the President’s most solemn constitutional obligation—the defense of the Nation. See also *In re Sealed Case*, 310 F.3d 717, 742 (Foreign Intel. Surv. Ct. of Rev. 2002) (explaining that “FISA could not encroach on the President’s constitutional power”). I did not mean to suggest otherwise.

Fourth, in response to questions from Senator Leahy about when the Administration first determined that the Force Resolution authorized the Terrorist Surveillance Program, I stated, “From the very outset, before the program actually commenced.” Tr. at 184. I also stated, “Sir, it has always been our position that the President has the authority under the authorization to use military force and under the Constitution.” Tr. at 187. These statements may give the misimpression that the Department’s legal analysis has been static over time. As I attempted to clarify more generally, “[i]t has always been the [Department’s] position that FISA cannot be

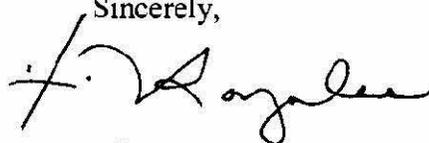
interpreted in a way that infringes upon the President's constitutional authority, that FISA must be interpreted, can be interpreted" to avoid that result. Tr. at 184; *see also* Tr. at 164 (Attorney General: "It has always been our position that FISA can be and must be read in a way that it doesn't infringe upon the President's constitutional authority."). Although the Department's analysis has always taken account of both the Force Resolution and the Constitution, it is also true, as one would expect, that the Department's legal analysis has evolved over time.

Fifth, Senator Cornyn suggested that the Terrorist Surveillance Program is designed to address the problem that FISA requires that we already know that someone is a terrorist before we can begin coverage. Senator Cornyn asked, "[T]he problem with FISA as written is that the surveillance it authorizes is unusable to discover who is a terrorist, as distinct from eavesdropping on known terrorists. Would you agree with that?" I responded, "That would be a different way of putting it, yes, sir." Tr. at 291. I want to be clear, however, that the Terrorist Surveillance Program targets the contents of communications in which one party is outside the United States and there are reasonable grounds to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. Although the President has authorized the Terrorist Surveillance Program in order to provide the early warning system we lacked on September 11th, I do not want to leave the Committee with the impression that it does so by doing away with a probable cause determination. Rather, it does so by allowing intelligence experts to respond agilely to all available intelligence and to begin coverage as quickly as possible.

Finally, in discussing the FISA process with Senator Brownback, I stated, "We have to know that a FISA Court judge is going to be absolutely convinced that this is an agent of a foreign power, that this facility is going to be a facility that is going to be used or is being used by an agent of a foreign power." Tr. at 300. The approval of a FISA application requires only probable cause to believe that the target is an agent of a foreign power and that the foreign power has used or is about to use the facility in question. 50 U.S.C. § 1805(a)(3). I meant only to convey how cautiously we approach the FISA process. It is of paramount importance that the Department maintain its strong and productive working relationship with the Foreign Intelligence Surveillance Court, one in which that court has come to know that it can rely on the representations of the attorneys that appear before it.

I hope that the Committee will find this additional information helpful.

Sincerely,

A handwritten signature in black ink, appearing to read "A. R. Gonzales", written in a cursive style.

Alberto R. Gonzales

cc: The Honorable Patrick Leahy
Ranking Member



U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

February 28, 2006

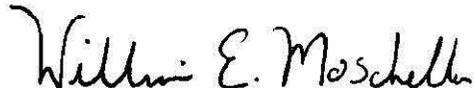
The Honorable Dianne Feinstein
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Senator Feinstein:

Please find attached responses to your letter, dated January 30, 2006, which posed questions to Attorney General Gonzales prior to his appearance before the Senate Committee on the Judiciary on February 6, 2006. The subject of the hearing was, "Wartime Executive Power and the National Security Agency's Surveillance Authority."

We trust you will find this information helpful. If we may be of further assistance on this, or any other matter, please do not hesitate to contact this office.

Sincerely,


William E. Moschella
Assistant Attorney General

Enclosure

cc: The Honorable Arlen Specter
Chairman, Committee on the Judiciary

The Honorable Patrick J. Leahy
Ranking Minority Member

RESPONSES TO QUESTIONS FROM SENATOR FEINSTEIN

1. I have been informed by former Majority Leader Senator Tom Daschle that the Administration asked that language be included in the “*Joint Resolution to Authorize the use of United States Armed Forces against those responsible for the recent attacks launched against the United States*” (P.L. 107-40) (hereinafter “the Authorization” or “AUMF”) which would add the words “in the United States” to its text, after the words “appropriate force.”

- **Who in the Administration contacted Senator Daschle with this request?**
- **Please provide copies of any communication reflecting this request, as well as any documents reflecting the legal reasoning which supported this request for additional language.**

The Congressional Research Service recently concluded that the account of Senator Daschle to which your question refers “is not reflected in the official record of the legislative debate” on the Authorization for Use of Military Force (hereinafter “Force Resolution”). See Richard F. Grimmet, *Authorization for Use of Military Force in Response to the 9/11 Attacks (P.L. 107-40): Legislative History* at 3 n.5 (Jan. 4, 2006). We do not recall such a discussion with former Senator Daschle and are not aware of any record reflecting such a conversation. In any event, a private discussion cannot change the plain meaning and evident intent of the Force Resolution, which clearly confirms and supplements the President’s authority to take military action within the United States.

In the Force Resolution, Congress expressly recognized that the September 11th attacks “render it both necessary and appropriate that the United States exercise its rights to self-defense and to protect United States citizens both *at home* and abroad.” Force Resolution pmbl. (emphasis added). Congress concluded that the attacks “continue to pose an unusual and extraordinary threat to the national security.” *Id.* Congress affirmed that “the President has authority under the Constitution to take action to deter and prevent actions of international terrorism *against the United States.*” *Id.* (emphasis added). Accordingly, Congress authorized the President “to use all necessary and appropriate force against those” associated with the attacks “in order to prevent future acts of international terrorism *against the United States.*” *Id.* (emphasis added).

The plain language of the Force Resolution clearly encompasses action within the United States. In addition, when Congress passed the Force Resolution on September 14, 2001, the World Trade Center was still burning, combat air patrols could be heard over many American cities, and there was great concern that another attack would follow shortly. Further, the attacks of September 11th were launched on United States soil by foreign agents who had been living in this country. Given this context and the plain meaning of the Force Resolution, Congress must be understood as having ratified the President’s authority to use force within the United States. A crucial responsibility of the President—charged by the Force Resolution and the Constitution to defend our Nation—

was and is to identify and disable those enemies, *especially if they are in the United States*, waiting to stage another strike.

2. Did any Administration representative communicate to any Member of Congress the view that the language of the Authorization as approved would provide legal authority for what otherwise would be a violation of the criminal prohibition of domestic electronic collection within the United States?

- **If so, who in the Administration made such communications?**
- **Are there any contemporaneous documents which reflect that view within the Administration?**

Although your question does not indicate what timeframe it covers, we understand it to ask whether, contemporaneous with the passage of the Force Resolution, Administration officials told Members of Congress that the Force Resolution would provide legal authorization for interception of the international communications of members and agents of al Qaeda and affiliated terrorist organizations. We are not aware of any specific communications between the Administration and Members of Congress during the three days between the September 11th attacks and the passage of the Force Resolution involving the particular issue of electronic surveillance—or, for that matter, any of the other fundamental incidents of the use of military force encompassed within the Force Resolution (such as the detention of U.S. citizens who are enemy combatants, which has since been upheld by the Supreme Court).

Although we are not aware of any specific discussion of what incidents of force would be authorized by a general authorization of force, the Supreme Court has explained that Congress must be understood to have authorized “fundamental and accepted” incidents of waging war. *Hamdi v. Rumsfeld*, 542 U.S. 507, 518 (2004) (plurality opinion); *see id.* at 587 (Thomas, J., dissenting). Consistent with this traditional understanding, other Presidents, including Woodrow Wilson and Franklin Roosevelt, have interpreted general force authorization resolutions to permit warrantless surveillance to intercept suspected enemy communications. *Cf. generally* Curtis A. Bradley & Jack L. Goldsmith, *Congressional Authorization and the War on Terrorism*, 118 Harv. L. Rev. 2048, 2091 (2005) (explaining that, with the Force Resolution, “Congress intended to authorize the President to take at least those actions permitted by the laws of war”).

The understanding at the time of the passage of the Force Resolution was that it was important to act quickly and to invest the President with the authority to use “all necessary and appropriate force” against those associated with the September 11th attacks and to prevent further terrorist attacks on the United States. Congress could not have cataloged every possible aspect of the use of military force it intended to endorse. Rather than engage in that difficult and impractical exercise, Congress authorized the President, in general but intentionally broad and powerful terms, to use the fundamental and accepted incidents of the use of military force and to determine how best to identify and to engage the enemy in the current armed conflict. That is traditionally how Congress has acted at the outset of armed conflict: “because of the changeable and

explosive nature of contemporary international relations . . . Congress—in giving the Executive authority over matters of foreign affairs—must of necessity paint with a brush broader than that it customarily wields in domestic areas.” *Zemel v. Rusk*, 381 U.S. 1, 17 (1965); *cf. Dames & Moore v. Regan*, 453 U.S. 654, 678 (1981) (“Congress cannot anticipate and legislate with regard to every possible action the President may find it necessary to take.”).

3. According to Assistant Attorney General William Moschella’s letter of December 22, 2005, and the subsequent “White Paper,” it is the view of the Department of Justice that the Authorization “satisfies section [FISA section] 109’s requirement for statutory authorization of electronic surveillance.”¹

- **Are there other statutes which, in the view of the Department, have been similarly affected by the passage of the Authorization?**
- **If so, please provide a comprehensive list of these statutes.**
- **Has the President, or any other senior Administration official, issued any order or directive based on the AUMF which modifies, supersedes or alters the application of any statute?**

Five members of the Supreme Court concluded in *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004), that the Force Resolution satisfies 18 U.S.C. § 4001(a)’s prohibition on detention of U.S. citizens “except pursuant to an Act of Congress,” and thereby authorizes the detention even of Americans who are enemy combatants. The Foreign Intelligence Surveillance Act of 1978 (“FISA”) contains a similar provision indicating that it contemplates that electronic surveillance could be authorized in the future “by statute.” Section 109 of FISA prohibits persons from “engag[ing] . . . in electronic surveillance under color of law *except as authorized by statute.*” 50 U.S.C. § 1809(a)(1) (emphasis added). Just as the Force Resolution satisfies the restrictions imposed by section 4001(a), it also satisfies the statutory authorization requirement of section 109 of FISA.

We have not sought to catalog every instance in which the Force Resolution might satisfy a statutory authorization requirement contained in another statute, other than FISA and section 4001(a), the provision at issue in *Hamdi*. We have not found it necessary to determine the full effect of the Force Resolution to conclude that it authorizes the terrorist surveillance program described by the President, which involves the interception of the contents of communications where one end of the communication is outside the United States and there are reasonable grounds to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization (hereinafter, the “Terrorist Surveillance Program”).

¹ **Letter, Assistant Attorney General Williams Moschella to Senator Pat Roberts, et al., December 22, 2005, at p. 3 (hereinafter “Moschella Letter”).**

4. The National Security Act of 1947, as amended, provides that “[a]ppropriated funds available to an intelligence agency may be obligated or expended for an intelligence or intelligence-related activity only if . . . (1) those funds were specifically authorized by the Congress for use for such activities . . .”² It appears that the domestic electronic surveillance conducted within the United States by the National Security Agency was not “specifically authorized,” and thus may be prohibited by the National Security Agency of 1947.

- **What legal authority would justify expending funds in support of this program without the required authorization?**

The General Counsel of the National Security Agency has assured the Department of Justice that the Terrorist Surveillance Program complies with section 504 of the National Security Act of 1947, the provision quoted in your question.

5. The Constitution provides that “[n]o money shall be drawn from the Treasury, but in consequence of appropriations made by law.”³ Title 31, Section 1341 (the Anti-Deficiency Act) provides that “[a]n officer or employee of the United States Government . . . may not – make or authorize an expenditure or obligation exceeding an amount available in an appropriation or fund for the expenditure or obligation,” and Section 1351 of the same Title adds that “an officer or employee of the United States Government or of the District of Columbia government knowingly and willfully violating sections 1341(a) or 1342 of this title shall be fined not more than \$5,000, imprisoned for not more than 2 years, or both.” In sum, the Constitution prohibits, and the law makes criminal, the spending of funds except those funds appropriated in law.

- **Were the funds expended in support of this program appropriated?**
- **If yes, which law appropriated the funds?**
- **Please identify, by name and title, what “officer or employee” of the United States made or authorized the expenditure of the funds in support of this program?**

As stated above, the General Counsel of the National Security Agency has assured the Department of Justice that the applicable statutory standard has been satisfied.

6. Are there any other intelligence programs or activities, including, but not limited to, monitoring internet searches, emails and online purchases, which, in the view of

² National Security Act of 1947, as amended, Section 504, codified at 50 U.S.C. 414.

³ U.S. Constitution, Article I, Section 7.

the Department of Justice, have been authorized by law, although kept secret from some members of the authorizing committee?

- **If so, please list and describe such programs.**

The National Security Act of 1947 contemplates that the Intelligence Committees of both Houses would be appropriately notified of intelligence programs and the Act specifically contemplates more limited disclosure in the case of exceptionally sensitive matters. Title 50 of the U.S. Code provides that the Director of National Intelligence and the heads of all departments, agencies, and other entities of the Government involved in intelligence activities shall keep the Intelligence Committees fully and currently informed of intelligence activities “[t]o the extent consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters.” 50 U.S.C. §§ 413a(a), 413b(b). It has long been the practice of both Democratic and Republican administrations to inform the Chair and Ranking Members of the Intelligence Committees about exceptionally sensitive matters. The Congressional Research Service has acknowledged that the leaders of the Intelligence Committees “over time have accepted the executive branch practice of limiting notification of intelligence activities in some cases to either the Gang of Eight, or to the chairmen and ranking members of the intelligence committees.” See Alfred Cumming, *Statutory Procedures Under Which Congress is to be Informed of U.S. Intelligence Activities, Including Covert Actions*, Congressional Research Service Memorandum at 10 (Jan. 18, 2006). This Administration has followed this well-established practice by briefing the leadership of the Intelligence Committees about intelligence programs or activities as required by the National Security Act of 1947.

7. Are there any other expenditures which have been made or authorized which have not been specifically appropriated in law, and which have been kept secret from members of the Appropriations Committee?

- **If so, please list and describe such programs.**

As stated above, the NSA has indicated that expenditures on the Terrorist Surveillance Program comply with the National Security Act and applicable appropriations law.

8. At a White House press briefing, on December 19, 2005, you stated that that the Administration did not seek authorization in law for this NSA surveillance program because “you were advised that that was not . . . something [you] could likely get” from Congress.

- **What were your sources of this advice?**
- **As a matter of constitutional law, is it the view of the Department that the scope of the President’s authority increases when he believes that the legislative branch will not pass a law he approves of?**

As the Attorney General clarified both later in the December 19th briefing that you cite and on December 21, 2005, it is not the case that the Administration declined to seek a specific authorization of the Terrorist Surveillance Program because we believed Congress would not authorize it. See Remarks by Homeland Security Secretary Chertoff and Attorney General Gonzales on the USA PATRIOT Act, *available at* <http://www.dhs.gov/dhspublic/display?content=5285>. Rather, as the Attorney General has testified, the consensus view in the discussions with Members of Congress was that it was unlikely, if not impossible, that more specific legislation could be enacted without compromising the Terrorist Surveillance Program by disclosing operational details, limitations, and capabilities to our enemies. Such disclosures would necessarily have compromised our national security.

9. The Department of Justice’s position, as explained in the Moschella Letter and the subsequent White Paper, is that even if the AUMF is determined not to provide the legal authority for conduct which otherwise would be prohibited by law, the President’s “inherent” powers as Commander-in-Chief provide independent authority.

- **Is this an accurate assessment of the Department’s position?**

As the Department has explained, the Force Resolution does provide legal authority for the Terrorist Surveillance Program. The Force Resolution is framed in broad and powerful terms, and a majority of the Justices of the Supreme Court concluded in *Hamdi v. Rumsfeld* that the Force Resolution authorized the “fundamental and accepted” incidents of the use of military force. Moreover, when it enacted the Force Resolution, Congress was legislating in light of the fact that past Presidents (including Woodrow Wilson and Franklin Roosevelt) had interpreted similarly broad resolutions to authorize much wider warrantless interception of international communications.

Even if there were some ambiguity regarding whether FISA and the Force Resolution may be read in harmony to allow the President to authorize the Terrorist Surveillance Program, the President’s inherent powers as Commander in Chief and as chief representative of the Nation in foreign affairs to undertake electronic surveillance against the declared enemy of the United States during an armed conflict would require resolving such ambiguity in favor of the President’s authority. Under the canon of constitutional avoidance, courts generally interpret statutes to avoid serious constitutional questions where “fairly possible.” *INS v. St. Cyr*, 533 U.S. 289, 299-300 (2001) (citations omitted); *Ashwander v. TVA*, 297 U.S. 288, 345-48 (1936) (Brandeis, J., concurring). The canon of constitutional avoidance has particular importance in the realm of national security, where the President’s constitutional authority is at its highest. See *Department of the Navy v. Egan*, 484 U.S. 518, 527, 530 (1988); 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”). Thus, we need not confront the question whether the President’s inherent powers in this area would authorize conduct otherwise prohibited by statute.

Even if the Force Resolution were determined not to provide the legal authority, it is the position of the Department of Justice, maintained by both Democratic and Republican administrations, that the President's inherent authority to authorize foreign-intelligence surveillance would permit him to authorize the Terrorist Surveillance Program. President Carter's Attorney General, Griffin Bell, testified at a hearing on FISA as follows: "[T]he current bill recognizes no inherent power of the President to conduct electronic surveillance, and I want to interpolate here to say that *this does not take away the power of the President under the Constitution.*" Hearing Before the Subcomm. on Legislation of the House Permanent Select Comm. on Intelligence (Jan. 10, 1978) (emphasis added). Thus, in saying that President Carter agreed to follow the procedures of FISA, Attorney General Bell made clear that FISA could not take away the President's Article II authority. More recently, the Foreign Intelligence Surveillance Court of Review, the specialized court of appeals that Congress established to review the decisions of the Foreign Intelligence Surveillance Court, recognized that the President has inherent constitutional authority to gather foreign intelligence that cannot be intruded upon by Congress. The court explained that all courts to have addressed the issue of the President's inherent authority 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). On the basis of that unbroken line of precedent, the court "[took] for granted that the President does have that authority," and concluded that, assuming that is so, "*FISA could not encroach on the President's constitutional power.*" *Id.* (emphasis added).

10. Based on the Moschella Letter and the subsequent White Paper, I understand that it is the position of the Department of Justice that the National Security Agency, with respect to this program of domestic electronic surveillance, is functioning as an element of the Department of Defense generally, and as one of a part of the "Armed Forces of the United States," as referred to in the AUMF.

- **Is this an accurate understanding of the Department's position?**

As explained above, the Terrorist Surveillance Program is not a program of "domestic" electronic surveillance.

The NSA is within the Department of Defense, and the Director of the NSA reports directly to the Secretary of Defense. Although organized under the Department of Defense, the NSA is not part of the "Armed Forces of the United States," which consists of the Army, Navy, Air Force, Marine Corps, and Coast Guard. 10 U.S.C. § 101(a)(4). The President has constitutional authority to direct that resources under his control (including assets that are not part of the Armed Forces of the United States) be used for military purposes. In addition, the Department would not interpret the Force Resolution to authorize the President to use only the Armed Forces in his effort to protect the Nation.

11. Article 8 of the Constitution provides that the Congress "shall make Rules for the Government and Regulation of the land and naval forces." It appears that the

Foreign Intelligence Surveillance Act (FISA), as applied to the National Security Agency, is precisely the type of “Rule” provided for in this section.

- **Is it the position of the Department of Justice that the President’s Commander-in-Chief power is superior to the Article 8 powers of Congress?**
- **Does the Department of Justice believe that if the President disagrees with a law passed by Congress as part of its responsibility to regulate the Armed Forces, the law is not binding?**

It is emphatically *not* the position of the Department of Justice that the President’s authority as Commander in Chief is superior to Congress’s authority set forth in Article I, Section 8 of the Constitution. As we have explained, the Terrorist Surveillance Program is fully consistent with FISA, because Congress authorized it through the Force Resolution. Nor is it the position of the Department of Justice “that if the President disagrees with a law passed by Congress as part of its responsibility to regulate the Armed Forces, the law is not binding.” No one is above the law.

The inherent authority of the President to conduct warrantless foreign intelligence surveillance is well established, and *every* court of appeals to have considered the question has determined that the President has such authority, even during peacetime. On the basis of that unbroken line of precedent, the Foreign Intelligence Surveillance Court of Review “[took] for granted that the President does have that authority” and concluded that, assuming that is so, “FISA could not encroach on the President’s constitutional power.” *In re Sealed Case*, 310 F.3d 717, 742 (2002).

The scope of Congress’s authority to make rules for the regulation of the land and naval forces is not entirely clear. The Supreme Court traditionally has construed this authority to provide for military discipline of members of the Armed Forces by, for example, “grant[ing] the Congress power to adopt the Uniform Code of Military Justice” for offenses committed by servicemembers, *Kinsella v. United States ex rel. Singleton*, 361 U.S. 234, 247 (1960), and by providing for the establishment of military courts to try such cases, *see Ryder v. United States*, 515 U.S. 177, 186 (1995); *Madsen v. Kinsella*, 343 U.S. 341, 347 (1952); *see also McCarty v. McCarty*, 453 U.S. 210, 232-233 (1981) (noting enactment of military retirement system pursuant to power to make rules for the regulation of land and naval forces). That reading is consistent with the Clause’s authorization to regulate “Forces,” rather than the *use* of force. Whatever the scope of Congress’s authority, however, Congress may not “impede the President’s ability to perform his constitutional duty,” *Morrison v. Olson*, 487 U.S. 654, 691 (1988); *see also id.* at 696-97, particularly not the President’s most solemn constitutional obligation—the defense of the Nation.

The potential conflict of Congress’s authority with the President’s in these circumstances would present a serious constitutional question, which, as described above, can and must be avoided by construing the Force Resolution to authorize the fundamental and accepted incidents of war, consistent with historical practice.

12. On January 24, 2006, during an interview with CNN, you said that “[a]s far as I’m concerned, we have briefed Congress . . . [t]hey’re aware of the scope of the program.”

- **Please explain the basis for the assertion that I was briefed on this program, or that I am “aware of the scope of the program.”**

The quotation to which your question refers is not from an interview on CNN, but is a quotation reported on the CNN Website that is attributed to the Attorney General’s remarks at Georgetown University on January 24, 2006. *See* <http://www.cnn.com/2006/POLITICS/01/24/nsa.strategy/index.html>. The prepared text of that speech accurately reflects that “[t]he *leadership of Congress, including the leaders of the Intelligence Committees of both Houses of Congress*, have been briefed about this program more than a dozen times since 2001.” *See* http://www.usdoj.gov/ag/speeches/2006/ag_speech_0601242.html (emphasis added). Similarly, during a January 16, 2006, interview on CNN, the Attorney General accurately stated that “we have briefed *certain members of Congress* regarding the operations of these activities and have given examples of where these authorities, where the activities under this program have been extremely helpful in protecting America.” *See* <http://archives.cnn.com/TRANSCRIPTS/060116/lkl.01.html> (emphasis added). The Attorney General has not asserted that every Member of Congress was briefed on the Terrorist Surveillance Program, or that you specifically have been briefed on it. However, in accordance with long-standing practice regarding exceptionally sensitive intelligence matters, the Department believes that the briefing of congressional leaders satisfies the Administration’s responsibility to keep Congress apprised of the Terrorist Surveillance Program. This view is shared by the Administration and by the Chairmen of both the House and Senate Intelligence Committees. *See* Letter from the Honorable Peter Hoekstra, Chairman, House Permanent Select Committee on Intelligence, to Daniel Mulholland, Director, Congressional Research Service at 1-3 (Feb. 1, 2006); Letter from the Honorable Pat Roberts, Chairman Senate Committee on Intelligence, to the Honorable Arlen Specter and the Honorable Patrick Leahy at 16-17 (Feb. 3, 2006).

13. It appears from recent press coverage that Mr. Rove has been briefed about this program, which, as I understand it, is considered too sensitive to brief to Senators who are members of the Senate Intelligence Committee.

- **Who decided that Mr. Rove was to be briefed about the program, and what is his need-to-know?**
- **Is the program classified pursuant to Executive Order 12958, and if so, who was the classifying authority, and under what authority provided in Executive Order 12958 was the classification decision made?**
- **How many executive branch officials have been advised of the nature, scope and content of the program? Please provide a list of their names and positions.**

- **How many individuals outside the executive branch have been advised of the nature, scope and content of the program? Please provide a list of their names and positions.**

The Terrorist Surveillance Program remains classified, and we may discuss only those aspects of the Program that have been described by the President. In general, the identity of individuals who have been briefed into the Program is also classified. The Program was classified pursuant to sections 1.4(c) and (e) of Executive Order 12958, as amended by Executive Order 13292 (March 28, 2003).

14. The AUMF authorizes the President to use “all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons.”

- **What do you believe are the conditions under which the President’s authority to conduct the NSA program pursuant to the Authorization would expire?**

As you know, al Qaeda leaders repeatedly have announced their intention to attack the United States again. As recently as December 7, 2005, Ayman al-Zawahiri stated that al Qaeda “is spreading, growing, and becoming stronger,” and that al Qaeda is “waging a great historic battle in Iraq, Afghanistan, Palestine, and even in the Crusaders’ own homes.” Ayman al-Zawahiri, videotape released on Al-Jazeera television network (Dec. 7, 2005). And just last month, Osama bin Laden warned that al Qaeda was preparing another attack on our homeland. After noting the deadly bombings committed in London and Madrid, he said:

The delay in similar operations happening in America has not been because of failure to break through your security measures. The operations are under preparation and you *will see them in your homes* the minute they are through (with preparations), with God’s permission.

Quoted at <http://www.breitbart.com/news/2006/01/19/D8F7SMRH5.html> (Jan. 19, 2006) (emphasis added). The threat from Al Qaeda continues to be real. Thus, the necessity for the President to take these actions continues today.

As a general matter, the authorization for the Terrorist Surveillance Program that is provided by the Force Resolution would expire when the “nations, organizations, or persons [the President] determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001,” no longer pose a threat to the United States. The authorization that is provided by the Force Resolution also would expire if it were repealed through legislation. In addition, the Program by its own terms expires

approximately every 45 days unless it is reauthorized after a review process that includes a review of the current threat to the United States posed by al Qaeda and its affiliates.

15. The Department of Justice White Paper states that the program is used when there is a “reasonable basis” to conclude that one party is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda.

- **Can the program be used against a person who is a member of an organization affiliated with al Qaeda, but where the organization has no connection to the 9/11 attacks themselves?**
- **Can you define the terms “reasonable basis” and “affiliated?” Are there any examples, for instance, from criminal law that can describe the “reasonable basis” standard that is being used for the NSA program? What about “affiliated?”**
- **Is it comparable to the “agent of” standard in FISA?**
- **Can the program be used to prevent terrorist attacks by an organization other than al Qaeda?**

The Terrorist Surveillance Program targets communications only where one party is outside the United States and where there are reasonable grounds to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. The “reasonable grounds to believe” standard is essentially a “probable cause” standard of proof. *See Maryland v. Pringle*, 540 U.S. 366, 371 (2003) (“We have stated . . . that “[t]he substance of all the definitions of probable cause is a reasonable ground for belief of guilt.”). The critical advantage offered by the Terrorist Surveillance Program compared to FISA is *who* makes the probable cause determination and how many layers of review will occur *before* surveillance begins. Under the Terrorist Surveillance Program, professional intelligence officers, who are experts on al Qaeda and its tactics (including its use of communication systems), with appropriate and rigorous oversight, make the decisions about which international communications should be intercepted. Relying on the best available intelligence, these officers determine before intercepting any communications whether there are “reasonable grounds to believe” that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. By contrast, even the most expedited traditional FISA process would involve review by NSA intelligence officers, NSA lawyers, Justice Department lawyers, and the Attorney General before even emergency surveillance would begin. In the narrow context of defending the Nation in this congressionally authorized armed conflict with al Qaeda, we must allow these highly trained intelligence experts to use their skills and knowledge to protect us.

Answering the rest of these questions would require discussion of operational aspects of the Program.

16. In addition to open combat, the detention of enemy combatants and electronic surveillance, what else do you consider being “incident to” the use of military force? Are interrogations of captives “incident to” the use of military force?

A majority of the Justices in *Hamdi v. Rumsfeld* concluded that the Force Resolution's authorization of "all necessary and appropriate force" includes fundamental and accepted incidents of the use of military force. See 542 U.S. 507, 518 (2004) (plurality opinion); *id.* at 587 (Thomas, J., dissenting). As your question acknowledges, a majority of the Justices concluded that the detention of enemy combatants is a fundamental and accepted incident of the use of military force. As explained at length in our January 19th paper, signals intelligence is a fundamental and accepted incident of the use of military force. Consistent with that understanding, other Presidents, including Woodrow Wilson and Franklin Roosevelt, have interpreted general force-authorization resolutions to permit warrantless surveillance during wartime to intercept suspected enemy communications. In addition, we note that the Supreme Court has stated in a slightly different context that "[a]n important incident to the conduct of war is the adoption of measures by the military command not only to repel and defeat the enemy, but to seize and subject to disciplinary measures those enemies who in their attempt to thwart or impede our military effort have violated the law of war." *Ex Parte Quirin*, 317 U.S. 1, 29 (1942).

In light of the strictly limited nature of the Terrorist Surveillance Program, we do not think it a useful or a practical exercise to engage in speculation about the outer limits of what kinds of military activity might be authorized by the Force Resolution. It is sufficient to note that, as discussed at length in the Department's January 19th paper, the use of signals intelligence to intercept the international communications of the enemy has traditionally been recognized as one of the core incidents of the use of military force.

17. The program is reportedly defined as where one party is in the U.S. and one party in a foreign country. Regardless of how the program is actually used, does the AUMF authorize the President to use the program against calls or emails entirely within the U.S.?

We believe that the Force Resolution's authorization of "all necessary and appropriate force," which the Supreme Court in *Hamdi* interpreted to include the fundamental and accepted incidents of the use of military force, clearly encompasses the narrowly focused Terrorist Surveillance Program. The Program targets only the communications where one party is outside the United States and where there are reasonable grounds to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. Indeed, the Program is much narrower than the wartime surveillances authorized by President Woodrow Wilson (*all* telephone, telegraph, and cable communications into and out of the United States) and President Franklin Roosevelt ("*all . . . telecommunications traffic* in and out of the United States"), based on their constitutional authority and general force-authorization resolutions like the Force Resolution. The narrow Terrorist Surveillance Program fits comfortably within this precedent and tradition. Interception of the contents of domestic communications presents a different legal question which is not implicated here.

18. FISA has safeguard provisions for the destruction of information that is not foreign intelligence. For instance, albeit with some specific exceptions, if no FISA order is obtained within 72 hours, material gathered without a warrant is destroyed.

- **Are there procedures in place for the destruction of information collected under the NSA program that is not foreign intelligence?**
- **If so, what are the procedures?**
- **Who determines whether the information is retained?**

Procedures are in place to protect U.S. privacy rights, including applicable procedures from Attorney General guidelines issued pursuant to Executive Order 12333, that govern acquisition, retention, and dissemination of information relating to U.S. persons.

19. The DOJ White Paper relies on broad language in the preamble that is contained in both the AUMF and the *Authorization for the Use of Military Force Against Iraq* as a source of the President’s authority.

- **Does the Iraq Resolution provide similar authority to the President to engage in electronic surveillance? For instance, would it have been authorized to conduct surveillance of communications between an individual in the U.S. and someone in Iraq immediately after the invasion?**

The Authorization for Use of Military Force Against Iraq, Pub. L. 107-243 (Oct. 16, 2002), provides that the “President is authorized to use the Armed Forces of the United States as he determines to be necessary and appropriate in order to—(1) defend the national security of the United States against the continuing threat posed by Iraq; and (2) enforce all relevant United Nations Security Council resolutions regarding Iraq.” *Id.* § 3(a). Under appropriate circumstances, the Iraq Resolution would authorize electronic surveillance of enemy communications. *See generally* Curtis A. Bradley & Jack L. Goldsmith, *Congressional Authorization and the War on Terrorism*, 118 Harv. L. Rev. 2047, 2093 (2005) (stating that the “generally accepted view” is “that a broad and unqualified authorization to use force empowers the President to do to the enemy what the laws of war permit”).

20. In a December 17, 2005, radio address the President stated, “I authorized the National Security Agency...to intercept the international communications of people with known links to al Qaeda and related terrorist organizations.”

- **What is the standard for establishing a link between a terrorist organization and a target of this program?**
- **How many such communications have been intercepted during the life of this program? How many disseminated intelligence reports have resulted from this collection?**
- **Has the NSA intercepted under this program any communications by journalists, clergy, non-governmental organizations (NGOs) or family**

members of U.S. military personnel? If so, for what purpose, and under what authority?

Before the international communications of an individual may be targeted for interception under the Terrorist Surveillance Program, there must be reasonable grounds to believe that the individual is a member or agent of al Qaeda or an affiliated terrorist organization. That standard of proof is appropriately considered as “a practical, nontechnical conception that deals with the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act.” *Maryland v. Pringle*, 540 U.S. 366, 370 (2003) (internal quotation marks omitted) (describing “probable cause” standard). We cannot provide more detail without discussing operational aspects of the Program.

21. In a December 17, 2005, radio address the President stated, “The activities I authorized are reviewed approximately every 45 days...The review includes approval by our Nation’s top legal officials, including the Attorney General and the Counsel to the President.”

- **As White House Counsel during the first 4 years this program was implemented, were you aware of this program and of the legal arguments supporting it when this Committee considered your nomination to be Attorney General?**
- **Who is responsible for determining whether to reauthorize this program, and upon what basis is this determination made?**

As an initial matter, the Department wishes to emphasize the seriousness with which this Administration takes these periodic reviews and reauthorizations of the Terrorist Surveillance Program. The requirement that the Terrorist Surveillance Program be reviewed and reauthorized at the highest levels of Government approximately every 45 days ensures that the Program will not be continued unless the al Qaeda threat to the United States continues to justify use of the Program.

The President sought legal advice prior to authorizing the Program and was advised that it is lawful. The Program has been reviewed by the Department of Justice, by lawyers at the NSA, and by the Counsel to the President. The Attorney General was involved in advising the President about the Program in his capacity as Counsel to the President, and he has been involved in approving the legality of the Program during his time as Attorney General. Since 2001, the Program has been reviewed multiple times by different counsel. The Terrorist Surveillance Program is lawful in all respects, as explained in the Justice Department paper of January 19, 2006.

The President is responsible for reauthorizing the Program. That determination is based on reviews undertaken by the Intelligence Community and Department of Justice, a strategic assessment of the continuing importance of the Program to the national security of the United States, and assurances that safeguards continue to protect civil liberties.

22. In a Press Briefing on December 19, 2005, you said that you “believe the President has the inherent authority under the Constitution, as Commander-in-Chief, to engage in this kind of activity [domestic surveillance].” This authority is further asserted in the Department of Justice White Paper of January 19, 2006.

- **Has the President ever invoked this authority, with respect to any activity other than the NSA surveillance program?**
- **Has any other order or directive been issued by the President, or any other senior administration official, based on such authority which authorizes conduct which would otherwise be prohibited by law?**

i. Can the President suspend (in secret or otherwise) the application of Section 503 of the National Security Act of 1947 (50 U.S.C. 413(b)), which states that “no covert action may be conducted which is intended to influence United States political processes, public opinion, policies or media?”

1. If so, has such authority been exercised?

ii. Can the President suspend (in secret or otherwise) the application of the Posse Comitatus Act (18 U.S.C. 1385)?

1. If so, has such authority been exercised?

iii. Can the President suspend (in secret or otherwise) the application of 18 U.S.C. 1001, which prohibits “the making the false statements within the executive, legislative, or judicial branch of the Government of the United States.”

1. If so, has such authority been exercised?

The Terrorist Surveillance Program targets for interception *international* communications of our enemy in the armed conflict with al Qaeda. As Congress expressly recognized in the Force Resolution, “the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States,” Force Resolution pmb., especially in the context of the current conflict. Article II of the Constitution vests in the President all executive power of the United States, including the power to act as Commander in Chief, *see* U.S. Const. art. II, § 2, and authority over the conduct of the Nation’s foreign affairs. As the Supreme Court has explained, “[t]he President is the sole organ of the nation in its external relations, and its sole representative with foreign nations.” *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 319 (1936) (internal quotation marks and citations omitted). In this way, the Constitution grants the President inherent power to protect the Nation from foreign attack, *see, e.g., The Prize Cases*, 67 U.S. (2 Black) 635, 668 (1863), and to protect national security information, *see, e.g., Department of the Navy v. Egan*, 484 U.S. 518, 527 (1988).

The President has used his constitutional authority to protect the Nation. Although no statute had yet authorized the use of military force, the President scrambled military aircraft during the attacks of September 11th to protect the Nation from further attack and continued those patrols for days before the Force Resolution was passed by Congress and signed by the President.

The Terrorist Surveillance Program is not, as your question suggests, “otherwise prohibited by law.” FISA expressly contemplates that in a separate statute Congress may authorize electronic surveillance outside FISA procedures. *See* 50 U.S.C. § 1809(a)(1) (FISA § 109, prohibiting any person from intentionally “engag[ing] . . . in electronic surveillance under color of law *except as authorized by statute*”) (emphasis added). That is what Congress did in the Force Resolution. As *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004), makes clear, a general authorization to use military force carries with it the authority to employ the fundamental and accepted incidents of the use of force. That is so even if Congress did not specifically address each of the incidents of force; thus, a majority of the Court concluded that the Force Resolution authorized the detention of enemy combatants as a fundamental incident of force, and Justice O’Connor stated that “it is of no moment that the [Force Resolution] does not use specific language of detention.” *Id.* at 519 (plurality opinion). Indeed, a majority of Justices in *Hamdi* concluded that the Force Resolution satisfied a statute nearly identical to section 109 of FISA, 18 U.S.C. § 4001(a), which prohibits the detention of United States citizens “except pursuant to an Act of Congress.” As explained at length in the Department’s January 19th paper, signals intelligence is a fundamental and accepted incident of the use of military force. Consistent with this traditional practice, other Presidents, including Woodrow Wilson and Franklin Roosevelt, have interpreted general force-authorization resolutions to permit interception of suspected enemy communications. Thus, the President has not “authorize[d] conduct which would otherwise be prohibited by law.”

It would not be appropriate for the Department to speculate about whether various other statutes, in circumstances not presented here, could yield to the President’s constitutional authority. As Justice Jackson has written, the division of authority between the President and Congress should not be delineated in the abstract. *See Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635 (1952) (Jackson, J., concurring) (“The actual art of governing under our Constitution does not and cannot conform to judicial definitions of the power of any of its branches based on isolated clauses or even single Articles torn from context.”); *see also Dames & Moore v. Regan*, 453 U.S. 654, 660-61 (1981). Without a specific factual circumstance in which such a decision would be made, speculating about such possibilities in the abstract is not fruitful.

Nevertheless, we have explained that the Force Resolution provides authority for the fundamental incidents of the use of force. The Department does not believe that covert action aimed at affecting the United States political process or lying to Congress would constitute a fundamental incident of the use of force.

Finally, the Posse Comitatus Act generally prohibits using the Army or Air Force for domestic law enforcement purposes absent statutory authorization. That statute does

not address the use of military force for military purposes, including national defense, in the armed conflict with al Qaeda.

23. Had the Department of Justice adopted the interpretation of the AUMF asserted in the Moschella letter and subsequent White Paper at the time it discussed the USA-Patriot Act with members of Congress? That act substantially altered FISA, and yet, to my knowledge, there was no discussion of the legal conclusions you now assert – that the AUMF has triggered the “authorized by other statute” wording of FISA.

- **Please provide any communications, internal or external, which are contemporaneous to the negotiation of the USA-Patriot Act, which contain information regarding this question.**

As you know, on January 19th, the Department of Justice released a 42-page paper setting out a comprehensive explanation of the legal authorities supporting the Terrorist Surveillance Program. The paper reflects the substance of the Department’s legal analysis of the Terrorist Surveillance Program. We have always interpreted FISA not to infringe on the President’s constitutional authority to protect the Nation from foreign attacks. It is also true, as one would expect, that our legal analysis has evolved over time.

It would be inappropriate for us to reveal any confidential and privileged internal deliberations of the Executive Branch. The Department is not aware of communications with Congress in connection with the negotiation of the USA PATRIOT Act concerning the effect of the Force Resolution.

24. The USA-Patriot Act reauthorization bill is currently being considered by the Congress. Among the provisions at issue is Section 215, which governs the physical search authorization under FISA. Does the legal analysis proposed by the Department also apply to this section of FISA? If so, is the Department’s position that, regardless of whether the Congress adopts the pending Conference Report, the Senate bill language, or some other formulation, the President may order the application of a different standard or procedure based on the AUMF or his Commander-in-Chief authority?

- **If so, is there any need to reauthorize those sections of the USA-Patriot Act which authorize domestic surveillance?**

FISA remains an essential and invaluable tool for foreign intelligence collection both in the armed conflict with al Qaeda and in other contexts. In contrast to surveillance conducted pursuant to the Force Resolution, FISA is not limited to al Qaeda and affiliated terrorist organizations. In addition, FISA has procedures that specifically allow the Government to use evidence in criminal prosecutions and, at the same time, protect intelligence sources and methods. In short, there is an urgent need to reauthorize the USA PATRIOT Act.

The Terrorist Surveillance Program does not involve physical searches. FISA's physical search subchapter contains a provision analogous to section 109, *see* 50 U.S.C. § 1827(a)(1) (prohibiting physical searches within the United States for foreign intelligence "except as authorized by statute"). Physical searches conducted for foreign intelligence purposes present questions different from those discussed in the January 19th paper addressing the legal basis for the Terrorist Surveillance Program. Thus, we would need to consider that issue specifically before taking a position.

25. Public statements made by you, as well as the President, imply that this program is used to identify terrorist operatives within the United States. Have any such operatives in fact been identified? If so, have these individuals been detained, and if so, where, and under what authority? Have any been killed?

- **The arrest and subsequent detention of Jose Padilla is, to my knowledge, the last public acknowledgement of the apprehension of an individual classified as an "enemy combatant" within the United States. Have there been any other people identified as an "enemy combatant" and detained with the United States, and if so, what has been done with these individuals?**

With respect, we cannot answer these questions without revealing the operational details of the Terrorist Surveillance Program, other than to point to the testimony of General Hayden and Director Mueller at the February 2d Worldwide Threat Briefing. Specifically, General Hayden stated that "the program has been successful; . . . we have learned information from this program that would not otherwise have been available" and that "[t]his information has helped detect and prevent terrorist attacks in the United States and abroad." Director Muller stated that "leads from that program have been valuable in identifying would-be terrorists in the United States, individuals who were providing material support to terrorists."

26. Senator Roberts has stated that the program is limited to: "when we know within a terrorist cell overseas that there is a plot and that plot is very close to its conclusion or that plot is very close to being waged against America – now, if a call comes in from an Al Qaeda cell and it is limited to that where we have reason to believe that they are planning an attack, to an American phone number, I don't think we're violating anybody's Fourth Amendment rights in terms of civil liberties."⁴

- **Is the program limited to such imminent threats against the United States, or where an attack is being planned? Is this an accurate description of the program?**

As the Attorney General has explained elsewhere, the Terrorist Surveillance Program is an early warning system aimed at detecting and preventing another

⁴ Senator Pat Roberts, CNN Late Edition with Wolf Blitzer, January 29, 2006

catastrophic al Qaeda terrorist attack. It targets communications only when one party to the communication is outside of the country and professional intelligence experts have reasonable grounds to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization.

Beyond that, it would be inappropriate to provide a more specific description of the Program, as the operational details remain classified and further disclosure would compromise the Program's effectiveness.

27. In a speech given in Buffalo, New York by the President, in April 2004, he said: "Now, by the way, any time you hear the United States government talking about wiretap, it requires – a wiretap requires a court order. Nothing has changed, by the way. When we're talking about chasing down terrorists, we're talking about getting a court order before we do so. It's important for our fellow citizens to understand, when you think Patriot Act, constitutional guarantees are in place when it comes to doing what is necessary to protect our homeland, because we value the Constitution."⁵

- **Is this statement accurate?**

We believe that the statement is accurate when placed in context. As the text of your question itself indicates, in his Buffalo speech, the President was talking about the USA PATRIOT Act, certain provisions of which amended FISA to change the standard for obtaining electronic surveillance orders. In the paragraphs surrounding the portion you quoted, the President reiterated three times that he is discussing the PATRIOT Act. In particular, the President was speaking about the roving wiretap provision of the USA PATRIOT Act, noting that while such wiretaps previously were not available under FISA to intercept the communications of suspected terrorists, "[t]he Patriot Act changed that." When surveillance is conducted under FISA, as amended by the PATRIOT Act, generally we are—as the President said—"talking about getting a court order." The President's statement cannot be taken out of context. In a wide variety of situations, we do not (and at times cannot) get court orders. For example, there is no provision by which the Executive Branch can obtain court orders to conduct certain surveillances overseas.

28. According to press reports, the Administration at some point determined that the authorities provided in the FISA were, in their view, inadequate to support the President's Commander-in-Chief responsibilities.

- **At what point was this determination reached?**
- **Who reached this determination?**

⁵ **Information sharing, Patriot Act Vital to Homeland Security, Remarks by the President in a Conversation on the USA Patriot Act, Kleinshans Music Hall, Buffalo, New York, April 20, 2004**

- **If such determination had been reached, why did the Administration conceal the view that existing law was inadequate from the Congress?**

FISA itself permits electronic surveillance authorized by statute, and, as explained above, the Force Resolution satisfies FISA and provides the authorization required for the Terrorist Surveillance Program.

The determination was made, based on the advice of intelligence experts, that we needed an early warning system, one that could help detect and prevent the next catastrophic al Qaeda attack and that might have prevented the attacks of September 11th, had it been in place. As the Department has explained elsewhere, including our paper of January 19, 2006, speed and agility are critical here and “existing law” is *not* inadequate. The Force Resolution, combined with the President’s authority under the Constitution, amply supports the Terrorist Surveillance Program. Because “existing law” provides ample authority for the Terrorist Surveillance Program, the Administration did not choose to seek additional statutory authority to support the Program, in part because, as discussed above, the consensus in discussions with congressional leaders was that pursuing such legislation would likely compromise the Program.

It would be inappropriate for us to reveal the confidential and privileged internal deliberations of the Executive Branch, including who made specific recommendations.

29. Based upon press reports, it does not appear that the NSA surveillance program at issue makes use of any intelligence sources and methods which have not been briefed (in a classified setting) to the Intelligence Committees. Other than the adoption of a legal theory which allows the NSA to undertake surveillance which on its face would be prohibited by law, what about this program is secret or sensitive?

- **Is there any precedent for developing a body of secret law such as has been revealed by last month’s *New York Times* article about the NSA surveillance program?**

As explained above, the Terrorist Surveillance Program is fully consistent with all applicable federal law, including FISA. Although the broad contours of the Terrorist Surveillance Program have been disclosed, details about the operation of the Terrorist Surveillance Program remain highly classified and exceptionally sensitive. Thus, we must continue to strive to protect the intelligence sources and methods of this vital program. It is important that we not damage national security through revelations of intelligence sources and methods during these proceedings or elsewhere.

The legal authorities for the Terrorist Surveillance Program do not constitute a “body of secret law,” as your question suggests. The Force Resolution and its broad authorizing language are public. Nor is it a secret that five Justices of the Supreme Court concluded in *Hamdi v. Rumsfeld* that the Force Resolution authorizes the use of the “fundamental incidents” of war. The breadth of the Force Resolution also has been the subject of prominent law review articles. *See, e.g.*, Curtis A. Bradley & Jack L.

Goldsmith, *Congressional Authorization and the War on Terrorism*, 118 Harv. L. Rev. 2048 (2005); Michael Stokes Paulsen, *Youngstown Goes to War*, 19 Const. Comment. 215, 252 (2002). It has long been public knowledge that other Presidents have concluded that their inherent powers under the Constitution, together with similarly broad authorizations of force, authorized the warrantless interception of international communications during armed conflicts. In short, all of the sources relied upon in the Department's January 19th paper to demonstrate that signals intelligence is a fundamental and accepted incident of the use of military force are readily available to the public.

30. At a public hearing of the Senate/House Joint Inquiry, then-NSA Director Hayden said: "My goal today is to provide you and the American people with as much insight as possible into three questions: (a) What did NSA know prior to September 11th, (b) what have we learned in retrospect, and (c) what have we done in response? I will be as candid as prudence and the law allow in this open session. If at times I seem indirect or incomplete, I hope that you and the public understand that I have discussed our operations fully and unreservedly in earlier closed sessions" (emphasis added).⁶

- **Under what, if any, legal authority did General Hayden make this inaccurate statement to the Congress (and to the public)?**

Although the Department cannot speak for General Hayden in this context, it does not appear that the statement was inaccurate. As discussed above, it has long been the practice of both Democratic and Republican administrations under the National Security Act of 1947 to limit full briefings of certain exceptionally sensitive matters to key members of the Intelligence Committees.

31. Were any collection efforts undertaken pursuant to this program based on information obtained by torture?

- **Was the possibility that information obtained by torture would be rejected by the FISA court as a basis for granting a FISA warrant a reason for undertaking this program?**

As the President has repeatedly made clear, the United States does not engage in torture and does not condone or encourage any acts of torture by anyone under any circumstances. In addition, we have already explained our reasons for establishing the

⁶ **Statement for the Record by Lieutenant General Michael V. Hayden, USAF, Director, National Security Agency/Chief, Central Security Service, Before the Joint Inquiry of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence, 17 October 2002, available at <http://intelligence.senate.gov/0210hrg/021017/hayden.pdf>.**

Terrorist Surveillance Program. It is an early warning system designed to detect and prevent another catastrophic terrorist attack on the United States.

32. If the President determined that a truthful answer to questions posed by the Congress to you, including the questions asked here, would hinder his ability to function as Commander-in-Chief, does the AUMF, or his inherent powers, authorize you to provide false or misleading answers to such questions?

Absolutely not. Congressional oversight is a healthy and necessary part of our democracy. This Administration would not under any circumstances countenance the provision of false or misleading answers to Congress. Under our system of government, no one—particularly not the Attorney General—is permitted to commit perjury. Nor is that something that the Force Resolution authorizes. We are not aware of any theory under which committing perjury before Congress is a fundamental and accepted incident of the use of force.

In those instances where the Administration believes that answering questions about certain intelligence operations would compromise national security, we would follow long-established principles of accommodation between the Branches, by, for example, informing the chairs and vice chairs of the Intelligence Committees, and the House and Senate leaders, as appropriate.

Subject: RE: staffing: 1/25 Statement at National Security Agency #2
From: "Kavanaugh, Brett M."
Date: 1/24/06, 1:36 PM
To: "Drouin, Lindsey E.", "Haenle, Paul T."
CC: "Staff Secretary", "DL-NSC-APNSA", "Michel, Christopher G.", "Thiessen, Marc A."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Wed Apr 03 15:40:17 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: staffing: 1/25 Statement at National Security Agency #2
From: "Haenle, Paul T."
Date: 1/24/06, 1:49 PM
To: "Kavanaugh, Brett M.", "Drouin, Lindsey E."
CC: "Staff Secretary", "DL-NSC-APNSA", "Michel, Christopher G.", "Thiessen, Marc A."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Wed Apr 03 16:57:47 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: staffing: 1/25 Statement at National Security Agency #2
From: "Drouin, Lindsey E."
Date: 1/24/06, 1:54 PM
To: "Haenle, Paul T.", "Kavanaugh, Brett M."
CC: "Staff Secretary", "DL-NSC-APNSA", "Michel, Christopher G.", "Thiessen, Marc A."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Wed Apr 03 16:57:48 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: staffing: 1/25 Statement at National Security Agency #2
From: "Kavanaugh, Brett M."
Date: 1/24/06, 2:00 PM
To: "Haenle, Paul T."
CC: "Drouin, Lindsey E."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Wed Apr 03 16:57:50 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: Re: POTUS Remarks -- DNI
From: [b3 50 USC 3024 (m)(1)]
Date: 1/24/06, 5:41 PM
To: "Carson, Melissa M."
CC: "Ward, Frank P.", "Merkley, Brendon A.", "Kavanaugh, Brett M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Wed Apr 03 16:57:52 EDT 2019

Releasability: Withheld In Part

Reasons for Withholding:

P3,b(3)

Notes:

50 USC 3024 (m)(1)

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: POTUS Remarks -- DNI
From: "Carson, Melissa M."
Date: 1/24/06, 5:50 PM
To: [b3 50 USC 3024 (m)(1)]
CC: "Ward, Frank P.", "Merkley, Brendon A.", "Kavanaugh, Brett M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Wed Apr 03 16:57:54 EDT 2019

Releasability: Withheld In Part

Reasons for Withholding:

P3,b(3)

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: can you email me draft 5 of NSA
From: "Drouin, Lindsey E."
Date: 1/24/06, 9:27 PM
To: "Kavanaugh, Brett M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Wed Apr 03 16:57:54 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P6,b(6),P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

From: "Kavanaugh, Brett M."

Date: 1/24/06, 9:28 PM

To: "Gerry, Brett C."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Wed Apr 03 16:57:55 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P6,b(6),P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: FW: Comments #5
From: "Drouin, Lindsey E."
Date: 1/24/06, 9:38 PM
To: "Kavanaugh, Brett M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Wed Apr 03 16:57:56 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P6,b(6),P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

FW: Draft Presidential remarks for your review.

Subject: FW: Draft Presidential remarks for your review.
From: "Sherzer, David"
Date: 1/24/06, 10:00 PM
To: "Kavanaugh, Brett M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Wed Apr 03 16:57:56 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P6,b(6),P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: FW: [Fwd: Final Version of the Speech]
From: "Gerry, Brett C."
Date: 1/24/06, 10:02 PM
To: "Kavanaugh, Brett M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Wed Apr 03 16:57:57 EDT 2019

Releasability: Withheld In Part

Reasons for Withholding:

P3,b(3)

Notes:

50 USC 3024 (m)(1)

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: FW: Draft Presidential remarks for your review.
From: "Kavanaugh, Brett M."
Date: 1/24/06, 10:33 PM
To: "Michel, Christopher G.", "Thiessen, Marc A."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Wed Apr 03 16:57:58 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P6,b(6),P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: FW: Draft Presidential remarks for your review.
From: "Gerry, Brett C."
Date: 1/24/06, 10:36 PM
To: "Kavanaugh, Brett M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Wed Apr 03 16:57:58 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P6,b(6),P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

From: "Gerry, Brett C."
To: "Kavanaugh, Brett M."
Subject: FW: [Fwd: Final Version of the Speech]
Received(Date): Tue, 24 Jan 2006 17:02:58 -0500
[NatIPressClub--23Jan--0915.doc](#)

This is the final, to my knowledge. Hayden quote is at top of p. 8.

From: b3 50 USC 3024 (m)(1)

Sent: Monday, January 23, 2006 9:26 AM

To: Bartlett, Dan; Kavanaugh, Brett M.; Miers, Harriet; Kelley, William K.; Addington, David S.; Bellinger, John B(Legal); Courtney.Elwood@usdoj.gov; Drummond, Michael; Perino, Dana M.; Rachel.Brand@usdoj.gov; Roebke, Heather M.; Wanda.Martinson@usdoj.gov; Allen, Michael; Coffin, Shannen W.; Gerry, Brett C.; Kyle.Sampson@usdoj.gov; Larry Pfeiffer; McClellan, Scott; McDonald, Matthew T.; Steve.Bradbury@usdoj.gov; West, Christal R.; Wolff, Candida P.

Subject: [Fwd: Final Version of the Speech]

final version prepared for delivery.

----- Original Message -----

Subject: Final Version of the Speech

Date: Mon, 23 Jan 2006 09:16:26 -0500

b3 50 USC 3024 (m)(1)

Principal Deputy Director of National Intelligence
Address to the National Press Club
23 January 2006

Good morning. I'm happy to be here to talk a bit about what American intelligence and especially NSA have been doing to defend the Nation.

I'm here today not only as Ambassador Negroponte's deputy in the Office of the Director of National Intelligence. I'm also here as the former Director of the National Security Agency, a post I took in March of 1999 and left only last spring.

Serious issues have been raised in recent weeks. And discussion of serious issues should be based on facts. There is a lot of information out there—some of it is frankly inaccurate, much of it is simply misunderstood. I'm here to tell the American people what NSA has been doing and why. And, perhaps more importantly, what it has not been doing.

Admittedly, this is a little hard to do while protecting our country's intelligence sources and methods. And people in my line of work generally don't like to talk about what they've done until it's a subject on the History Channel.

But let me make one thing very clear: as challenging as this might be, this is the speech I want to give. I much prefer being here with you today telling you about the things we have done when there hasn't been an attack on the US Homeland.

This is a far easier presentation to make than the ones I had to give four years ago—telling audiences like you *what we hadn't done* in the days and months leading up to the tragic events of September 11th. Today's story is not an easy one to tell in this kind of unclassified environment, but it is by far the brief I prefer to present.

We all have searing memories of the morning of September 11th. I know I do: making a decision to evacuate non-essential workers at NSA while the situation was still unclear; seeing the NSA counter terrorist shop in tears while black out curtains were being stapled to walls around their windows; like many of you, asking my wife to find our kids and then hanging up the phone on her.

Another memory comes from two days later when I addressed the NSA workforce to lay out our mission in a new environment. It was a short video talk beamed throughout our headquarters at Fort Meade and globally. Most of what I said was what anyone would expect. I tried to inspire. Our work was important and the Nation was relying on us. I tried to comfort. Look on the bright side I said to them: right now a quarter billion Americans wished they had your job...being able to go after the enemy. I ended the talk by trying to give perspective. I noted that all free peoples have had to balance the demands of liberty with the demands of security. Historically we Americans had planted our

flag well down the spectrum toward liberty. Here was our challenge. “We were going to keep America free,” I said, “by making Americans feel safe again.”

But to start the story with that Thursday, September 13th is misleading, because it is really near the end of the first reel of this movie. To understand that moment and that statement, you would have to know a little bit about what had happened to the National Security Agency in the preceding years.

NSA intercepts communications and it does so for only one purpose: to protect the lives, the liberties and the well being of the citizens of the United States from those who would do us harm. By the late 1990s, that job was becoming increasingly more difficult. The explosion of modern communications in terms of volume, variety and velocity threatened to overwhelm us.

The Agency took a lot of criticism in those days—that it was going deaf; that it was ossified in its thinking; that it had not and could not keep up with the changes in modern communications. All that was only reinforced when all the computer systems at Fort Meade went dark for three days in January of 2000 and we couldn’t quickly or easily explain why.

Those were interesting times. As we were being criticized for being incompetent and going deaf, others seemed to be claiming that we were omniscient and reading your e-mails.

The Washington Post and New Yorker Magazine during that time incorrectly wrote that, “NSA has turned from eavesdropping on the Communists to eavesdropping on businesses and private citizens,” and that, “NSA has the ability to extend its eavesdropping network without limits.” We were also referred to as “a global spying network that can eavesdrop on every single phone call, fax, or e-mail, anywhere on the planet.”

I used those quotes in a speech I gave at American University in February 2000. The great “urban legend” then was something called Echelon and the false accusation that NSA was using its capabilities to advance American corporate interests: signals intelligence for General Motors or something like that. With these kinds of charges, the turf back then feels familiar now: how could we prove a negative (that we weren’t doing certain things) without revealing the appropriate things we were doing that kept America safe.

You see, NSA had (and has) an existential problem. In order to protect American lives and liberties it has to be two things: powerful in its capabilities and secretive in its methods. And we exist in a political culture that distrusts two things most of all: power and secrecy.

Modern communications didn’t make this any easier. Gone were the days when “signals of interest” went along a dedicated microwave link between strategic rocket forces headquarters in Moscow to an ICBM base in western

Siberia. By the late nineties, what NSA calls “targeted communications”—things like al Qaeda communications—co-existed out there in a great global web with your phone calls and my e-mails. NSA needed the power to pick out the one and the discipline to leave the others alone.

So this question of security and liberty wasn’t a new one for us in September 2001. We always have had this question: how do we balance the legitimate need for foreign intelligence with our responsibility to protect individual privacy rights? It is a question drilled into every employee of NSA from day one, and it shapes every decision about how NSA operates.

September 11th didn’t change that. But it did change some things.

This ability to intercept communications, commonly referred to as Signals Intelligence (SIGINT), is a complex business with operational, technological and legal imperatives often intersecting and overlapping. There is routinely some freedom of action—within the law—to adjust operations. After the attacks I exercised some options I always had that collectively better prepared us to defend the Homeland.

Let me talk about this for a minute. Because a big gap in understanding is what’s standard—what does NSA do routinely?

Where we set the threshold for what constituted “inherent foreign intelligence value” in reports involving a US person, for example, shapes the level of some of our collection and reporting. The American SIGINT system in the normal course of its foreign intelligence activities inevitably captures this kind of information—information to, from or about what we call a US person (by the way, that routinely includes anyone in the United States, citizen or not.) So, for example, because they were in the United States Mohammad Atta and his fellow 18 hijackers were presumed to be protected persons.

“Inherent foreign intelligence value” is one of the metrics we must use to ensure that we conform to the 4th Amendment’s “reasonableness” standard when it comes to protecting the privacy of that person. If the US person information isn’t relevant, the data is suppressed or what we call minimized. The individual is not mentioned, or if he is, he is referred to as US person number one. If the US person is actually the named terrorist, well, that could be a different matter.

The standard by which we decided that—the standard of what was relevant and valuable, and therefore what was reasonable—would understandably change as smoke billowed from two American cities and a Pennsylvania farm field, and we acted accordingly. To somewhat oversimplify the question of inherent intelligence value—to just use an example—we had a different view of Zacarias Moussaoui’s computer hard drive after the attacks than we had before.

This is not unlike what happened in other areas. Prior to September 11th airline passengers were screened in one way. After September 11th, we changed how we screened passengers. Similarly, although prior to September 11th certain communications weren't considered valuable intelligence, it became immediately clear after September 11 that intercepting and reporting these same communications were, in fact, critical to defending the homeland.

These decisions were easily within my authorities as Director of NSA under an executive order, known as Executive Order 12333, that was signed in 1981—an Executive Order that has governed NSA for nearly a quarter century.

Let me summarize: in the days after 9-11, NSA was using its authorities and its judgment to appropriately respond to the most catastrophic attack on the Homeland in the history of the Nation.

That shouldn't be a headline, but as near as I can tell, these actions on my part have created some of the noise in recent press coverage. Let me be clear on this point--except that they involved NSA, these programs were not related to the authorization that the President has recently talked about. I asked to update the Congress on what NSA had been doing and I briefed the entire House Intelligence Committee on the 1st of October 2001 on what we had done under NSA's previously existing authorities.

As part of our adjustments, we also turned on the spigot of NSA reporting to FBI in an unprecedented way. We found that we were giving them too much data in too raw a form. We recognized it almost immediately—a question of weeks—and made adjustments.

This flow of data to the FBI has also become part of the current background noise. Despite reports in the press of “thousands of tips a month,” our reporting has not even approached that kind of pace.

I actually find all of this a little odd. After all the findings of the 9-11 Commission and other bodies about the failure to *share* intelligence, I'm up here feeling like I have to explain pushing data to those who might be able to use it.

And it is the nature of intelligence that many tips lead nowhere but you have to go down some blind alleys to find the tips that pay off.

Beyond the authorities that I exercised under the standing executive order, as the war on terror has moved forward we have aggressively used FISA warrants. The Act and the Court have provided us with important tools and we make full use of them. Published numbers show us using the Court at record rates and the results have been outstanding.

But the revolution in telecommunications technology has extended the actual impact of the FISA regime far beyond what Congress could ever have

anticipated in 1978. And I don't think that anyone could make the claim that the FISA statute is optimized to deal with a 9/11 or to deal with a lethal enemy who likely already had combatants inside the United States.

I testified in open session to the House Intelligence Committee in April of the year 2000. At the time I created some looks of disbelief when I said that if Usama bin Ladin crossed the bridge from Niagara Falls, Ontario to Niagara Falls, New York, there were provisions of US law that would kick in, offer him protections and affect how NSA could now cover him. At the time I was just using this as a stark hypothetical. Seventeen months later this was about life and death.

So we now come to one additional piece of NSA's authorities: these are the activities whose existence the President confirmed several weeks ago. The authorization was based on an intelligence community assessment of a serious and continuing threat to the homeland. The lawfulness of the actual authorization was reviewed by lawyers at the Department of Justice and the White House and was approved by the Attorney General.

There is a certain sense of sufficiency here: authorized by the President, duly ordered, its lawfulness attested to by the Attorney General, and its content briefed to the Congressional leadership.

But we all have a personal responsibility. And in the end, NSA would have to implement this--and every operational decision the Agency makes is made with the full involvement of its legal office.

NSA professional career lawyers—and the Agency has a lot of them—have a well-deserved reputation. They're good. They know the law. And they don't let the Agency take many close pitches.

And so, even though I knew that program had been reviewed by the White House and the Department of Justice, I asked the three most senior and experienced lawyers in NSA. Our enemy in the global war on terrorism doesn't divide the United States from the rest of the world. The global telecommunications system doesn't make that distinction either. Our laws do—and should. How did these activities square with these facts? They reported back that they supported the lawfulness of the program—supported, not acquiesced. This was very important to me.

A veteran NSA lawyer, now retired, told me that a correspondent had suggested to him recently that all of the lawyers connected with this program had been very careful from the outset because they knew there would be a "day of reckoning." The NSA lawyer replied that that had not been the case. NSA had been so careful, he said—and I'm using his words here--because in this very focused, limited program NSA had to ensure that it dealt with privacy interests in an appropriate manner.

In other words, our lawyers weren't careful out of fear. They were careful out of a heartfelt and principled view that NSA operations had to be consistent with bedrock legal protections.

In early October 2001 I gathered key members of the NSA work force in our conference room and introduced our new operational authorities to them. With the historic culture at NSA being what it was (and is), I had to do this personally. I told them what we were going to do and why. I also told them that we were going to carry out the program and not go one step further. NSA's legal and operational leadership then went into the details of our new task.

The 9-11 Commission criticized our ability to link things happening in the United States with things that were happening elsewhere. In that light, there are no communications more important to the safety of the Homeland than those affiliated with al Qa'ida with one end in the United States. The President's authorization allows us to track this kind of call more comprehensively and more efficiently.

The trigger is quicker and a bit softer than it is for a FISA warrant but the intrusion into privacy is also limited—only international calls and only those we have a reasonable basis to believe involve al Qa'ida or one of its affiliates. The purpose of all of this is not to collect reams of intelligence but to detect and prevent attacks.

The Intelligence Community has neither the time, the resources, nor the legal authority to read communications that aren't likely to protect us, and NSA has no interest in doing so.

These are communications that we have reason to believe are al Qa'ida communications, a judgment made by the American intelligence professionals (not political appointees) most trained to understand al Qa'ida tactics, communications and aims.

Their work is actively overseen by the most intense oversight regime in the history of the National Security Agency. The Agency's conduct of the program is thoroughly reviewed by the NSA's General Counsel and Inspector General. The program has also been reviewed by the Department of Justice for compliance with the President's authorization.

Oversight also includes an aggressive training program to ensure that all activities are consistent with the letter and intent of the authorization and with the preservation of civil liberties.

Let me also talk for a minute about what this program is not. It is not a driftnet over Dearborn or Lackawanna or Fremont grabbing conversations that

we then sort out by these alleged keyword searches or data mining tools or other devices that so-called experts keep talking about. This is targeted and focused.

This is not about intercepting conversations between people in the United States. This is hot pursuit of communications entering or leaving the United States involving someone we believe is associated with al Qa'ida.

We bring to bear all the technology we can to ensure that this is so. And if there were an anomaly and we discovered there had been an inadvertent intercept of a domestic-to-domestic call, that intercept would be destroyed and not reported but the incident—the inadvertent collection—would be recorded and reported. But that's a normal NSA procedure—for at least a quarter century.

And, as we always do when dealing with US person information, US identities are expunged when they are not essential to understanding the intelligence value of reports. Again, that's a normal NSA procedure.

So let me make this clear. When you are talking to your daughter away at State college, this program *cannot* intercept your conversations. And when she takes a semester abroad to complete her Arabic studies, this program *will* not intercept your conversations.

Let me emphasize one more thing that this program is not. Look, I know how hard it is to write a headline that is accurate, short and grabbing. But we should really shoot for all three attributes.

“Domestic Spying” doesn't really make it. One end of any call targeted under this program is always outside the United States. I have flown a lot in this country and I've taken hundreds of domestic flights. I have never boarded a domestic flight in this country and landed in Waziristan.

In the same way—and I am speaking illustratively here—if NSA had intercepted al Qa'ida ops chief Khalid Sheik Mohammed in Karachi talking to Mohammed Atta in Laurel, Maryland in say July of 2001...if NSA had done that and the results had been made public, I'm convinced that the crawler on all the 7/24 news networks would not have been: NSA domestic spying!

Had this program been in effect prior to 9-11, it is my professional judgment that we would have detected some of the 9-11 al Qa'ida operatives in the United States, and we would have identified them as such.

I've said earlier that this program has been successful. Clearly not every lead pans out, from this or any other source, but this program has given us information that we would not otherwise have been able to get. It's impossible for me to talk about this more in any public way without alerting our enemies to our tactics or what we have learned. I can't give details without increasing the danger to Americans. On one level I wish that I could, but I can't.

Our enemy has made his intentions clear. He has declared war on us. Since September 11th al Qa'ida and its affiliates have continued to announce their intention and continue to act on their clearly stated goal of attacking America. They have succeeded against our friends in London, Madrid, Bali, Amman, Istanbul and elsewhere. They desperately want to succeed against us.

The 9-11 Commission told us that “Bin Laden and Islamist terrorists mean exactly what they say: to them America is the font of all evil, the ‘head of the snake’, and it must be converted or destroyed.” Bin Laden reminded us of this intention as recently as last Thursday.

The people at NSA, and the rest of the Intelligence Community, are committed to defend us against this evil and to do it in a way consistent with our values.

[We know that we can only do our jobs if we have the trust of the American people. And we can only have your trust if we are careful about how we use our tools and resources. That sense of care is part of the fabric of the intelligence community—it helps defines who we are.]

I recently went out to Fort Meade to talk to the work force involved in this program. They know what they have contributed and they know the care with which it has been done. Even in today's heated environment, the only concern expressed to me was continuing their work in the defense of the nation, and doing so in a manner that honors the law and the Constitution.

As I was talking with them I looked out over their heads to see a large sign fixed to one of the pillars that breaks up their office space. The sign is visible from almost all of the work area. It's yellow with bold black letters. The title is readable from 50 feet: “What Constitutes a US Person.” And that is followed by an explanation of the criteria.

That has always been the fundamental tenet of privacy for NSA. And here it was, in the center of a room, guiding the actions of a workforce determined to prevent another attack on the United States.

Security and liberty. The people at NSA know what their job is.

I know what my job is, too. I learned a lot from NSA and its culture during my time there. But I come from a culture, too. I have been a military officer for nearly 37 years and from the start I have taken an oath to protect and defend the Constitution of the United States. I would never violate that Constitution nor would I abuse the rights of the American people. As Director I was the one responsible to ensure that this program was limited in its scope and disciplined in its application.

American intelligence and especially American SIGINT is the front line of defense in dramatically changed circumstances, circumstances in which—if we fail to do our job well and completely—more Americans will almost certainly die. The speed of operations, the ruthlessness of our enemy, the pace of modern communications has called on us to do things and do them in ways never before required. We have worked hard to find innovative ways to protect the American people and the liberties we hold dear. And in doing so we have not forgotten who we are.

Subject: NSA statement post-staffing draft #7 (this still could change some)

From: "Kavanaugh, Brett M."

Date: 1/25/06, 12:15 AM

To: "McClellan, Scott", "Hervey, Tina"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 16:51:05 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P6,b(6),P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: NSA statement post-staffing draft #7 (this still could change some)
From: "McClellan, Scott"
Date: 1/25/06, 12:19 AM
To: "Kavanaugh, Brett M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 16:51:05 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P6,b(6),P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: NSA statement post-staffing draft #7 (this still could change some)
From: "Kavanaugh, Brett M."
Date: 1/25/06, 12:21 AM
To: "McClellan, Scott"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 16:51:06 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P6,b(6),P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: FW: Draft 7 of President's Statement at the NSA sent to DNI for final review/concurrence

From: "Sherzer, David"

Date: 1/25/06, 12:24 AM

To: "Kavanaugh, Brett M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 16:51:07 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P6,b(6),P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: NSA statement post-staffing draft #7 for final review (General Hayden is also reviewing) -- Please provide any comments by 8:00 a.m.

From: "Gerry, Brett C."

Date: 1/25/06, 12:34 AM

To: "Kavanaugh, Brett M."

CC: "Miers, Harriet", "Kelley, William K.", "Addington, David S.", "Coffin, Shannen W."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 16:51:07 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P6,b(6),P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: NSA statement post-staffing draft #7 for final review (General Hayden is also reviewing) -- Please provide any comments by 8:00 a.m.

From: "Kavanaugh, Brett M."

Date: 1/25/06, 12:37 AM

To: "Gerry, Brett C."

CC: "Miers, Harriet", "Kelley, William K.", "Addington, David S.", "Coffin, Shannen W."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 16:51:08 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P6,b(6),P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: Re: NSA statement post-staffing draft #7 for final review (General Hayden is also reviewing) -- Please provide any comments by 8:00 a.m.

From: <Kyle.Sampson@usdoj.gov>

Date: 1/25/06, 2:40 AM

To: "Kavanaugh, Brett M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 16:51:09 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P6,b(6),P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: NSA draft #9 (current updated draft)

From: "Kavanaugh, Brett M."

Date: 1/25/06, 4:51 PM

To: "Weinstein, Jared B.", "West, Christal R.", "Haenle, Paul T.", "Hervey, Tina", "Roebke, Heather M.", "McClellan, Scott", "Miers, Harriet"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 16:51:10 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P6,b(6),P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: FW: NSA draft #9 (current updated draft)
From: "Kavanaugh, Brett M."
Date: 1/25/06, 4:52 PM
To: "Sherzer, David"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 16:51:11 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P6,b(6),P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: FW: NSA draft #9 (current updated draft)
From: "Kavanaugh, Brett M."
Date: 1/25/06, 4:54 PM
To: "Slick, Stephen B."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 16:51:12 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P6,b(6),P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: FW: NSA draft #9 (current updated draft)
From: "Kavanaugh, Brett M."
Date: 1/25/06, 4:55 PM
To: "Gerry, Brett C."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 16:51:13 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P6,b(6),P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

harriet's office is still reviewing...

Subject: harriet's office is still reviewing...
From: "Bartlett, Dan"
Date: 1/26/06, 12:59 AM
To: "Kavanaugh, Brett M.", "McClellan, Scott"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 16:51:14 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: final with harriet's approval
From: "Bartlett, Dan"
Date: 1/26/06, 1:17 AM
To: "Kavanaugh, Brett M."
CC: "McClellan, Scott", "Wallace, Nicolle"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 16:51:14 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: Q & A formatted
From: "Kavanaugh, Brett M."
Date: 1/26/06, 1:33 AM
To: "Bartlett, Dan"
CC: "McClellan, Scott", "Wallace, Nicolle"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 16:51:15 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

from Dan for Chief in morning

Subject: from Dan for Chief in morning
From: "Kavanaugh, Brett M."
Date: 1/26/06, 2:06 AM
To: "Weinstein, Jared B.", "West, Christal R."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 16:51:16 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: Annotated Remarks

From: "Carson, Melissa M."

Date: 1/26/06, 2:08 AM

To: "Kavanaugh, Brett M."

CC: "Thiessen, Marc A.", "Michel, Christopher G.", "Drouin, Lindsey E.", "Ward, Frank P.", "Merkley, Brendon A.", "Green, Anneke E."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 16:51:17 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P6,b(6),P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: Fw: final with harriet's approval
From: "Kavanaugh, Brett M."
Date: 1/26/06, 3:38 AM
To: "Miers, Harriet"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 17:22:29 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: Fw: Newsweek – Palace Revolt
From: "Gottesman, Blake"
Date: 1/29/06, 10:41 AM
To: "Kavanaugh, Brett M."

-----Original Message-----

From: White House News Update <News.Update@WhiteHouse.Gov>
To: Gottesman, Blake <Blake_Gottesman@who.eop.gov>
Sent: Sun Jan 29 09:00:57 2006
Subject: Newsweek – Palace Revolt

Palace Revolt

They were loyal conservatives, and Bush appointees. They fought a quiet battle to rein in the president's power in the war on terror. And they paid a price for it. A NEWSWEEK investigation.

By Daniel Klaidman, Stuart Taylor Jr. and Evan Thomas, Newsweek

Feb. 6, 2006 issue – James Comey, a lanky, 6-foot-8 former prosecutor who looks a little like Jimmy Stewart, resigned as deputy attorney general in the summer of 2005. The press and public hardly noticed. Comey's farewell speech, delivered in the Great Hall of the Justice Department, contained all the predictable, if heartfelt, appreciations. But mixed in among the platitudes was an unusual passage. Comey thanked "people who came to my office, or my home, or called my cell phone late at night, to quietly tell me when I was about to make a mistake; they were the people committed to getting it right—and to doing the right thing—whatever the price. These people," said Comey, "know who they are. Some of them did pay a price for their commitment to right, but they wouldn't have it any other way."

One of those people—a former assistant attorney general named Jack Goldsmith—was absent from the festivities and did not, for many months, hear Comey's grateful praise. In the summer of 2004, Goldsmith, 43, had left his post in George W. Bush's Washington to become a professor at Harvard Law School. Stocky, rumpled, genial, though possessing an enormous intellect, Goldsmith is known for his lack of pretense; he rarely talks about his time in government. In liberal Cambridge, Mass., he was at first snubbed in the community and mocked as an atrocity-abetting war criminal by his more knee-jerk colleagues. ICY WELCOME FOR NEW LAW PROF, headlined The Harvard Crimson.

They had no idea. Goldsmith was actually the opposite of what his detractors imagined. For nine months, from October 2003 to June 2004, he had been the central figure in a secret but intense rebellion of a small coterie of Bush administration lawyers. Their insurrection, described to NEWSWEEK by current and former administration officials who did not wish to be identified discussing confidential deliberations, is one of the most significant and intriguing untold stories of the war on terror.

These Justice Department lawyers, backed by their intrepid boss Comey, had stood up to the hard-liners, centered in the office of the vice president, who wanted to give the president virtually unlimited powers in the war on terror. Demanding that the White House stop using what they saw as farfetched rationales for riding rough-shod over the law and the Constitution, Goldsmith and the others fought to bring government spying and interrogation methods within the law. They did so at their peril; ostracized, some were denied promotions, while others left for more comfortable climes in private law firms and academia. Some went so far as to line up private lawyers in 2004, anticipating that the president's eavesdropping program would draw scrutiny from Congress, if not prosecutors. These government attorneys did not always succeed, but their efforts went a long way toward vindicating the principle of a nation of laws and not men.

The rebels were not whistle-blowers in the traditional sense. They did not want—indeed avoided—publicity. (Goldsmith confirmed public facts about himself but otherwise declined to comment. Comey also declined to comment.) They were not downtrodden career civil servants. Rather, they were conservative political appointees who had been friends and close colleagues of some of the true believers they were fighting against. They did not see the struggle in terms of black and white but in shades of gray—as painfully close calls with unavoidable

pitfalls. They worried deeply about whether their principles might put Americans at home and abroad at risk. Their story has been obscured behind legalisms and the veil of secrecy over the White House. But it is a quietly dramatic profile in courage. (For its part the White House denies any internal strife. "The proposition of internal division in our fight against terrorism isn't based in fact," says Lea Anne McBride, a spokeswoman for Vice President Dick Cheney. "This administration is united in its commitment to protect Americans, defeat terrorism and grow democracy.")

The chief opponent of the rebels, though by no means the only one, was an equally obscure, but immensely powerful, lawyer-bureaucrat. Intense, workaholic (even by insane White House standards), David Addington, formerly counsel, now chief of staff to the vice president, is a righteous, ascetic public servant. According to those who know him, he does not care about fame, riches or the trappings of power. He takes the Metro to work, rather than use his White House parking pass, and refuses to even have his picture taken by the press. His habitual lunch is a bowl of gazpacho, eaten in the White House Mess. He is hardly anonymous inside the government, however. Presidential appointees quail before his volcanic temper, backed by assiduous preparation and acid sarcasm.

Addington, 49, has worked as an adviser to Dick Cheney off and on since Cheney was a member and Addington a staffer on the House Intelligence Committee in the mid-'80s. When Cheney became secretary of Defense in the Bush 41 administration, Addington served at the Pentagon as general counsel. When Cheney became vice president to Bush 43, he brought Addington into the White House as his lawyer. Counsel to the vice president is, in most administrations, worth less than the proverbial bucket of warm spit, but under Prime Minister Cheney, it became a vital power center, especially after 9/11.

Like his boss, Addington has long believed that the executive branch was pitifully weakened by the backlash from Vietnam and the Watergate scandal. Fearful of investigative reporters and congressional subpoenas, soldiers and spies had become timid—"risk averse" in bureaucratic jargon. To Addington and Cheney, the 9/11 attacks—and the threat of more and worse to come—were perfect justification for unleashing the CIA and other long-blunted weapons in the national-security arsenal. Secretary of Defense Donald Rumsfeld, who disdains lawyers, was ready to go. So, too, was CIA Director George Tenet—but only if his spooks had legal cover, so they wouldn't be left holding the bag if things went wrong.

Addington and a small band of like-minded lawyers set about providing that cover—a legal argument that the power of the president in time of war was virtually untrammelled. One of Addington's first jobs had been to draft a presidential order establishing military commissions to try unlawful combatants—terrorists caught on the global battlefield. The normal "interagency process"—getting agreement from lawyers at Defense, State, the intelligence agencies and so forth—proved glacial, as usual. So Addington, working with fellow conservative Deputy White House Counsel Timothy Flanigan, came up with a solution: cut virtually everyone else out. Addington is a purist, not a cynic; he does not believe he is in any way ignoring or twisting the law. It is also important to note that Addington was not sailing off on some personal crusade; he had the full backing of the president and vice president, who shared his views. But, steeped in bureaucratic experience and clear in his purpose, Addington was a ferocious infighter for his cause. (Addington declined to comment. But McBride, the vice president's spokeswoman, said, "David Addington has a long, distinguished record of public service. He's committed to the president's agenda.")

Inexperienced in national-security law, White House Counsel Alberto Gonzales was steered by more-expert lawyers like Addington and Flanigan. Others, like John Bellinger, the National Security Council's top lawyer, were simply not told what was going on. Addington and the hard-liners had particular disregard for Bellinger, who was considered a softie—mocked by Addington because he had lunch once a month or so with a pillar of the liberal-leaning legal establishment, the late Lloyd Cutler. When Addington and Flanigan produced a document—signed by Bush—that gave the president near-total authority over the prosecution of suspected terrorists, Bellinger burst into Gonzales's office, clearly upset, according to a source familiar with the episode. But it was too late.

Addington was just getting started. Minimizing dissent by going behind the backs of bureaucratic rivals was how he played the game. A potentially formidable obstacle, however, was the Justice Department's Office of Legal Counsel. The OLC is the most important government office you've never heard of. Among its bosses—before they went on the Supreme Court—were William Rehnquist and Antonin Scalia. Within the executive branch, including the Pentagon and CIA, the OLC acts as a kind of mini Supreme Court. Its carefully worded opinions are regarded as binding precedent—final say on what the president and all his agencies can and cannot legally do.

Addington found an ally in an OLC lawyer whose name—John Yoo—would later become synonymous with the notion that power is for the president to use as he sees fit in a time of war. Shortly after 9/11, Yoo wrote, in a formal OLC opinion, that Congress may not "place any limits on the President's determinations as to any terrorist threat, the amount of military force to be used in response, or the method, timing, and nature of the response."

The brainy, pleasant and supremely self-confident Yoo became Addington's main man at Justice, a prolific author of legal opinions granting the president maximum power during wartime. In the winter of 2002, the CIA began catching top Qaeda terrorists—so-called High Value Targets—like Abu Zubaydah. These hard-case jihadists proved resistant to normal methods of interrogation. In the fevered atmosphere of the time, the Bush administration feared a "second wave" attack from Qaeda sleeper cells still inside the United States. The CIA wanted legal permission to use "coercive methods."

An August 2002 OLC memo, signed by the then head of the OLC—Jay Bybee—but drafted by Yoo, gave the agency what it needed. The controversial document, which became famous as the "torture memo" when it leaked two years later, defined torture so narrowly that, short of maiming or killing a prisoner, interrogators had a free hand. What's more, the memo claimed license for the president to order methods that would be torture by anyone's definition—and to do it wholesale, and not just in specific cases. A very similar Yoo memo in March 2003 was even more expansive, authorizing military interrogators questioning terror suspects to ignore many criminal statutes—as well as the strict interrogation rules traditionally used by the military. Secretary of Defense Rumsfeld put some limits on interrogation techniques, and they were intended to be used only on true terror suspects. Perhaps inevitably, however, "coercive interrogation methods" spread from Guantanamo Bay, which housed terror suspects, into prisons like Abu Ghraib, where detainees could be almost anyone. (Poor leadership in the chain of command and on the ground was partly to blame, as well as loose or fuzzy legal rules.) The result: those grotesque images of Iraqis being humiliated by poorly trained and sadistic American prison guards, not to mention prisoners who have been brutalized and in some cases killed by interrogators in Afghanistan and elsewhere.

In the summer of 2003, Yoo, who stands by his body of work, left the Justice Department and returned to teaching law. His departure came in the midst of a critical power struggle. Addington and Gonzales had both wanted to make Yoo head of the OLC when Bybee went off to take a federal judgeship in March 2003, but Attorney General John Ashcroft balked. Ashcroft's reasons were apparently bureaucratic. (He declined to speak for this story.) According to colleagues, he resented Yoo's going behind his back to give the White House a private pipeline into the OLC. Yoo denied circumventing Ashcroft. "OLC kept the attorney general or his staff fully informed of all of its work in the war on terrorism," he said.

Jack Goldsmith, a law professor who was working in the general counsel's office at the Pentagon, was the eventual compromise choice to head the OLC. Goldsmith seemed like a natural fit. He was brilliant, a graduate of Oxford and Yale Law School, and he was conservative. Like Yoo, he was tagged a "New Sovereignist" for his scholarly argument that international laws including prohibitions on human-rights abuses should not be treated as binding law by the U.S. courts.

But somehow, in the vetting of Goldsmith, one of his important views was overlooked. Goldsmith is no executive-power absolutist. What's more, his friends say, he did not intend to be a patsy for Addington and the hard-liners around Cheney. Goldsmith was not the first administration lawyer to push back against Addington & Co. At the CIA, general counsel Scott Muller had caused a stir by ruling that CIA agents could not join with the military in the interrogation of Iraqi prisoners. But Goldsmith became a rallying point for Justice Department lawyers who had legal qualms about the administration's stance.

Goldsmith soon served notice of his independence. Shortly after taking over the OLC in October 2003, he took the position that the so-called Fourth Geneva Convention—which bars the use of physical or moral coercion on prisoners held in a militarily occupied country—applied to all Iraqis, even if they were suspected of belonging to Al Qaeda.

Addington soon suffered pangs of buyer's remorse over Goldsmith. There was no way to simply ignore the new head of the OLC. Over time, Addington's heartburn grew much worse. In December, Goldsmith informed the Defense Department that Yoo's March 2003 torture memo was "under review" and could no longer be relied upon. It is almost unheard-of for an administration to overturn its own OLC opinions. Addington was beside himself. Later, in frequent face-to-face confrontations, he attacked Goldsmith for changing the rules in the middle of the game and putting brave men at risk, according to three former government officials, who declined to speak on the record given the sensitivity of the subject.

Addington's problems with Goldsmith were just beginning. In the jittery aftermath of 9/11, the Bush

administration had pushed the top-secret National Security Agency to do a better and more expansive job of electronically eavesdropping on Al Qaeda's global communications. Under existing law—the Foreign Intelligence Surveillance Act, or FISA, adopted in 1978 as a post-Watergate reform—the NSA needed (in the opinion of most legal experts) to get a warrant to eavesdrop on communications coming into or going out of the United States. Reasoning that there was no time to obtain warrants from a secret court set up under FISA (a sometimes cumbersome process), the Bush administration justified going around the law by invoking a post-9/11 congressional resolution authorizing use of force against global terror. The eavesdropping program was very closely held, with cryptic briefings for only a few congressional leaders. Once again, Addington and his allies made sure that possible dissenters were cut out of the loop.

There was one catch: the secret program had to be reapproved by the attorney general every 45 days. It was Goldsmith's job to advise the A.G. on the legality of the program. In March 2004, John Ashcroft was in the hospital with a serious pancreatic condition. At Justice, Comey, Ashcroft's No. 2, was acting as attorney general. The grandson of an Irish cop and a former U.S. attorney from Manhattan, Comey, 45, is a straight arrow. (It was Comey who appointed his friend—the equally straitlaced and dogged Patrick Fitzgerald—to be the special prosecutor in the Valerie Plame leak-investigation case.) Goldsmith raised with Comey serious questions about the secret eavesdropping program, according to two sources familiar with the episode. He was joined by a former OLC lawyer, Patrick Philbin, who had become national-security aide to the deputy attorney general. Comey backed them up. The White House was told: no reauthorization.

The angry reaction bubbled up all the way to the Oval Office. President Bush, with his penchant for put-down nicknames, had begun referring to Comey as "Cuomey" or "Cuomo," apparently after former New York governor Mario Cuomo, who was notorious for his Hamlet-like indecision over whether to seek the Democratic presidential nomination in the 1980s. A high-level delegation—White House Counsel Gonzales and chief of staff Andy Card—visited Ashcroft in the hospital to appeal Comey's refusal. In pain and on medication, Ashcroft stood by his No. 2.

A compromise was finally worked out. The NSA was not compelled to go to the secret FISA court to get warrants, but Justice imposed tougher legal standards before permitting eavesdropping on communications into the United States. It was a victory for the Justice lawyers, and it drove Addington to new levels of vexation with Goldsmith.

Addington is a hard man to cross. Flanigan, his former White House colleague, described his M.O.: "David could go from zero to 150 very quickly. I'm not sure how much is temper and how much is for effect. At a meeting with government bureaucrats he might start out very calm. Then he would start with the sarcasm. He could say, 'We could do that, but that would give away all of the president's power.' All of a sudden here comes David Addington out of his chair. I'd think to myself we're not just dancing a minuet, there's a little slam dancing going on here." But Addington "usually had the facts, the law and the precedents on his side," says Flanigan. He had another huge advantage. He never needed to invoke Cheney's name, but everyone knew that he spoke for the vice president.

Addington was particularly biting with Goldsmith. During a long struggle over the legality of the August 2002 torture memo, Addington confronted Goldsmith, according to two sources who had heard accounts of the conversation: "Now that you've withdrawn legal opinions that the president of the United States has been relying on, I need you to go through all of OLC's opinions [relating to the war on terror] and let me know which ones you still stand by," Addington said.

Addington was taking a clever dig at Goldsmith—in effect, accusing him of undermining the entire edifice of OLC opinions. But he was not making a rhetorical point. Addington began keeping track of opinions in which he believed Goldsmith was getting wobbly—carrying a list inside his suit pocket.

Goldsmith was not unmoved by Addington's arguments, say his friends and colleagues. He told colleagues he openly worried that he might be putting soldiers and CIA officers in legal jeopardy. He did not want to weaken America's defenses against another terrorist attack. But he also wanted to uphold the law. Goldsmith, known for putting in long hours, went to new extremes as he reviewed the OLC opinions. Colleagues received e-mails from him at all hours of the night. His family—his wife, 3-year-old son and newborn baby boy—saw him less and less often. Sometimes he would take his older boy down to the Justice Department's Command Center on Saturdays, just to be near him.

By June 2004, the crisis came to a head when the torture memo leaked to The Washington Post. Goldsmith was worn out but still resolute. He told Ashcroft that he was formally withdrawing the August 2002 torture memo. With some prodding from Comey, Ashcroft again backed his DOJ lawyers—though he was not happy to engage in another battle with the White House. Comey, with Goldsmith and Philbin at his side, held a not-for-attribution background briefing to announce that the Justice Department was disavowing the August 2002 torture memo. At

the same time, White House officials held their own press conference, in part to counter what they saw as Comey's grandstanding. A fierce behind-the-scenes bureaucratic fight dragged on until December, when the OLC issued a new memo that was hardly to the taste of human-rights activists but contained a much more defensible (and broader) definition of torture and was far less expansive about the power of the president to authorize coercive interrogation methods. The author of the revised memo, senior Justice Department lawyer Daniel Levin, fought pitched battles with the White House over its timing and contents; yet again, Comey's intervention was crucial in helping Levin and his allies carry the day.

By then, Goldsmith was gone from Justice. He and his wife (who is a poet) and two children had moved to Cambridge, where Goldsmith had taken a job on the Harvard Law faculty. Other dissenting lawyers had also moved on. Philbin, who had been the in-house favorite to become deputy solicitor general, saw his chances of securing any administration job derailed when Addington, who had come to see him as a turncoat on national-security issues, moved to block him from promotion, with Cheney's blessing; Philbin, who declined to comment, was planning a move into the private sector. Levin, whose battles with the White House took their toll on his political future as well, left for private practice. (Levin declined to comment.) Comey was working for a defense contractor.

But the national security/civil liberties pendulum was swinging. Bellinger, who had become legal adviser to Secretary of State Condoleezza Rice, began pushing, along with lawyers in the Pentagon, to roll back unduly harsh interrogation and detention policies. After the electronic eavesdropping program leaked in The New York Times in December 2005, Sen. Arlen Specter announced that the Senate Judiciary Committee would hold hearings that will start next week. The federal courts have increasingly begun resisting absolutist assertions of executive authority in the war on terror. After Cheney's chief of staff, Scooter Libby, pleaded not guilty to perjury charges in the Plame leak case, Addington took Libby's place. He is still a force to be reckoned with in the councils of power. And he still has the ear of the president and vice president; last week Bush was out vigorously defending warrantless eavesdropping. But, thanks to a few quietly determined lawyers, a healthy debate has at last begun.

You are currently subscribed to News Update (wires) as: Blake_Gottesman@who.eop.gov.
To unsubscribe send a blank email to leave-whitehouse-news-wires-1000207E@list.whitehouse.gov

Subject: Annotated Remarks on SOTU #23

From: "Carson, Melissa M."

Date: 1/30/06, 1:22 AM

To: "Kavanaugh, Brett M."

CC: "McGurn, William J.", "Gerson, Michael J.", "McConnell, John P.", "Drouin, Lindsey E.", "Kropp, Emily L.", "Ward, Frank P.", "Merkley, Brendon A.", "Fahy, Brian D."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 17:22:30 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

b(6),P5,P6

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: annotated DRAFT
From: "Carson, Melissa M."
Date: 1/31/06, 5:26 AM
To: "Kavanaugh, Brett M."
CC: "Ward, Frank P.", "Merkley, Brendon A.", "Fahy, Brian D.", "Drouin, Lindsey E."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 17:22:31 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

b(6),P5,P6

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: Annotated Remarks -- SOTU #31

From: "Carson, Melissa M."

Date: 1/31/06, 7:24 AM

To: "Kavanaugh, Brett M."

CC: "McGurn, William J.", "Gerson, Michael J.", "McConnell, John P.", "Drouin, Lindsey E.", "Kropp, Emily L.", "Ward, Frank P.", "Merkley, Brendon A.", "Fahy, Brian D."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 17:22:33 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

b(6),P5,P6

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: Fw: Annotated Remarks -- SOTU #31
From: "Gerson, Michael J."
Date: 1/31/06, 10:33 AM
To: "Kavanaugh, Brett M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 17:22:33 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

b(6),P5,P6

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: FW: PAT ACT/NSA Insert
From: "Thiessen, Marc A."
Date: 2/8/06, 9:19 PM
To: "Kavanaugh, Brett M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 17:22:35 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: PAT ACT/NSA Insert
From: "Kavanaugh, Brett M."
Date: 2/8/06, 9:21 PM
To: "Thiessen, Marc A."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 17:22:36 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: War on Terror #8
From: "Green, Anneke E."
Date: 2/9/06, 12:50 AM
To: "Kavanaugh, Brett M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 17:22:37 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

b(6),P5,P6

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: Please send to Ambassador Negroonte (DNI Watch Ctr) and Director Goss (CIA Ops Ctr)

From: "Sherzer, David"

Date: 2/9/06, 3:29 AM

To: "DL-NSC-WHSR"

CC: "Sherzer, David", "Kavanaugh, Brett M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 17:22:39 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

b(6),P5,P6

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: For FINAL Review -- Draft #14, Remarks on the Global War on Terror -- National Guard Association

From: "Sherzer, David"

Date: 2/9/06, 3:35 AM

To: [b3 50 USC 3024 (m)(1)]

CC: "Kavanaugh, Brett M.", "Burck, Bill", "Sherzer, David"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 12:49:48 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P3,P6,P5,b(6),b(3)

Notes:

50 USC 3024 (m)(1)

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: UPDATED: Remarks on the War on Terror #14

From: "Kavanaugh, Brett M."

Date: 2/9/06, 12:01 PM

To: "17324305", "West, Christal R.", "Weinstein, Jared B.", <kr@rove.com>, "Hughes, Taylor A.", "Bolten, Joshua B.", "Kaplan, Joel", "Dick, Denise Y.", "Dryden, Logan E.", "Morgan, Derrick D.", "Miers, Harriet", "Roebke, Heather M.", "Drummond, Michael", "Kelley, William K.", "McMillin, Stephen S.", "Gerry, Brett C.", "Gerdelman, Sue H.", "Trulio, David V.", "Townsend, Frances F.", "Rapuano, Kenneth", "Parrish, Jobi A.", "Hughes, Taylor A.", "17435416", "Haenle, Paul T.", "Naranjo, Brian R.", "Crouch, Jack D.", "McClellan, Scott", "Hervey, Tina", "Mamo, Jeanie S."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 17:22:40 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

b(6),P5,P6

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: draft 14 ...
From: "Kavanaugh, Brett M."
Date: 2/9/06, 12:23 PM
To: "Gottesman, Blake"
CC: "Keller, Karen E.", "Campbell, Sarah"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 17:28:12 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P6,b(6),P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: RE: Annotated Drafts...
From: "Drouin, Lindsey E."
Date: 2/9/06, 12:26 PM
To: "Kavanaugh, Brett M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 17:28:12 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P6,b(6),P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: FW: UPDATED: Remarks on the War on Terror #14
From: "Kaplan, Joel"
Date: 2/9/06, 1:23 PM
To: "Kavanaugh, Brett M."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 17:28:14 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P6,b(6),P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: Weekly Summary Gift Report

From: "Taplett, Claire"

Date: 2/9/06, 9:29 PM

To: "Burck, Bill", "Drogin, Leslie", "Hipp, Duke", "Houser, Molly M.", "Kavanaugh, Brett M.", "Murer, Marguerite A.", "Slaughter, Kristen K."

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 17:28:15 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P6,b(6)

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: FW: Weekley Summary Gift Report
From: "Kavanaugh, Brett M."
Date: 2/9/06, 11:01 PM
To: "Keller, Karen E.", "Gottesman, Blake", "Campbell, Sarah"

THIS RECORD IS A WITHDRAWAL SHEET

Date created: Mon Apr 08 17:28:16 EDT 2019

Releasability: Withheld In Full

Reasons for Withholding:

P6,b(6),P5

Notes:

Case ID: gwb.2018-0258-F.3

Additional Information:

Subject: FW: AP – Bush defends domestic surveillance program to fellow Republicans
From: "Gottesman, Blake"
Date: 2/10/06, 1:59 PM
To: "Kavanaugh, Brett M.", "Hagin, Joseph W"

jared has already passed this to the chief. not sure what happened yet. i assume whca continued feeding this back to master control, but i'm not sure about that -- and i haven't heard anything further yet.

“I want to share some thoughts with you before I answer your questions,” said Bush, unaware that microphones were still on and were transmitting his comments back to the White House press room. “First of all, I expect this conversation we're about to have to stay in the room. I know that's impossible in Washington.”

From: White House News Update [mailto:News.Update@WhiteHouse.Gov]
Sent: Friday, February 10, 2006 1:43 PM
To: Gottesman, Blake
Subject: AP - Bush defends domestic surveillance program to fellow Republicans

Bush defends domestic surveillance program to fellow Republicans

By JENNIFER LOVEN

CAMBRIDGE, Md. (AP) _ President Bush defended his warrantless eavesdropping program Friday, saying during what he thought were private remarks that he concluded that spying on Americans was necessary to fill a gap in the United States' security.

“I wake up every morning thinking about a future attack, and therefore, a lot of my thinking, and a lot of the decisions I make are based upon the attack that hurt us,” Bush told the House Republican Caucus which was in retreat at a luxury resort along the Choptank River on Maryland's Eastern Shore.

The president said he asked the National Security Agency to devise a way to gather intelligence on terrorists' potential activities, and the result was the super-secret spy outfit's program to monitor the international e-mails and phone calls of people inside the United States with suspected ties to terrorists overseas. Bush said lawyers in the White House and at the Justice Department signed off on the program's legality, and “we put constant checks on the program.”

“I take my oath of office seriously. I swear to uphold the Constitution and laws of the United States,” Bush said.

The president's comments on the NSA eavesdropping came after eight minutes of remarks intended for public consumption. In them, Bush stroked lawmakers with thanks and gave a gentle push for his 2006 priorities in a scaled-back version of last month's State of the Union address.

“I'm looking forward to working with you. And I'm confident we'll continue the success we have had together,” he said. “So I've come to say thanks for your hard work in the past

and thanks for what we're going to do to make this country continue to be the greatest country on the face of the Earth."

Reporters then were ushered out _ ``I support the free press, let's just get them out of the room," Bush said _ so the president could speak privately to his fellow Republicans.

``I want to share some thoughts with you before I answer your questions," said Bush, unaware that microphones were still on and were transmitting his comments back to the White House press room. ``First of all, I expect this conversation we're about to have to stay in the room. I know that's impossible in Washington."

That was not to be _ and it was telling that the president chose the controversial NSA program as the first topic to raise out of reporters' earshot. Even so, there was no substantive difference between those statements and the series of public speeches he has given recently to defend the program.

The eavesdropping program has come under fire from Republicans as well as Democrats. They argue that Bush already has the authority to monitor such communications through existing law that requires a warrant from a secret court set up to act quickly, or even after the fact. Bush has argued that the system isn't nimble enough.

The president faced a House Republican Caucus in turmoil.

At the start of an election year, the House GOP is just off a bruising fight to replace former Majority Leader Tom DeLay, R-Texas, is fighting over reforming the time-honored congressional tradition of funding individual pet projects known as earmarks, and faces potentially damaging revelations in an ongoing public corruption investigation centered on a high-flying lobbyist with extensive ties to Republicans.

Though the lawmakers gave Bush a standing ovation and interrupted his remarks several times with applause, the questions were sharp.

White House press secretary Scott McClellan said that Bush kept his prepared remarks brief so that he would have extra time for the more free-wheeling portion of the discussion.

You are currently subscribed to News Update (wires) as: Blake_Gottesman@who.eop.gov. To unsubscribe send a blank email to leave-whitehouse-news-wires-1000207E@list.whitehouse.gov

Subject: RE: AP – Bush defends domestic surveillance program to fellow Republicans
From: "Gottesman, Blake"
Date: 2/10/06, 1:59 PM
To: "Gottesman, Blake", "Kavanaugh, Brett M.", "Hagin, Joseph W"

[needless to say, todd and chris are aware and investigating what happened.](#)

From: Gottesman, Blake
Sent: Friday, February 10, 2006 1:59 PM
To: Kavanaugh, Brett M.; Hagin, Joseph W
Subject: FW: AP - Bush defends domestic surveillance program to fellow Republicans

[jared has already passed this to the chief. not sure what happened yet. i assume whca continued feeding this back to master control, but i'm not sure about that -- and i haven't heard anything further yet.](#)

“I want to share some thoughts with you before I answer your questions,” said Bush, unaware that microphones were still on and were transmitting his comments back to the White House press room. “First of all, I expect this conversation we’re about to have to stay in the room. I know that’s impossible in Washington.”

From: White House News Update [mailto:News.Update@WhiteHouse.Gov]
Sent: Friday, February 10, 2006 1:43 PM
To: Gottesman, Blake
Subject: AP - Bush defends domestic surveillance program to fellow Republicans

Bush defends domestic surveillance program to fellow Republicans

By JENNIFER LOVEN

CAMBRIDGE, Md. (AP) – President Bush defended his warrantless eavesdropping program Friday, saying during what he thought were private remarks that he concluded that spying on Americans was necessary to fill a gap in the United States' security.

“I wake up every morning thinking about a future attack, and therefore, a lot of my thinking, and a lot of the decisions I make are based upon the attack that hurt us,” Bush told the House Republican Caucus which was in retreat at a luxury resort along the Choptank River on Maryland's Eastern Shore.

The president said he asked the National Security Agency to devise a way to gather intelligence on terrorists' potential activities, and the result was the super-secret spy outfit's program to monitor the international e-mails and phone calls of people inside the United States with suspected ties to terrorists overseas. Bush said lawyers in the White House and at the Justice Department signed off on the program's legality, and “we put constant checks on the program.”

"I take my oath of office seriously. I swear to uphold the Constitution and laws of the United States," Bush said.

The president's comments on the NSA eavesdropping came after eight minutes of remarks intended for public consumption. In them, Bush stroked lawmakers with thanks and gave a gentle push for his 2006 priorities in a scaled-back version of last month's State of the Union address.

"I'm looking forward to working with you. And I'm confident we'll continue the success we have had together," he said. "So I've come to say thanks for your hard work in the past and thanks for what we're going to do to make this country continue to be the greatest country on the face of the Earth."

Reporters then were ushered out "I support the free press, let's just get them out of the room," Bush said "so the president could speak privately to his fellow Republicans.

"I want to share some thoughts with you before I answer your questions," said Bush, unaware that microphones were still on and were transmitting his comments back to the White House press room. "First of all, I expect this conversation we're about to have to stay in the room. I know that's impossible in Washington."

That was not to be "and it was telling that the president chose the controversial NSA program as the first topic to raise out of reporters' earshot. Even so, there was no substantive difference between those statements and the series of public speeches he has given recently to defend the program.

The eavesdropping program has come under fire from Republicans as well as Democrats. They argue that Bush already has the authority to monitor such communications through existing law that requires a warrant from a secret court set up to act quickly, or even after the fact. Bush has argued that the system isn't nimble enough.

The president faced a House Republican Caucus in turmoil.

At the start of an election year, the House GOP is just off a bruising fight to replace former Majority Leader Tom DeLay, R-Texas, is fighting over reforming the time-honored congressional tradition of funding individual pet projects known as earmarks, and faces potentially damaging revelations in an ongoing public corruption investigation centered on a high-flying lobbyist with extensive ties to Republicans.

Though the lawmakers gave Bush a standing ovation and interrupted his remarks several times with applause, the questions were sharp.

White House press secretary Scott McClellan said that Bush kept his prepared remarks brief so that he would have extra time for the more free-wheeling portion of the discussion.

You are currently subscribed to News Update (wires) as:

Blake_Gottesman@who.eop.gov.

To unsubscribe send a blank email to leave-whitehouse-news-wires-1000207E@list.whitehouse.gov

Subject: NITRD Transmittal letter clearance for OSTP
From: "Merzbacher, Celia"
Date: 2/13/06, 1:00 PM
To: "Kavanaugh, Brett M."
CC: "Sokul, Stanley S.", "Romine, Charles H."

To: WH Staff Secretary

Please find attached a one-page transmittal letter from Dr. Marburger to Congress conveying the annual Networking and Information Technology Research and Development (NITRD) Budget Supplement. I request approval of this draft letter so that we may transmit the Budget Supplement to Congress with the memo attached. Following last year's ruling by the WH Staff Secretary, the transmittal letter alone, and not the budget supplement, is being submitted for WH clearance. However, for information purposes, a copy of the budget supplement is also provided as an attachment.

The multi-agency NITRD Program spans a broad spectrum of information technology R&D efforts across a dozen agencies. The NITRD budget supplement is prepared annually, in accordance with Congressional reporting requirements, by the Networking and Information Technology R&D Subcommittee of the National Science and Technology Council (NSTC). It summarizes the current fiscal year's accomplishments and the upcoming fiscal year's plans for the Federal NITRD Program.

If possible, we would like to have a decision on White House clearance of the one page letter by **4:00 PM today, 13 February**, to ensure that the Budget Supplement can be conveyed to Congress in advance of Dr. Marburger's scheduled testimony before the House Science Committee on Wednesday, 15 February, at 10AM. Questions regarding the letter can be directed to Stan Sokul, Deputy Associate Director of the Office of Science and Technology Policy's Technology Division (ssokul@ostp.eop.gov <<mailto:ssokul@ostp.eop.gov>> , 456-6070) or to me (see contact info below).

Thank you very much.

Celia Merzbacher, Ph.D.

Acting Assistant Director for Technology
Office of Science and Technology Policy

Executive Director
President's Council of Advisors on Science and Technology

Executive Office of the President
Tel: 202-456-6108
Fax: 202-456-6021

— Attachments: —

FY07 NITRD Transmittal-FINAL(3).doc	24.0 KB
07Supp_draft4_0212b_9pm.doc	236 KB

February 14, 2006

MEMBERS OF CONGRESS:

I am pleased to forward with this letter the annual report on the interagency Networking and Information Technology Research and Development (NITRD) Program. This Supplement to the President's Budget for Fiscal Year 2007 describes activities funded by Federal NITRD agencies in advanced networking, high-end computing and information technologies. Innovations in science and technology derived from NITRD investments contribute substantially to strengthening the Nation's economy. Cyber security and information assurance research and development in the NITRD Program are enhancing the future security of the Nation's information infrastructure.

The President's 2007 Budget provides an increase of over nine percent for the NITRD Program as a whole, recognizing the important contribution of information technology research and development to the Nation's competitiveness. I am particularly pleased to be able to draw attention to the effect that the President's American Competitiveness Initiative (ACI) has had on the NITRD Program. The 2007 Budget proposes an increase for the three agencies highlighted in the ACI (the National Science Foundation, the Department of Energy's Office of Science, and the National Institute of Standards and Technology) of 17 percent over 2006 levels.

Tools and capabilities that result from NITRD investments propel advances in nearly every area of science and technology, and enhance the Nation's competitiveness. Agencies participating in the NITRD Program actively coordinate both the planning and execution of their research programs, avoiding duplication and making these programs more productive. This Budget Supplement provides details of such interagency coordination for the NITRD Program.

I am pleased to provide you with this timely report.

Sincerely,

John H. Marburger III
Director

SUPPLEMENT TO THE PRESIDENT'S BUDGET
FOR FISCAL YEAR 2007



THE
NETWORKING AND INFORMATION TECHNOLOGY
RESEARCH AND DEVELOPMENT
PROGRAM

A Report by the
Subcommittee on Networking and Information Technology
Research and Development

Committee on Technology
National Science and Technology Council

FEBRUARY 2006

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF SCIENCE AND TECHNOLOGY POLICY
WASHINGTON, D.C.

February XX, 2006

MEMBERS OF CONGRESS:

I am pleased to forward with this letter the annual report on the interagency Networking and Information Technology Research and Development (NITRD) Program. This Supplement to the President's Budget for Fiscal Year 2007 describes activities funded by Federal NITRD agencies in advanced networking, high-end computing and information technologies. Innovations in science and technology derived from NITRD investments contribute substantially to strengthening the Nation's economy. Cyber security and information assurance research and development in the NITRD Program are enhancing the future security of the Nation's information infrastructure.

The President's 2007 Budget provides an increase of over nine percent for the NITRD Program as a whole, recognizing the important contribution of networking and information technology research and development to the Nation's competitiveness. I am particularly pleased to be able to draw attention to the effect that the President's American Competitiveness Initiative (ACI) has had on the NITRD Program. The 2007 Budget proposes an increase for the three agencies highlighted in the ACI (the National Science Foundation, the Department of Energy's Office of Science, and the National Institute of Standards and Technology) of 17 percent over 2006 levels.

Tools and capabilities that result from NITRD investments propel advances in nearly every area of science and technology, and enhance the Nation's competitiveness. Agencies participating in the NITRD Program actively coordinate both the planning and execution of their research programs, avoiding duplication and making these programs more productive. This Budget Supplement provides details of such interagency coordination for the NITRD Program.

I am pleased to provide you with this timely report.

Sincerely,

John H. Marburger III
Director

Table of Contents

Executive Summary	ii
High End Computing Infrastructure and Applications (HEC I&A)	1
High End Computing Research and Development (HEC R&D)	3
Coordinated Implementation of the <i>Federal Plan for High-End Computing</i>	5
Cyber Security and Information Assurance (CSIA)	6
Human-Computer Interaction and Information Management (HCI&IM)	9
Large Scale Networking (LSN)	11
High Confidence Software and Systems (HCSS)	13
Social, Economic, and Workforce Implications of IT and IT Workforce Development (SEW)	15
Software Design and Productivity (SDP)	17
Agency NITRD Budgets	19
NITRD Program Budget Analysis	20
NITRD Subcommittee Roster	24
Participation in the NITRD Program	25
Glossary	26
Acknowledgements	29
Copyright Information	30
To Request Additional Copies	30

Executive Summary

This Supplement to the President's Fiscal Year (FY) 2007 Budget provides a technical summary of the budget request for the Networking and Information Technology Research and Development (NITRD) Program, as required by the High-Performance Computing Act of 1991 (P.L. 102-194) and the Next Generation Internet Research Act of 1998 (P.L. 105-305). The NITRD Program, now in its 15th year, represents the coordinated efforts of many Federal agencies that support R&D in networking and information technology. The NITRD enterprise is an Administration interagency R&D budget priority for FY 2007.

The Supplement to the President's Budget for the NITRD Program describes current technical and coordination activities and FY 2007 plans of the 12 Federal agencies in the NITRD budget crosscut, as well as those of other agencies that are not part of the formal crosscut but participate in NITRD activities. In the NITRD Program, the term "agency" may refer to a department, a major departmental subdivision, or a research office or laboratory. NITRD activities and plans are coordinated in eight Program Component Areas (PCAs): high-end computing research and development; high-end computing infrastructure and applications; cyber security and information assurance; human-computer interaction and information management; large-scale networking; high-confidence software and systems; social, economic, and workforce implications of IT and IT workforce development; and software design and productivity. Agency program managers in each PCA meet monthly in an Interagency Working Group (IWG) or Coordinating Group (CG) to exchange information and coordinate R&D technical plans and activities such as workshops and joint solicitations.

Overall NITRD Program coordination is carried out by the Subcommittee on Networking and Information Technology Research and Development, under the aegis of the Committee on Technology of the National Science and Technology Council (NSTC). Changes within the NITRD Program that are highlighted in the FY 2007 Supplement include the chartering of the High End Computing CG as an IWG, which reports to the NITRD Subcommittee, and the re-chartering of the Cyber Security and Information Assurance (CSIA) IWG, which now reports to both the NSTC's NITRD Subcommittee and its Subcommittee on Infrastructure. The re-chartering of the CSIA IWG (which previously existed as the Critical Information Infrastructure Protection IWG, outside of the NITRD Program) is the result of incorporating CSIA as a new PCA within the NITRD Program, and is reflected in the addition of a new technical element in the budget reporting contained in this document. **This year's NITRD budget also includes for the first time reporting by the Department of Defense Services (Air Force, Army, and Navy).**

The Administration's recently announced American Competitiveness Initiative, which calls for a doubling over 10 years of the investment in key Federal agencies that support basic research in the physical sciences and engineering, also contributes to the NITRD Program FY 2007 budget. NITRD agencies NSF, DOE/SC, and NIST show budget increases that exceed the base percentage increase in the overall Program budget (for details, please see the NITRD Program Budget Analysis, page 20).

For each PCA, the NITRD Budget Supplement presents strategic priorities underlying the FY 2007 budget request, highlights of the request, ongoing and anticipated interagency planning and coordination activities, and additional technical activities, by agency. Agencies that are engaged in cited activities as funders, performers, in-kind contributors, and participants in focused coordination activities are identified, with funders and performers listed first and, following the word "with," the in-kind contributors and participants. When applicable, lead agencies are listed first. Some large-scale activities may be listed in more than one PCA because they involve R&D efforts in a variety of technologies across multiple disciplines. In such cases, agencies report the portion of program funding in each relevant PCA. Additional agency activities are reported with NITRD member agencies listed first, followed by participating agencies.

High End Computing (HEC) Infrastructure and Applications (I&A)

NITRD Agencies: NSF, OSD, NIH, DOE/SC, NASA, NIST, DOE/NNSA, NOAA, EPA

HEC I&A agencies coordinate Federal activities to provide advanced computing systems, applications software, data management, and HEC R&D infrastructure to meet agency mission needs and to keep the United States at the forefront of 21st century science, engineering, and technology. HEC capabilities enable researchers in academia, Federal laboratories, and industry to model and simulate complex processes in biology, chemistry, climate and weather, environmental sciences, materials science, nanoscale science and technology, physics, and other areas to address Federal agency mission needs.

President's 2007 Request***Strategic Priorities Underlying This Request***

Supporting Federal agencies' science, engineering, and national security missions and sustaining U.S. scientific leadership require ongoing investment in Federal HEC facilities as well as advanced computational and data-intensive applications. HEC I&A strategic priorities to address these needs include:

Production-quality HEC resources: Increase resources to meet expanding Federal agency mission needs

Federal HEC acquisitions: Reduce time and cost by improving benchmarking and procurement coordination

Productivity: Collaborate on new assessments that more accurately predict computing system performance on diverse scientific problems, total time to solution, and total cost of ownership

Science and engineering applications: Develop more detailed and accurate applications for next-generation HEC platforms

Access to leadership-class systems: Provide access for the broad academic, industrial, and government R&D communities through peer-reviewed processes

Access to Federal HEC resources: Expand access for leading researchers to develop and execute HEC science and engineering applications that address Federal agencies' mission needs. This includes access to HEC capability and capacity systems for researchers associated with agencies that do not have HEC facilities.

Highlights of Request***Acquisition of prototype leadership-class and production R&D systems***

NSF: Five-year High Performance Computing System Acquisition: Towards a Petascale Computing Environment for Science and Engineering program for deployment and support of world-class HEC resources for academic research; new platform expected in 2006 and petascale resources by 2010

DOE/SC (ORNL): Upgrade ORNL's Leadership Computing Facility (LCF) to over 250 TF, with 10 percent of available cycles for use across Federal agencies

DOE/SC (ANL): Diversify LCF resources through acquisition of 100-TF BlueGene/P at ANL

DOE/SC (LBNL): For National Energy Research Scientific Computing Center (NERSC), acquire next-generation computational platform, the NERSC-5 (100-150 TF)

NASA (Headquarters): Establish a central HEC office under agency-wide "Shared Capability" theme

NASA (ARC): Continue enhancing Columbia supercomputer's quality of service for science and engineering users and prepare for transition to next-generation computational platform

NASA (GSFC): Acquire next-generation platform for Earth and space science research

Applications

NSF: New Office of Cyberinfrastructure to enable exploration of both emerging and established science and engineering applications through new uses of balanced HEC computing, storage, software, services, and other resources for advanced academic research

DOE/SC: Re-competition of modeling and simulation applications in Scientific Discovery Through Advanced Computing (SciDAC) program, to extend SciDAC's multidisciplinary, multi-institutional teams of computer and disciplinary scientists developing advanced applications in physical and biological sciences

DOE/SC: Competition to select small number of university-based SciDAC institutes to become centers of excellence in high-end computational science in areas critical to DOE missions and HEC software centers

DOE/SC: Expand 2005 Innovative and Novel Computational Impact on Theory and Experiment (INCITE) program to include all major DOE/SC platforms through open call for proposals from agencies and industry

NASA: Through National Leadership Computing System call for proposals, open part of Columbia system to users outside of NASA who present the most demanding science and engineering challenges

DOE/NNSA: Develop verification and validation methodologies for weapons simulations including quantification of margins and uncertainties

NOAA, NSF: Improve capabilities for dynamic data assimilation

Planning and Coordination Supporting Request

Access to leadership-class computing: Coordinated efforts by agencies to make their most powerful HEC resources more widely available through open calls for proposals – DOE/SC, NASA, NSF

Benchmarking: Measuring HEC system performance on a broad range of applications – DARPA, DOE/SC, EPA, NASA, NOAA, NSF, **OSD (HPCMPO and ODDR&E)**

Acquisition coordination: Information sharing, procedural streamlining, and collaborative analysis of total cost of ownership – DOE/SC, EPA, NASA, NOAA, NSF, **OSD (HPCMPO and ODDR&E)**

Cooperative platform development: Design collaboration on systems for a common set of applications – DOE/NNSA, DOE/SC, NSA

Modeling of infectious disease: NSF providing Extensible Terascale Facility (ETF) resources and expertise for NIH large-scale Models of Infectious Disease Agents Study (MIDAS) – NSF, NIH

SciDAC program: Re-competition of applications and infrastructure components – DOE/SC, DOE/NNSA

Shared infrastructure for climate and weather modeling: Module interface standards for software interoperability – DOE/SC, EPA, NASA, NOAA, NSF (NCAR), **OSD**

Air quality modeling: Atmospheric dispersion models and other simulation techniques used in assessing source impacts and control strategies – EPA, NOAA

Additional 2006 and 2007 Activities by Agency

NSF: Continue ETF, core centers (SDSC and NCSA), and middleware initiative in support of academic science and engineering activities

OSD (HPCMPO): HEC capabilities and services; HEC software development and life cycle support; expert computational consulting services for DoD laboratories from the academic community; develop future HEC workforce through fellowships, internships, and workshops; keep HEC systems current; recapitalize 25 percent of systems; HEC system security

NIH: NIH Roadmap National Centers for Biomedical Computing (NCBCs); Cancer Imaging and Computational Centers; P41 Computational Centers; NLM information and analysis servers; international networks for biomedical data and software sharing; bioinformatics resource centers for emerging and re-emerging infectious disease; proteomics and protein structure initiatives

DOE/SC: LCF at ORNL – X1e (18 TF), XT3 (25 TF), expansion in 2007; LCF at ANL – BlueGene/L (5 TF), expansion in 2007; NERSC – NERSC-4 SP3 (9 TF), NCS-A, Infiniband cluster (3 TF), NCS-B capacity system (7 TF) available to users in 2006, NERSC-5 initially available to users in 2007; expansion of SciDAC applications and infrastructure across DOE/SC and including DOE/NNSA, NSF participation in 2006 and 2007; applied mathematics research for computational science including multiscale mathematics

NASA: Columbia system (62 TF) at NASA ARC, with 2,048-processor shared memory environment and integrated support model, to aggressively scale application codes for rapid mission impact; NASA GSFC acquired system (7 TF) for Earth and space science research

NIST: Parallel and distributed algorithms such as for computational nanotechnology; interoperable MPI standards; virtual measurement laboratory immersive visualization; fundamental mathematical tools

DOE/NNSA: Develop, deploy, and maintain weapons and engineering codes; provide production-quality computational environment for the ASC Purple system; build common capacity computing environment across three labs; re-compete Alliance Centers program; develop and improve verification and validation methods for scientific simulations

NOAA: Integrated acquisition of next-generation R&D HEC systems for all of NOAA; integrated management and allocation of HEC resources; modeling frameworks for WRF and ESMF; grid technologies

EPA: HEC capabilities for GEOSS demonstrations; air-quality algorithm enhancements; computational toxicology for faster, more accurate, less expensive analysis; grid services deployment

High End Computing (HEC) Research and Development (R&D)

NITRD Agencies: NSF, **OSD**, DARPA, DOE/SC, NSA, NASA, NIST, DOE/NNSA, NOAA

HEC R&D agencies conduct and coordinate hardware and software R&D to enable the effective use of high-end systems to meet Federal agency mission needs, to address many of society's most challenging problems, and to strengthen the Nation's leadership in science, engineering, and technology. Research areas of interest include hardware (e.g., microarchitecture, memory subsystems, interconnect, packaging, I/O, and storage), software (e.g., operating systems, languages and compilers, development environments, algorithms), and systems technology (e.g., system architecture, programming models).

President's 2007 Request

Strategic Priorities Underlying This Request

Sustain U.S. leadership in HEC: Develop new generation of economically viable, high-productivity computing systems to meet Federal agencies' HEC needs, which will require managing rapidly increasing volumes of data and integrating multiscale (in space and time), multidisciplinary simulations

Hardware and software: Integrate innovations, especially language and development environments, to reduce barriers to use of systems that may have tens of thousands of processors and to increase the productivity of end-user applications

System prototypes: Develop, test, and evaluate robust, innovative HEC systems and software to reduce industry and end-user risk and to increase competitiveness. Industries using HEC include aeronautics, automobile, biomedicine, chemicals, petrochemicals, and pharmaceuticals.

Research pipeline: Continue HEC University Research Activity (HEC-URA) to help refill the workforce pipeline with highly skilled researchers who can develop future-generation HEC systems and software

Highlights of Request

HEC-URA: New R&D in file systems and I/O – NSF, DARPA, DOE/NNSA, DOE/SC, NSA

High-Productivity Computing Systems (HPCS) Phase III: Final phase of program to develop economically viable prototypes for national security and industrial user communities, to address all aspects of HEC systems (packaging, processor/memory interfaces, networks, operating systems, compilers, languages, and runtime systems) – DARPA, DOE/SC, DOE/NNSA, NSA, with NASA, NSF, **OSD**, other agencies

Advanced capabilities for scientific research: Expand SciDAC-enabling organizational resources including centers, institutes, and partnerships – DOE/SC, DOE/NNSA

Prototype research and evaluation: Prepare users for future generations of high-end systems and reduce procurement risk – DOE/SC

Vector processor system: Continue cooperative development – NSA, with other NITRD agencies

Quantum computing program: DARPA, NIST, NSA

Software environments: Develop common system software and tools for high-end systems – DOE/NNSA, DOE/SC, NSF, **OSD**

Weapons applications: Sustain advanced systems development effort to meet programmatic needs for increased productivity – DOE/NNSA

Planning and Coordination Supporting Request

Planning

Technical and planning workshops: HPCS Productivity Workshops, Storage and I/O Workshop to coordinate new HEC-URA file systems and I/O effort, HEC Requirements Workshop supporting new NSF HEC initiative – DARPA, DOE/NNSA, DOE/SC, NASA, NIH, NSA, NSF, **OSD**

Council on Competitiveness HPC Initiative: Fund studies, conferences, and educational activities to stimulate and facilitate wider usage of HEC across the private sector to propel productivity, innovation, and competitiveness – DARPA, DOE/NNSA, DOE/SC, NSF

Open-source software: Research to enable users to read, modify, and redistribute source code, fostering more efficient development and increased collaboration to improve software quality – DOE/NNSA, DOE/SC, NASA

Systems architecture

HEC hardware and software testbeds: Facilitate access, share knowledge gained and lessons learned – DOE/SC, NASA, NIST, NOAA, NSF, **OSD**

HPCS Phase III: DARPA, DOE/SC, DOE/NNSA, NSA, with NASA, NSF, **OSD**

Black Widow performance reviews: Assess progress on developmental milestones – NSA, with DARPA, DOE/NNSA, DOE/SC, NASA, NSF, **OSD**

Quantum information science: Study information, communication, and computation based on devices governed by the principles of quantum physics – DARPA, NIST, NSA, NSF

Systems software development

HEC-URA: Coordinate research in operating/runtime systems, languages, compilers, libraries – DARPA, DOE/NNSA, DOE/SC, NASA, NSF

HEC metrics: Coordinate research on effective metrics for application development and execution on high-end systems – DARPA, DOE/SC, NSF, with DOE/NNSA, NASA, NSA, **OSD**

Benchmarking and performance modeling: Collaborate on developing measurement tools to help improve the productivity of HEC systems – DARPA, DOE/NNSA, DOE/SC, NASA, NSA, NSF, **OSD**

File systems: Coordinate R&D funding based on a national research agenda and update agenda on a recurring basis – DARPA, DOE/NNSA, DOE/SC, NASA, NSA, NSF, **OSD**

Additional 2006 and 2007 Activities by Agency

NSF: University-based research on formal and mathematical foundations (algorithmic and computational science); foundations of computing processes and artifacts (software, architecture, design); emerging models for technology and computation (biologically motivated, quantum, and nanotechnology-based computing and design); distributed systems and next-generation software; data-driven science including bioinformatics, geoinformatics, and cognitive neuroscience; infrastructure development (create, test, and harden next-generation systems); and software and tools for high-end computing

OSD: Software Protection Initiative research in protection of critical defense software; applications software profiling and development; extend benchmarking and performance modeling to support system acquisitions and applications software development

DARPA: Architectures for cognitive information processing program – a new class of processing approaches, algorithms, and architectures to efficiently enable and implement cognitive information processing; begin transition of polymorphous computing architectures to DoD and commercial products; networked embedded systems technologies

DOE/SC: Research in programming models, performance modeling and optimization, software component architectures; development time and execution time productivity (with HPCS); data analysis and management, interoperability, software development environments

NSA: Eldorado – work with vendor on XT3 modifications, fully funding development in 2005-2006, available in 2006-2007

NASA: Participate in interagency coordination of architectures, testbeds, and system performance assessment

NIST: Architectures and algorithms for quantum computers; secure quantum communications

DOE/NNSA: Platforms; problem-solving environments; numeric methods; re-compete Alliance Centers program; user-productivity baseline in context of weapons simulations

Coordinated Implementation of the *Federal Plan for High-End Computing*

In 2003, the High-End Computing Revitalization Task Force (HECRTF) was chartered under the National Science and Technology Council (NSTC) to develop a plan for undertaking and sustaining a robust Federal high-end computing program to maintain U.S. leadership in science and technology. The *Federal Plan for High-End Computing*, released in May 2004, offers a vision for a proactive Federal effort that advances high-end computing technology to address many of society's most challenging large-scale computational problems and, in doing so, strengthens the Nation's global leadership in the sciences, engineering, and technology.

The HEC IWG is implementing this Plan through the coordination of high-end computing policy, strategies, and programs across NITRD member and participating agencies. Emphasis is placed on identifying and integrating requirements, conducting joint program planning, and developing and implementing joint strategies. Coordination activities encompass fundamental and applied research and development, technology development and engineering, infrastructure and applications, demonstrations, and education and training. The coordination is carried out through monthly HEC IWG meetings, agency-sponsored workshops, technical forums, and a variety of focused multiagency activities. The following list highlights some of these multiagency activities:

High-End Computing University Research Activity (HEC-URA): Beginning in 2004, NSF, DARPA, DOE/SC, and NSA engaged in joint planning and expanded funding for university research in operating systems, languages, compilers, and libraries, and in software tools and development environments. Beginning in 2006, NSF and other agencies will expand funding for research in file systems, storage, and I/O.

DARPA High-Productivity Computing System (HPCS) Program: The DARPA HPCS Program was initiated in 2001 to develop a new generation of high-end computing systems providing leap-ahead advances in performance, robustness, and programmability. Since then, DARPA has expanded its HPCS collaboration with other agencies to now include NSA, DOE/SC, DOE/NNSA, NASA, and NSF. Starting in 2006, HPCS enters Phase III, which will involve active collaboration with these agencies through such mechanisms as funding, participation in review panels, and requirements analysis.

Leadership Systems: The *Federal Plan* advanced the concept of "leadership high-end computing systems" to offer leading-edge computing facilities to enable breakthrough computational science and engineering for problems important to Federal agency missions and to the Nation. Today, this concept has been implemented by DOE/SC at four of its national laboratories through its INCITE program and by NASA through its National Leadership Computing Systems (NLCS) initiative. The two agencies either are completing or have completed solicitations for leadership-class computing resources, and they plan to conduct additional solicitations on a recurring basis. Other agencies are planning similar procurements of leadership-class systems in the near future.

System Performance Assessment: One of the major challenges in guiding research, development, and procurement of high-end computing systems is to measure, compare, and assess system performance. Currently, DOE and DARPA in collaboration with other agencies are developing methods to measure both execution performance and ease of programming. This includes novel work in combining software engineering experiments customized to high-performance computing. In addition, OSD (HPCMPO), DOE/SC (NERSC), and NSF are sharing selected benchmarks and procurement practices in order to streamline and improve the effectiveness of high-end computing systems procurements.

These examples illustrate the collaborative efforts underway in implementing the *Federal Plan for High-End Computing*. These and other HEC activities are described in further detail in the HEC I&A and HEC R&D sections of this Supplement.

Cyber Security and Information Assurance (CSIA)

NITRD Agencies: NSF, **OSD**, NIH, DARPA, NSA, NASA, NIST

Other Participants: CIA, DHS, DOE, DOJ, DOT, DTO, FAA, FBI, State, Treasury, TSWG

CSIA focuses on research and advanced development to prevent, resist, detect, respond to, and/or recover from actions that compromise or threaten to compromise the availability, integrity, or confidentiality of computer-based systems. These systems provide both the basic infrastructure and advanced communications in every sector of the economy, including critical infrastructures such as power grids, emergency communications systems, financial systems, and air-traffic-control networks. These systems also support national defense, national and homeland security, and other vital Federal missions, and themselves constitute critical elements of the IT infrastructure. Broad areas of concern include Internet and network security; confidentiality, availability, and integrity of information and computer-based systems; new approaches to achieving hardware and software security; testing and assessment of computer-based systems security; and reconstitution and recovery of computer-based systems and data.

Incorporation of the CSIA Program Component Area and the CSIA Interagency Working Group (IWG) into the NITRD Program

In August 2005, the NSTC chartered the Cyber Security and Information Assurance (CSIA) IWG. This IWG succeeds the IWG on Critical Information Infrastructure Protection (CIIP), which had been chartered in August 2003 and reported to the Subcommittee on Infrastructure of the NSTC's Committee on Homeland and National Security. The CSIA IWG reports jointly to the Subcommittee on Infrastructure and the NITRD Subcommittee. This change facilitates better integration of CSIA R&D with NITRD activities and reflects the broader impact of cyber security and information assurance beyond critical information infrastructure protection.

The first steps in integrating CSIA R&D into NITRD activities involve incorporating the budget associated with the CSIA PCA and the coordination by the CSIA IWG into the NITRD Program, and completing and releasing the Federal Plan for CSIA R&D (described below). Future steps will include roadmapping CSIA R&D and adjusting the activities in NITRD PCAs in light of the Program's expanded scope. Selected areas requiring cross-PCA coordination are described below.

President's 2007 Request

Strategic Priorities Underlying This Request

Fundamental and applied research for CSIA: New knowledge, technologies, and tools to achieve significantly improved security for the computer-based systems that support national defense, national and homeland security, economic competitiveness, and other national priorities. Key research areas include:

- **Network security:** New communications protocols, especially for wireless networks and mobile ad hoc networks, required to effectively secure networks and the data that travel over them (with LSN)
- **Dependable systems:** Systems with characteristics that include fault tolerance, reliability, safety, and security (with HCSS)
- **Situational awareness and response:** Data fusion and forensics, security visualization, and security management
- **Secure distributed systems:** Ability to function as network-centric multi-domain enterprise with ubiquitous secure collaboration

Infrastructure for R&D: Testbeds, tools, platforms, standards, and data collection and sharing to enable academic, industry, and government researchers to effectively conduct CSIA R&D

Infrastructure protection: Computer-based systems that function as intended, even in the face of cyber attack, and that are able to process, store, and communicate sensitive information according to specified security policies (with HCSS)

Industry outreach and technology transfer: Effective transition and diffusion of R&D results into mainstream products and services and improved practices; increased coordinated industry outreach and technology transfer

to aid timely transition of existing and newly created CSIA R&D to practice, including standards, guidelines, metrics, benchmarks, and best practices

Highlights of Request

Cyber Trust: Academic research in foundations, network security, secure systems software, security of information systems – NSF, DARPA

Testbeds: Development, testing, and evaluation of testbeds for the DETER, EMIST, and GENI projects – NSF, DHS

Datasets: Complete secure, trusted data-sharing infrastructure and initial data collection and sharing – NIST, NSF, DHS

Internet infrastructure security: Domain Name System (DNS) security roadmap, testing, guidance, and routing protocol security – NIST, DHS

Planning and Coordination Supporting Request

Federal Plan for Cyber Security and Information Assurance Research and Development

The CSIA IWG was charged with developing an interagency Federal Plan for CSIA R&D. This forthcoming document, which represents a collaborative effort by the CSIA IWG members, provides a baseline framework for coordinated, multiagency CSIA R&D. The Plan is currently in final clearance.

The Federal Plan resulted from a process in which CSIA R&D needs were identified, analyzed, and prioritized. Part I of the Federal Plan includes sections on:

- Technology Trends
- The Federal Role
- Types of Threats and Threat Agents
- Threat and Vulnerability Trends
- Recent Calls for CSIA R&D
- Strategic Federal Objectives
- R&D Technical and Funding Priorities
- Top Technical and Funding Priorities
- Findings and Recommendations

Part II of the Plan contains commentaries on technical topics. Each commentary includes a definition of the topic and discussions of its importance, the state of the art, and capability gaps requiring R&D. The technical topics are grouped in the following eight broad R&D categories identified in the CSIA IWG’s analysis: functional cyber security; securing the infrastructure; domain-specific security; cyber security characterization and assessment; foundations for cyber security; enabling technologies for CSIA R&D; advanced and next-generation systems and architecture for cyber security; and social dimensions of cyber security.

Other Interagency Planning and Coordination Activities

Roadmapping: Develop an initial roadmap that provides a timeline for activities needed to implement the Federal Plan for CSIA R&D – CSIA IWG

Cyber security R&D:

- **System resilience:** Intrusion tolerance, self-regenerating systems, dynamic quarantine of worms, detection and containment of malicious code – DARPA, **OSD (AFRL)**
- **Adaptive quarantine:** Development of adaptive quarantine to prevent and preempt active, passive, novel insider and outsider cyber attacks against safety-critical and mission support networks and systems enterprise-wide – DTO, FAA
- **Intrusion detection:** Intrusion detection and monitoring, cyber attack detection, traceback, and attribution – NSA, **OSD (AFRL)**, DTO
- **Countermeasures:** Flash ROM countermeasures tool and technologies that address identity theft, fraud detection – TSWG, FBI
- **Power grid:** Trustworthy cyber infrastructure for the power grid – DHS, NSF, DOE
- **Election systems:** Trustworthy election systems – NIST, NSF

Grants and proposals: Collaborate/coordinate on solicitations and evaluations – DARPA, NSA, NSF, DHS, DTO

Federal Plan on National Critical Infrastructure Protection Research and Development: Provide input to the NSTC Subcommittee on Infrastructure on cyber aspects of critical infrastructure protection – CSIA IWG

INFOSEC Research Council *Hard Problem List*: Support the preparation of the *Hard Problem List* released in November 2005 – multiple agencies
Cyber Security: A Crisis of Prioritization: Respond to the PITAC report’s recommendations – CSIA IWG
Improving Cybersecurity Research in the United States: Continue support for National Academies study – DARPA, NIST, NSF

Additional 2006 and 2007 Activities by Agency

NSF: Team for Research in Ubiquitous Secure Technology (TRUST) to transform the ability of organizations to design, build, and operate trustworthy information systems for critical infrastructures; industry/university cooperative research centers in information protection, computer systems, and identification technology; Scholarship for Service program; advanced technology education

OSD (AFRL): Recovery and repair of networks, systems, and applications to operational state following cyber attack, to assure and defend wireless networks, provide predictable end-to-end QoS under degraded network conditions

OSD (AFRL, ARL, and ONR): Research in enhancing network robustness, cyber security; Multidisciplinary University Research Initiative (MURI) in critical infrastructure protection and high-confidence adaptable software

OSD (ODDR&E): Through the High Performance Computing Modernization Program, adapt network intrusion detection and analysis tools to improve collective analysis of multiple sensor inputs and to support IPv6

DARPA: R&D in security-aware systems

NSA: Cryptography, cryptographic infrastructure; high-speed security solutions, security-enhanced operating environment, secure wireless multimedia; authentication, privilege management; attack-sensing warning and response, insider threat, and network dynamics

NASA: Next-generation HEC perimeter protection architecture and system for Columbia supercomputer (a possible model for HEC system security at other agencies), including a new security approach for network-intensive applications and the coupling of two-factor authentication to unattended file transfers

NIST: FISMA standards and guidelines; state and local municipality outreach; secure OS and application configuration specifications, identity management, smart-card interoperability specifications, conformance testing; cryptographic standards, guidelines, tool kit, module validation; PDA forensics guidelines and computer forensics tool effectiveness testing; access control, policy management modeling and prototypes; technology-specific security guidelines (e.g., RFID, Web services, Wi-Max, etc.); remote authentication methods; wireless/PDA security protocols, mechanisms, and seamless/secure mobility; automated combinatorial testing; National Vulnerability Database

DHS: Vulnerability prevention, discovery, and remediation; cyber security assessment; security and trustworthiness for critical infrastructure protection; wireless security; network attack forensics; technologies to defend against identity theft; continued support for the Process Control Systems Forum

DOE: R&D on extracting novel forensic information from hostile scan data and developing statistical and trending analysis for cooperative protection program data

DOJ: Common solutions to security requirements to achieve cost efficiency through broad implementation; incident response and situational awareness

DOT: Secure aircraft data networks and applications; security testing and penetration testing methods; biometrics and access control security for aircraft cockpits and aircraft; risk assessment methods; credentialing; advanced wireless technologies

FAA: Rapid quarantine capability; test biometrics single sign-on; test behavior-based security; enterprise architecture based on the DoD architecture framework; information systems security architecture as enclave with demilitarized zone; integrity and confidentiality lab to test wireless systems security; validate Web data mining that uses concept chain graphs to find vulnerabilities

FBI: Advanced visualization concepts for analyzing various data media types; state-of-the-art integrated analytical tools that support law enforcement investigations; cyber-capabilities-driven enterprise architecture as a business and management tool

TSWG: Secure ground-to-air data communications; automate cyber assessment at the Nuclear Regulatory Commission; develop commercially viable cyber security testing; establish cyber security training center; assess state of the art in infrastructure modeling capabilities

Human-Computer Interaction and Information Management (HCI&IM)

NITRD Agencies: NSF, **OSD**, NIH, DARPA, NASA, AHRQ, NIST, NOAA, EPA

Other Participants: GSA, NARA

HCI&IM R&D aims to increase the benefit of computer technologies to humans, particularly the science and engineering R&D community. To that end, HCI&IM R&D invests in technologies for mapping human knowledge into computing systems, communications networks, and information systems and back to human beings, for human analysis, understanding, and use. R&D areas include: cognitive systems, data analysis in fields such as human health and the environment, information integration, multimodal and automated language translation, robotics, and user interaction technologies.

Highlights of the President's 2007 Request

Strategic Priorities Underlying This Request

Advanced HCI&IM capabilities support key national priorities – including large-scale scientific research, national defense, homeland security, air-traffic control, emergency planning and response, health care, space exploration, weather forecasting, and climate prediction. Key R&D priorities are:

Information accessibility, integration, and management: Next-generation methods, tools, and technologies to make it possible to access, integrate, analyze, and efficiently manage massive stores of widely distributed, heterogeneous information (e.g., science and engineering research data, Federal records). These capabilities will help human analysts make better use of all available information resources in the pursuit of new knowledge. The initial focus is on domain-specific collections, with the long-term goal of developing techniques that can be generalized across domains. Needs also include:

- **Federal information management architecture testbeds:** To evaluate issues in petascale collections of information governed by differing requirements (e.g., national security, personal privacy)
- **Long-term preservation:** Maintenance of and access to long-lived science and engineering data collections and Federal records

Multimodal devices and interfaces: Human-computer interaction capabilities enabling rapid, easy access (e.g., without a keyboard) to and communication and understanding of heterogeneous information (e.g., audio and text in diverse languages, video, images) for national security applications as well as for assistive devices

Systems that know what they are doing: Cognitive systems able to “learn,” adjust to change, and repair themselves, to enhance battlefield capabilities, overall system security, and deployability of robotic devices in emergency-response and hazardous environments

Highlights of Request

Cognitive systems: Continue programs in learning, reasoning, and integrated cognitive systems – DARPA

Global Autonomous Language Exploitation (GALE): New program expanding on Translingual Information Detection, Extraction, and Summarization (TIDES) effort, to reduce the need for linguists and analysts by automatically and rapidly providing translated, distilled information that is relevant and useful to military personnel – DARPA, with NSA, NIST, DLI, CENTCOM, other agencies

Multimodal language recognition and translation: Improved performance and evaluation of human language technologies, including speech-to-text, text retrieval, document summarization, automatic content extraction, speaker and language recognition, dialogue and conversation understanding and summarization, meeting room transcription and summarization, question answering, and machine translation; interactive systems, multimodal user interfaces, and usability – DARPA, NSA, NSF, NIST, DTO, with NARA, other agencies

Data security and data analysis methods: New focus on information privacy and security; research in analysis of digital images and videos; research in methods for computational analysis of data collected in the observational sciences; Office of Cyberinfrastructure strategic plan component for sharing science and engineering data – NSF

Data-intensive discovery and design environments: Interdisciplinary team environments leveraging hyperwalls (wall-size high-resolution tiled display systems) for terascale/petascale data exploration, analysis, and understanding, including concurrent visualization (e.g., real-time rendering, computational steering, and remote access to ongoing computations) and algorithms and tools – NASA

Remote Sensing Information Gateway: Global Earth Observation Systems of Systems (GEOSS) demonstration project to share and integrate Earth observational data with initial applications to support air quality goals – EPA, with NASA, NIH, NOAA

Text Retrieval Conference (TREC): Continue evaluations of information-discovery technologies with tracks on Web retrieval, retrieval of documents for genomics research, question answering, personalized retrieval, and a new legal track – DTO, NIST, NSF, with NARA

Planning and Coordination Supporting Request

National workshop on information integration R&D: Identify key issues for coordinated research such as interoperability, privacy, security, and standards to advance utility of heterogeneous, multimodal information environments – NSF, AHRQ, EPA, NARA, with NIST, GSA, OSD (ONR), other HCI&IM agencies

Drug information and standards: Build system to obtain drug information with standardized definitions and in standardized formats from manufacturers, approve and transmit the information to Federal Web sites, including mapping clinical vocabularies and coding systems to clinical reference terminology adopted by HHS, VA, and DoD, and metadata registry of data standards terms – AHRQ, NIH, NIST, FDA, HHS (CMS), other agencies

Earth System Modeling Framework: Information interoperability and reuse in Earth science applications – NASA, DOE/SC, NOAA, NSF, OSD, other agencies

Eco-Informatics: Workshop and plans for possible second joint solicitation – NSF, NASA, EPA, other agencies

Health informatics: Planning for collaboration to include workshop(s), joint program – NSF, NIH

Additional 2006 and 2007 Activities by Agency

NSF: University-based research in science and engineering informatics; information integration; data mining, information retrieval; knowledge management; human-computer interaction, universal access, digital government; intelligent robots, machine vision technologies; automatic multilingual speech-recognition toolkits

OSD (ONR): New program in human-robot interaction and collaboration; continue programs in persistent surveillance including autonomous systems (e.g., robots, unattended vehicles) and information exploitation; information integration including multiple sources, disparate data types, and shared analysis tools; human factors and organizational design; portable bi-directional language translator

NIH: Curation and analysis of massive biomedical and clinical research data collections; tools to manage and use new databases; tools for building and integrating ontologies; software tools for visualizing complex datasets; curation tools; build nationwide support for standard vocabularies; information integration

NASA: Continue efforts on agencywide data exploration architecture with centralized data repository; mobile autonomous robots and intelligent systems; speech-based human-computer interaction; wind down space exploration systems projects, including team-centered virtual adaptive automation, automated design of spacecraft systems, some robotics applications, and decision support system for health management

AHRQ: Continue health information technology patient safety/quality improvement program including focus on reducing medical errors in ambulatory care settings and promoting safe use of medications, personal safety, and care delivery that achieves the highest-quality outcome; patient safety health-care IT data standards program; and rural/non-rural/regional projects including health information exchange and state information networks.

NIST: Evaluation and standards for biometrics including fingerprint, face recognition, multimodal biometrics for identification and verification; evaluation methodology for multimedia, including video retrieval, motion image quality, video analysis, and content extraction and standards for multimedia (MPEG-7, JPEG); usability of interactive systems and user interfaces for mobile robots, human-robot interaction (HRI); usability and accessibility of voting systems; standards for software usability reporting, IT accessibility; measuring performance of smart systems; ontologies for information integration in manufacturing, commerce; developments in the semantic Web and health-care informatics

NOAA: Technologies for disseminating weather and climate data in multiple formats to professionals, academia, and the public; management of very large datasets, use of metadata, and development of decision support tools for knowledge discovery and data display

EPA: Tools and approaches exploring potential linkages between air quality and human health; integration of search and retrieval techniques across environmental and health libraries; evaluation and investigation of the distribution, integration, management, and archiving of models and datasets

NARA: Advance decision support technologies contributing to high-confidence processing of large collections (e.g., collections of Presidential records)

Large Scale Networking (LSN)

NITRD Agencies: NSF, **OSD**, NIH, DARPA, DOE/SC, NSA, NASA, AHRQ, NIST, DOE/NNSA, NOAA
Other Participants: USGS

LSN members coordinate Federal agency networking R&D in leading-edge networking technologies, services, and enhanced performance, including programs in new architectures, optical network testbeds, security, infrastructure, middleware, end-to-end performance measurement, and advanced network components; grid and collaboration networking tools and services; and engineering, management, and use of large-scale networks for scientific and applications R&D. The results of this coordinated R&D, once deployed, can assure that the next generation of the Internet will be scalable, trustworthy, and flexible.

President's 2007 Request

Strategic Priorities Underlying This Request

Large-scale data transfers: Enable near-real-time petabyte and above data transfers, by 2008, to support science cooperation and modeling in high-energy physics, bioinformatics, weather, astrophysics, and other areas, overcoming scalability limitations of current technology and the Internet Protocol (IP)

New architectures: Develop future Internet architectures that are flexible, trustworthy (secure, reliable, ensuring privacy), and able to support pervasive computing using wireless access and optical light paths, networked sensors, and innovative applications (e.g., applications on the fly and large-scale information dissemination)

End-to-end performance measurement: Develop visibility into the interior of networks to enable optimization of application performance over networks; implement standard measurement boxes, standard protocols, and cooperation across domain boundaries to allow end-to-end application performance tuning

Highlights of Request

Optical network testbeds (ONTs): NSF's CHEETAH and DRAGON networks, DOE/SC's UltraScience Net; coordinate with OMNInet, OptiPuter, NationalLambda Rail, and regional ONTs; develop GMPLS, QoS, agile circuit-switching, and interdomain control plane protocols, tools, services, and management (e.g., resource reservation, security) – DARPA, DOE/SC, NASA, NSF

Innovative network architectures: Global Environment for Network Investigations (GENI) support of R&D for a large-scale testbed for new scalable, flexible, usable new Internet architectures – NSF with DARPA, DOE/SC, NASA, NIST

Network security research: Provide more trustworthy networking – DARPA, DHS, DOE/SC, NSF, NIST, **OSD**

End-to-end agile networking, QoS, GMPLS: Develop robust capability and technologies to provide on-demand networking and assured bandwidth for advanced networking applications – DARPA, DOE/SC, NASA, NSF, other agencies

Wireless and sensor networking: Advance capabilities for highly distributed, ubiquitous networking – DARPA, NIST, NSF, other agencies

Large-scale data flows: Infiniband and single-stream flows over WANs – DOE/SC, NASA, NSF, **OSD (NRL)**

High-speed transport protocols: Develop protocols to move massive amounts of data – DOE/SC, NSF

IPv6 and cyber security implementation: Rollout of IPv6 into research networks in response to OMB requirements – All

End-to-end network performance monitoring and measurement: Identify intrusions and bottlenecks and isolate faults – DARPA, DOE/SC, NSA, NSF, **OSD**

Network backup: Provide alternative capacity during network outages, stress, or national crises – DOE/SC, NASA, **OSD**

International coordination: Leverage investments in federated security regimes and optical networking transparency – DOE/SC, NSF

Planning and Coordination Supporting Request

Co-funding: NSF networking research projects receive support from DARPA, DOE/SC, NSA, DHS

Workshops: Annual government/private sector ONT workshops to provide input into coordinated Federal activities for R&D and promote technology transfer; NSF GENI workshops to coordinate research on new architectures, experimental infrastructure, and control plane technology; academia/industry/government workshop to identify networking R&D needs – Multiple agencies

Coordination by LSN Teams:

- **Joint Engineering Team (JET):** DOE/SC, NASA, NIH, NIST, NOAA, NSA, NSF, **OSD**, USGS, with participation by academic organizations (CAIDA, CENIC, Internet2, MAX, NLANR, StarLight), national labs (ANL, PSC), research organizations (ISI), supercomputing centers (ARSC, MCNC), universities (FIU, IU, UIC, UMd, UNC, UW), and vendors – ONTs; engineering research networks (JETnets); security best practices; applications testbeds (IPv6, IPv6 multicast, performance measurement); metrics and monitoring: interdomain, end-to-end, internal network visibility; tool sharing and data exchange; 9,000-byte MTU recommendation; international coordination; transit and services cooperation
- **Middleware and Grid Infrastructure Coordination (MAGIC) Team:** DOE/SC, NIH, NIST, NOAA, NSF, with participation by academic organizations (EDUCAUSE, Internet2), national labs (ANL, LANL, LBL, PNL), research organizations (ISI, UCAR), universities (UIUC, UMd, UNC, UWisc), and vendors – Middleware and grid tools and services; applications; coordinated certificate authorities for security and privacy; collaboration infrastructure; standards development; international coordination (e.g., federated certificate authorities under Americas Policy Management Authority)
- **Networking Research Team (NRT):** DARPA, DOE/SC, NASA, NIST, NSA, NSF – Basic research (technology and systems); prototyping and testing of optical networks (dynamic provisioning, GMPLS-based control plane); applications; wireless, nomadic (ad hoc, mobile) networking; education and training

Information exchange: Multiagency LSN participation in review panels, informational meetings, principal investigator (PI) meetings; tactical coordination among program managers with common interests; coordination of JET meetings with DOE ESSC and Internet2 Joint Techs Meetings; GMPLS forum coordinating development of interdomain signaling in agile optical networks

Additional 2006 and 2007 Activities by Agency

NSF: Support university-based fundamental networking research in trust, pervasive computing; innovative research in architectures, algorithms, protocols, sensor network programming, hardware/software, and privacy/security; programmable wireless networks; network measurement; CAREER awards for networking research; infrastructure research (create, test, harden next-generation systems); middleware development and dissemination

OSD (HPCMPO): IP end-to-end performance measurement, network monitoring tools, IPv6 pilots and IPv6 multicast, network security (IPsec, VPN portals, attack detection tools, filters, encryption), automated management, disaster recovery planning, research network broadband access to Hawaii and Alaska

NIH: R&D on data and computational grids in support of biomedical research, including Biomedical Informatics Research Network (BIRN) and cancer Biomedical Informatics Grid (caBIG); focus on QoS, security, medical data privacy, network management, and collaboratory infrastructure technologies

DARPA: Network-aware control plane; connectionless sensor networks minimizing energy consumption; Situation-Aware Protocols In Edge Network Technologies (SAPIENT); optical data router for >100 Tbps bandwidth

DOE/SC: Middleware and network research (security, data management, standards-based protocols, advanced reservation and scheduling); Open Science Grid (operational infrastructure for large-scale applications); UltraScience Net (research and engineering prototype); connectivity (ESnet, MANs, collaboration services, trust federations and authentication services)

NSA: Internet measurement; wireless networks (ad hoc sensor networks, wireless capacity enhancement, wireless in noisy environments, WLAN QoS, WLAN/WAN simulation); GMPLS evolution for optical networks

NASA: Real-time interactive and grid applications; Columbia supercomputer networking support; network security, data distribution, and real-time visualization

NIST: Internet infrastructure protection, quantum information networks, health-care networks, criminal-justice information systems, wireless ad hoc networks, public safety communications; standards and guidelines for management and assistance; and process control systems protocols and security

NOAA: Advanced networking infrastructure, including lambda-based networking, IPv6, distributed Web servers; computer and network security; applications (collaboration, grid computing (e.g., for storm-scale simulations), wireless, remote operation)

High Confidence Software and Systems (HCSS)

NITRD Agencies: NSF, **OSD**, NIH, DARPA, NSA, NASA, NIST

Other Participants: USASMD/ARSTRAT, DHS, DOE (OE), FAA, FDA

The goal of HCSS R&D is to bolster the Nation's capability and capacity for engineering effective and efficient distributed, real-time, IT-centric systems that are certifiably and inherently dependable, reliable, safe, secure, fault-tolerant, survivable, and trustworthy. These systems, which are often embedded in larger physical and IT systems, are essential for the operation and evolution of the country's national defense, key industrial sectors, and critical infrastructures.

President's 2007 Request

Strategic Priorities Underlying This Request

Demand for new classes of computationally enabled, adaptive, distributed, embedded, and real-time systems for mission- and safety-critical applications. Research is needed to develop:

Next-generation capabilities: Complex new capabilities and foundations for advances in physical and engineered systems for Federal missions and U.S. industrial innovation in key areas such as:

- **Aerospace systems:** Aircraft autonomy, future airspace operations, human-rated space systems
- **Automotive systems:** "Drive-by-wire" and intelligent vehicle and highway systems
- **Critical infrastructure systems:** Beyond supervisory control and data acquisition [SCADA], power grid automation, water management, supply chain integration
- **Defense systems:** Real-time, distributed, embedded [RDE] systems in a highly network-centric environment for applications ranging from counterterrorism to ballistic and cruise missile defense
- **Medical care:** "Operating room of the future," telemedicine, medical devices, paramedic support systems)

New high-confidence enabling technologies: Revolutionary paradigms to replace today's operating systems (OSs), middleware (MW), and virtual machines (VMs) that integrate complex mechanisms and enable fault tolerance, dynamic adaptation, partitioning for fault isolation, real-time scheduling, and security

Assurance for complex, integrated systems: New systems built on a principled framework and a new computing technology base for integrating assured concepts that can replace today's inadequate technologies, which were designed for benign environments and noncritical applications and are underpinned by a fragmented collection of theories. Priority research topics include:

Scientific foundations: Software and systems assurance

Design and engineering advances: Model-based system design, formal methods, correct-by-construction techniques, and tools for designing, testing, verifying, and validating systems with software as key components, in part to expand the types of software-intensive systems that can be confidently deployed

Assurance measures and metrics: Ability to justify the degree of confidence in established properties

Highlights of Request

High-confidence, real-time operating systems (RTOS), MW, and VMs: Continue examination of the adequacy of current real-time OS, MW, and VM technologies to identify R&D needed to achieve a next generation high-confidence RTOS technology base; foster university/industry/government R&D partnership; launch a multiagency effort in high-confidence RTOS software, systems, and assurance technologies – NSF, NSA, NIST, **OSD (ODDR&E)**, AFRL, with NASA, DOE (OE), FAA, FDA, **OSD (ONR)**

Science of Design (SoD): Basic research in design of software-intensive systems that imports and adapts creative scientific ideas from other design fields (e.g., engineering, urban planning, economics, the arts) – NSF

Assured information systems: R&D toward an intelligent, secure flexible, self-protecting global infrastructure; robust protection mechanisms to support sharing of information across diverse communities; development of safe computing platforms that can securely isolate, measure, and attest to correct operations; cryptographic algorithms and engineering to protect the content of information systems – NSA

Verification Grand Challenge: Develop deployable high-assurance technologies for large-scale software systems; begin by convening panels of specialists (i.e., integrated verification systems, theory, system certification) to identify research directions, propose action plan, and suggest projects – NSA, NSF

Deployed and near-term SCADA and industrial control systems: Develop requirements, standards, software assurance metrics, and guidelines – NIST, DHS

Software assurance metrics, tools, evaluation, and databases – NIST, NSA, DHS***Planning and Coordination Supporting Request***

High-confidence RTOS technology needs assessments and national roadmapping workshop: Non-disclosure briefings by technology development and systems integration vendors, academic researchers, and RTOS standards organization; initiate university/industry/government collaboration; convene workshop(s) to roadmap RTOS R&D – NSF, NSA, NIST, **OSD (AFRL)**, with NASA, DOE (OE), FAA, FDA, **OSD (ONR)**

High Confidence Medical Device Software and Systems: Ongoing national workshop series – NSF, NSA, with NIST, FDA

Software for Critical Aviation Systems: Begin national workshop series – NSF, NSA, AFRL, with NASA, FAA

Beyond SCADA and Distributed Control Systems: Begin national workshop series on high-confidence devices and software to enable, protect, and evolve critical infrastructures – NSF, NIST, NSA, **OSD (ODDR&E)**, with **OSD (AFRL)**

Black boxes for medical devices: Preliminary study of the benefits of building data recording technologies into medical device systems to provide complete detailed records about their operation for analysis of processes and state prior to and during failures – NSF, with FDA

Open-source software for high-confidence medical devices: Exploration of future directions and practices for certification – NIH, NSF, FDA, other agencies

Sixth annual HCSS conference – NSA, with other HCSS agencies

National Voluntary Lab Accreditation Program (NVLAP): calibration and/or test methods, protocols, and standards to meet accreditation needs for a variety of products and processes – NIST, NSA

Software Assurance Metrics and Tool Evaluation Workshops: Bring together users, developers of software assurance tools, compare effectiveness of tools and techniques, develop taxonomies of vulnerabilities and tools, and expand a software security assurance standard reference database – NIST, DHS, with other agencies

Sufficient Evidence? Building Certifiably Dependable Systems: Complete National Academies/CSTB study assessing current practices for developing and evaluating mission-critical software, including assurance for medical devices and aviation systems – NSA, NSF, FAA, **OSD (ONR)**, with DARPA, NASA, NIST, **OSD (ARO)**, FDA

Additional 2006 and 2007 Activities by Agency

NSF: Fundamental research in distributed, real-time, and embedded systems; operating systems; hybrid discrete and continuous control systems; formal methods for composition and verification; rigorous models of computation; compositional software methods; critical infrastructure component of Cyber Trust

OSD (AFRL): Technology for affordable, safe software; certification technologies for advanced flight-critical systems project; high-confidence design of distributed, embedded systems; advocate high-assurance security architecture for embedded systems

OSD (ODDR&E): Software Engineering Institute research – designs for networked systems that recognize, resist, and recover quickly from attacks; quality attribute reasoning; software architectures and practices that enable automated support, predict runtime behavior of software, and select software components based on certified properties and predicted contribution to assembly behavior; principles, methods, techniques for integration and interoperation across components, systems, systems of systems; model-based software engineering for real-time systems; methods for evidence-based assurance

NASA: Exploration systems – tools and techniques that support cost effective development and verification for autonomous and adaptive systems; aeronautics research – enabling technologies for integrated vehicle health management, integrated intelligent flight deck, and integrated resilient aircraft control sub-elements

NIST: Software diagnostic and conformance tests, tools, and methods; source code analysis tools; National Software Reference Library; voting accuracy standards; software engineering method development

FAA: Certifiably dependable systems, including software certification and incremental certification in traditional safety-critical systems; enhanced methods and standards for engineering security into products and improved continuous external monitoring of a system's internal vital signs; improved continuous security risk assessment in complex networked environment

FDA: Formal-methods-based design, including safety models, forensics, and design for infusion pumps, and blood bank regulatory policy models and certification; architecture, platform, middleware, and resource management, including plug-and-play in the operating room of the future

Social, Economic, and Workforce Implications of IT and IT Workforce Development (SEW)

NITRD Agencies: NSF, NIH, DOE/SC, DOE/NNSA

Other Participants: GSA

The activities funded under the SEW PCA focus on the nature and dynamics of IT and its implications for social, economic, and legal systems as well as the interactions between people and IT devices and capabilities; the workforce development needs arising from the growing demand for workers who are highly skilled in information technology; and the role of innovative IT applications in education and training. SEW also supports efforts to speed the transfer of networking and IT R&D results to the policymaking and IT user communities at all levels in government and the private sector. A key goal of SEW research and dissemination activities is to enable individuals and society to better understand and anticipate the uses and consequences of IT, so that this knowledge can inform social policymaking, IT designs, the IT user community, and broadened participation in IT education and careers.

President's 2007 Request

Strategic Priorities Underlying This Request

Interactions between IT and society: Develop new knowledge about and understanding of the implications of new technologies for economic, social, and technical systems, and their dynamic interactions

Public policy: Sponsor activities that bring SEW researchers and research findings together with policymakers to foster informed decision making

Federal information sharing: Implement a Data Reference Model for information sharing as part of the Federal Enterprise Architecture and e-government initiatives

Government IT practitioner communities: Build communities of practice across all levels of government and private-sector organizations in which practitioners, with support from researchers, can work collaboratively on issues associated with implementing emerging technologies to improve government services

IT education and training: Support innovative educational approaches to broadening participation in IT careers, and doctoral and post-graduate programs to expand the highly skilled workforce in such fields as bio-informatics and computational science

Highlights of Request

Ecology of IT: New program emphasizes on understanding the ecology of IT, knowledge creation, innovation, and intellectual property issues; information privacy and other human-centered computing priorities; continue broadening participation by underserved communities in IT activities – NSF

Computational Science Graduate Fellowship Program: Continue support for advanced computational science training activity at national laboratories – DOE/NNSA, DOE/SC

Collaborative Expedition Workshops: Continue monthly series of open workshops exploring cost-effective implementations of emerging technologies in delivery of public services at all levels of government, establishing “communities of practice” among IT implementers across government and the private sector, and evaluating Data Reference Model for interoperable Federal information sharing – CIO Council, GSA, NSF, with SEW

Planning and Coordination Supporting Request

SEW functions as a crossroads between the IT R&D community and the larger arena of policymakers and IT implementers. SEW has developed a partnership with GSA and the Federal Chief Information Officers (CIO) Council that sponsors a monthly open workshop series – the Collaborative Expedition Workshops – to encourage collaboration among government and community implementers of IT and to demonstrate promising IT capabilities emerging from Federal research. NSF co-sponsors these events and invites researchers to give academic talks on selected topics in an attempt to bridge gaps between research and policy. The workshops draw participants from Federal, state, and local government, nongovernmental organizations, IT researchers, and IT developers. The focus is on emerging technologies for applications in such areas as emergency preparedness and

response, environmental protection, public health and health care systems, government information services for citizens, and agency projects under the Administration's Federal Enterprise Architecture e-government initiative. Examples of current activities include:

Communities of Practice (COPs): As of 2006, a dozen COPs have been established, including the Data Reference Model Forum, the Federal Data Repository Users Group, the Government Semantic Interoperability COP, Grants.gov COPs, a geospatial COP, the Interoperable Manufacturing COP, and the National Infrastructure for Community Statistics COP

Workshop co-sponsorship: Expedition Workshop held in early FY 2006 on information integration in environments with complex legal and access issues co-sponsored by the HCI&IM Coordinating Group; other collaborations planned in FY 2006

Additional 2006 and 2007 Activities by Agency

NSF: Continue SEW-related R&D initiated under ITR and core research and education programs; socio-technical issues in intelligence informatics; computing education and the IT workforce; collaborations with the European Commission Information Society and Media Programme; expand opportunities for innovative education and curriculum development projects; participate in human and social dynamics program

NIH: Graduate and postdoctoral fellowship programs in bioinformatics

GSA: Explore emerging standards and technologies that improve interoperability, ease of use, and cost-effectiveness of Federal IT implementations; foster open COPs around application of emerging technologies to improve government services

Software Design and Productivity (SDP)

NITRD Agencies: NSF, **OSD**, NIH, DARPA, NASA, NIST, DOE/NNSA, NOAA

Other Participants: FAA

SDP R&D will lead to fundamental advances in concepts, methods, techniques, and tools for software design, development, and maintenance that can address the widening gap between the needs of Federal agencies and society for usable and dependable software-based systems and the ability to produce them in a timely, predictable, and cost-effective manner. The SDP R&D agenda spans both the engineering components of software creation (e.g., development environments, component technologies, languages, tools, system software) and the economics of software management (e.g., project management, schedule estimation and prediction, testing, document management systems) across diverse domains that include sensor networks, embedded systems, autonomous software, and highly complex, interconnected systems of systems.

President's 2007 Request

Strategic Priorities Underlying This Request

Improved software development methods: The overall cost – in time, money, and labor – of developing, upgrading, and maintaining software is the most difficult problem in IT deployment. Assuring the correct functionality, reliability, and security of products and processes that include software adds costs and delays implementation. SDP R&D focuses on cost-effective methods to solve these problems, which undermine overall advancement of IT capabilities. Priorities include:

- **Frameworks and environments:** Frameworks and environments that enable agencies to more efficiently develop and certify high-quality software that is critical to Federal agency missions
- **Next-generation software engineering tools and techniques:** New approaches that reduce the cost, risk, and difficulties of software development; increase the reliability, security, interoperability, scalability, and reusability of software components; and enable software validation and verification

Seamless content interoperability: Software capabilities that enable diverse IT systems, software applications, and networks to exchange and use large volumes of data accurately, effectively, and consistently, both among agencies and between government and the private sector (e.g., data sharing by NASA, NOAA, and DOE/SC across the many interacting modules in the Earth System Modeling Framework (ESMF); availability of HHS electronic health records for doctors, hospitals, and others in the health care industry; and DHS information sharing with 50,000 public-safety agencies)

Highlights of Request

Science of Design (SoD): Make creative scientific advances in the design of software-intensive systems through foundational ideas and theories, including approaches from other design fields; produce intellectually rigorous, analytical, formalized, and teachable body of design knowledge from empirical studies – NSF

Biomedical modeling tools: Develop and disseminate tools to enhance computational modeling of biological, biomedical, and behavioral sciences at scales ranging from the molecular to large populations – NSF, NIH

Collaborative research in computational neuroscience: Provide a theoretical foundation and technological approaches for enhancing understanding of nervous system function through analytical and modeling tools that describe, traverse, and integrate different organizational levels and span broad temporal and spatial scales and multiple levels of abstraction – NIH, NSF

Dynamic Data-Driven Applications Systems (DDDAS): Develop ability to dynamically incorporate additional data into executing applications and enable applications to dynamically steer the measurement process, creating new capabilities in a wide range of science and engineering areas – NSF, NIH, NOAA

Software technology transfer: Embedded Systems Consortium for Hybrid and Embedded Research (ESCHER) for transitioning government-sponsored research results into mainstream or commercial use, including through a quality-controlled software repository – DARPA, NSF

Interoperable biology databases: Develop data standards and ensure interoperability of Internet-based databases important to biotechnology, with emphasis on structural biology – DOE/SC, NIH, NIST, NSF

Software producibility: 2006 new start in building, assuring functionality of, managing, and sustaining software, including net-centric and systems of systems – **OSD**

Common software infrastructure for climate modeling: ESMF collaboration on building high-performance, flexible software infrastructure to increase ease of use, performance, portability, interoperability, and reuse in climate modeling, numerical weather prediction, data assimilation, and other Earth science applications – NASA, NOAA, DOE/SC

Open-source software: Research that enables users to read, modify, and redistribute source code, fostering more efficient development and increased collaboration to improve software quality – NSF, OSD

Planning and Coordination Supporting Request

Software interoperability workshop: To identify barriers to interoperability, centering on challenge problems whose solution requires new interoperability techniques – SDP CG

Large-scale implementation issues: Briefings by Federal IT user agencies with critical requirements for large-scale software applications to identify development issues and software engineering techniques – SDP CG

Software producibility: National Academies study – OSD, NSF

Additional 2006 and 2007 Activities by Agency

NSF: Software design methods; tools for software testing, analysis, and verification; semantics, design, and implementation of programming languages; scalable software architectures; techniques for handling complex combinations of requirements such as meeting real-time constraints and coordinating control in an embedded, failure-prone environment; compiler and runtime techniques for developing and controlling the execution of complex, dynamically changing applications; requirements for the design and construction of successful-by-design information systems; emphasis on interoperability, robustness, reliability, programmer productivity, maintainability, and software-intensive systems

OSD (HPCMPO): Applications software development in areas such as physics-based design, modeling, simulation, testing; institutes on battlespace topics; PET program tools and techniques for benchmarking, remote visualization, debugging and optimization, interactive computing environments for large datasets

NIH: National Centers for Biomedical Computing (NCBCs) to develop, disseminate, and train users of biomedical computing tools and user environments; encourage collaboration between big and small science at NCBCs; create and disseminate curriculum materials to embed quantitative tools in undergraduate biology education; cancer imaging and computational centers; modeling of infectious disease; bioinformatics resource centers for emerging and re-emerging infectious disease; proteomics and protein structure initiatives; interagency opportunities in multiscale modeling in biomedical, biological, and behavioral systems; individual grants in such topics as simulation and informatics, imaging tools

NIST: Integrated design, procurement, and operation through software interoperability; automated generation of test suites for integration standards; digital library of mathematical functions; ontology for mathematical functions; supply chain software interoperability; international testbed for business-to-business solutions; interoperability of databases for bioinformatics, chemical properties, properties of inorganic materials, and neutron research; ontological approaches to automate integration of supply chain systems; Units Mark-up Language; interface standards for manufacturing control systems; product representation scheme for interoperability among computer-aided engineering systems; standards for exchange of instrument data and chemical reference data; ontological methods for representation and exchange of mathematical data

DOE/NNSA: Provide a production-level, computational environment for ASC platforms, encompassing development tools, visualization and data analysis software, and networking and storage capabilities

FAA: Development of secure, dependable software-based systems in a timely, predictable, and cost-effective manner

NOTE: Budget table numbers are final, pending OMB review
Agency NITRD Budgets By Program Component Area

FY 2006 Budget Estimates
and
FY 2007 Budget Requests
(Dollars in Millions)

Agency		High End Computing Infrastructure & Applications (HEC I&A)	High End Computing Research & Development (HEC R&D)	Cyber Security & Information Assurance ¹ (CSIA)	Human-Computer Interaction & Information Management (HCI &IM)	Large Scale Networking (LSN)	High Confidence Software & Systems (HCSS)	Social, Economic, & Workforce (SEW)	Software Design & Productivity (SDP)	Total
NSF	2006 Estimate	220.3	62.7	57.6	207.4	82.2	41.3	91.1	47.9	810.3
	2007 Request	272.4	64.1	67.6	220.9	84.0	51.3	92.9	50.7	903.7
OSD ^{2,3}		214.6	9.8	0.6	138.5	141.8	31.2	0.2	6.9	543.7
		186.0	8.7	0.7	135.6	130.7	29.1	0.3	6.8	497.8
NIH ⁴		198.5			188.7	74.9	8.4	12.3	17.9	500.6
		194.7			183.2	74.6	8.3	12.2	17.7	490.7
DARPA ³			94.1	78.7	174.2	21.3				368.3
			117.7	81.6	233.2	33.2				465.7
DOE/SC ⁵		104.4	109.1			38.9		3.5		255.8
		135.3	160.4			45.0		4.0		344.7
NSA ³			89.2	14.1		1.0	36.2			140.5
			62.4	13.3		2.3	39.9			117.9
NASA		60.3		1.3	2.0	5.7	7.0		1.8	78.1
		63.9		1.3	2.0	6.0	7.0		1.8	82.0
AHRQ ⁴					40.1	21.6				61.7
					37.3	20.0				57.3
NIST ⁶		2.3	1.2	9.1	7.8	4.3	9.6		4.6	38.9
		2.3	1.2	11.1	9.8	4.3	9.6		4.6	42.9
DOE/NNSA ⁵		10.0	15.9			1.6		4.6	3.3	35.4
		9.5	23.4			1.6		4.6	2.8	41.9
NOAA ⁶		11.4	1.9		0.2	0.7			1.6	15.8
		16.4	1.9		0.5	2.9			1.6	23.3
EPA		3.3			3.0					6.3
		3.3			3.0					6.3
TOTAL (2006 Estimate)		825.0	383.9	161.3	761.9	393.9	133.6	111.6	84.0	2,855
TOTAL (2007 Request)		883.8	439.9	175.5	825.4	404.5	145.2	114.0	85.9	3,074

- ¹ The CSIA PCA budget should not be viewed as the total Federal investment in cyber security R&D. This figure includes only reporting for NITRD member agencies; it does not include investments at other agencies that support cyber security R&D, including DHS, DOJ, TSWG, non-NITRD-member organizations within DOE, and others. Furthermore, funding categorized under the HCSS PCA includes investments in various areas associated with secure and trustworthy systems. These investments are classified under HCSS – a PCA that has historically been part of the NITRD Program – but would be considered to fall within the generic scope of cyber security R&D if HCSS did not exist as a separate PCA.
- ² The OSD budget includes for the first time this year funding from the DoD Services (Air Force, Army, Navy) as well as DoD's High Performance Computing Modernization Program Office (HPCMPO). Total NITRD budgets for the DoD services are as follows: Air Force – \$133 million (2006 estimate) and \$139 million (2007 request); Army – \$141 million (2006 estimate) and \$120 million (2007 request), and Navy – \$35 million (2006 estimate) and \$33 million (2007 request). NITRD-related R&D budgets for the HPCMPO are \$203 million (2006 estimate) and \$174 million (2007 request).
- ³ Combined OSD, DARPA, and NSA agency totals supersede the Department of Defense total appearing in the President's 2007 Budget. Discrepancies result from rounding and late shifts in budget accounting.
- ⁴ Combined NIH and AHRQ agency totals supersede the Department of Health and Human Services total appearing in the President's 2007 Budget. Discrepancies result from rounding and late shifts in budget accounting.
- ⁵ Combined DOE/SC and DOE/NNSA agency totals supersede the Department of Energy total appearing in the President's 2007 Budget. Discrepancies result from...
- ⁶ Combined NIST and NOAA agency totals supersede the Department of Commerce total appearing in the President's 2007 Budget. Discrepancies result from rounding and late shifts in budget accounting.

NITRD Program Budget Analysis

Fiscal Year Overview for 2006-2007

In general, differences between the President's Budget request for a given year and estimated spending for that year reflect revisions to program budgets due to evolving priorities, as well as Congressional actions and appropriations. While budget information reported on the preceding page includes such variations, several additional factors specific to the NITRD Program have led to substantial differences between the 2006 budget request and 2006 estimated spending. These include the addition of the CSIA PCA to the NITRD Program, new reporting of activities in response to evolving definitions of NITRD PCAs, and the addition of reporting from organizations that had participated in coordinated NITRD activities but had not previously been included in the NITRD budget crosscut. For example, the DoD services (Air Force, Army, and Navy) have been added to OSD's reporting. In addition, efforts at several agencies to improve the classification and characterization of agency activities have resulted in noteworthy changes in budget reporting ranging from additional reporting or removal of out-of-scope investments to shifts of funds between PCAs.

2006 Summary

The estimated 2006 NITRD budget is \$2.86 billion, which is a \$0.70 billion increase over the \$2.16 billion 2006 request. Of this increase, approximately \$0.07 billion represents actual increases in spending above 2006 requested funds. The remaining \$0.63 billion increase is the combination of an additional \$0.18 billion in newly reported funding due to the addition of the CSIA PCA and evolving PCA definitions, an increase of \$0.31 billion due to the addition of the DoD Services to OSD's reporting, an additional \$0.22 billion reported by other organizations that did not previously report funds in the NITRD budget, and a reduction of \$0.08 billion due to improved classification and characterization of agency activities.

Changes to NITRD agency budgets are explained in detail in the Analysis by Agency section below. Due to these changes, the 2006 budget request published in last year's NITRD Budget Supplement no longer provides an effective baseline for comparison to the 2007 request and future budgets.

2007 Summary

The 2006 estimates and the 2007 budget requests in the table on the preceding page include reporting from the same agencies and make use of the same scope, definitions, and classification of investments. Thus, the 2006 estimates serve as an appropriate baseline for comparison with the 2007 requests and future budgets.

The President's 2007 Budget request for the NITRD Program is \$3.07 billion, an increase of \$0.21 billion over the \$2.86 billion 2006 estimate. The 2007 budget requests funding increases above 2006 estimated spending for all eight NITRD PCAs. The high-end computing PCAs account for slightly more than half of the increase, and the HCI&IM PCA accounts for approximately another quarter of the increase.

The Administration's recently announced American Competitiveness Initiative has had a positive influence on NITRD budgets for agencies that are part of the Initiative. The Initiative calls for a doubling over 10 years of the investment in key Federal agencies that support basic research programs in the physical sciences and engineering. These agencies – NSF, DOE/SC, and NIST – are NITRD Program member agencies. All three received 2007 NITRD budget increases that exceed the percentage increase in the overall Program budget, as follows: NSF, 12 percent; DOE/SC, 35 percent; and NIST, 10 percent. The aggregated NITRD budget increase for these three agencies from 2006 estimates to 2007 request is \$186 million (17 percent above 2006 estimates), which accounts for over 85 percent of the overall NITRD Program budget increase for 2007.

NITRD Program Budget Analysis by Agency

The following NITRD Program budget analysis by agency summarizes 2006 estimates and 2007 requests for each NITRD agency and provides explanations of significant⁷ changes in budget – either differences between 2006 requested funding and 2006 estimated spending or changes between 2006 estimated spending and 2007 requests.

⁷ For the purpose of this analysis, budget differences that exceed \$10 million for an agency within a single PCA are considered "significant" enough to warrant explicit explanation. For agencies with smaller overall NITRD budgets, explanations are provided for differences that account for significant percentages of an agency's PCA budget, even in instances where those changes are smaller than \$10 million.

Budget numbers are rounded to the nearest million in the discussions that follow, and may result in minor discrepancies in sums due to rounding.

NSF

Comparison of 2006 request (\$803 million) and 2006 estimate (\$810 million): The increase in HEC I&A is due largely to pooling 2005 and 2006 funding to increase the size of a planned HEC system acquisition. Some HEC R&D funding has been moved to HEC I&A to better reflect the nature of work being done under certain HEC grants. HEC funding for work related to the collection and management of large datasets resulting from HEC applications has been moved to HCI&IM. The increase in HCI&IM is also due to increased R&D for better management of scientific data, as part of NSF's cyberinfrastructure investments. HCSS shows a decrease because some funding previously reported in HCSS is now reported under CSIA; however the sum of the CSIA and HCSS budgets has increased by \$23 million due to greater investment in related areas. This increase is offset by decreases in the LSN and SDP budgets.

Comparison of 2006 estimate (\$810 million) and 2007 request (\$904 million): HEC I&A increases \$52 million to support the acquisition of a petascale leadership-class HEC system. HCI&IM increases \$14 million for cyberinfrastructure-related data and information management R&D. CSIA and HCSS each increase \$10 million, reflecting continued emphasis on Cyber Trust and related high-confidence and information assurance research activities.

OSD

Comparison of 2006 request (\$23 million) and 2006 estimate (\$544 million): The increase in the two HEC PCAs is primarily due to the addition of the High Performance Computing Modernization Program Office (HPCMPO) (which has been participating in HEC coordination on an ongoing basis) to NITRD Program reporting, with a small additional contribution due to the addition of the DoD Services to OSD's reporting. The reporting of funding in HCI&IM is due to the addition of the DoD Services to OSD's reporting, as is nearly all of the funding reported in LSN. To more accurately reflect the nature of the work being performed by the Software Engineering Institute, the \$18 million investment associated with this work was shifted from the SDP budget to the HCSS budget. The remaining increases in these two PCA budgets are due to the addition of the DoD services to OSD's reporting.

Comparison of 2006 estimate (\$544 million) and 2007 request (\$498 million): The reduction in the HEC I&A budget is the result of reductions to the HPCMPO budget, as part of broader DoD funding reallocations. The reduction in the LSN budget is the result of reductions to the Army budget, as part of broader DoD funding reallocations.

NIH

Comparison of 2006 request and 2006 estimate (both \$501 million): Nearly all NIH investments previously reported as HEC R&D have been reclassified as HEC I&A. This and other movements of funds from one PCA to another do not represent changes in programmatic investments, but have been made to better align the reporting of NIH investments with the definitions of the NITRD PCAs.

Comparison of 2006 estimate (\$501 million) and 2007 request (\$491 million): The overall agency budget reflects a two percent reduction in the NIH NITRD budget.

DARPA

Comparison of 2006 request (\$176 million) and 2006 estimate (\$368 million): The \$13 million increase in the HEC R&D budget reflects the inclusion of the Architectures for Cognitive Information Processing program. The addition of the CSIA PCA to the NITRD Program resulted in \$79 million of new reporting. The evolving definition of HCI&IM led to \$100 million of new funding reported for that PCA, for DARPA's Learning, Reasoning and Integrated Cognitive Systems programs.

Comparison of 2006 estimate (\$368 million) and 2007 request (\$466 million): The \$24 million increase in HEC R&D is for Phase III of the High Productivity Computing Systems program. The \$59 million increase in HCI&IM is due to increases in DARPA's language translation programs. The \$12 million increase in LSN is the result of scaling up cognitive networking activities for technical demonstrations and testbeds with the military services.

DOE/SC

Comparison of 2006 request (\$227 million) and 2006 estimate (\$256 million): The \$27 million increase in HEC R&D is to support development of a HEC Leadership Computing Facility at Oak Ridge National Laboratory.

Comparison of 2006 estimate (\$256 million) and 2007 request (\$345 million): The \$31 million increase in HEC I&A is to enhance SciDAC partnerships to deliver applications for petascale computing systems in areas critical to DOE missions and complementary investments to expand high-performance computing capacity at NERSC. The \$51 million increase in HEC R&D is for enhancements to the Leadership Computing Facility including investments at ORNL and investments at ANL in low power density leadership-class computing, which were a part of the original competitively selected Leadership Computing Facility proposal.

NSA⁸

Comparison of 2006 request (\$101 million) and 2006 estimate (\$141 million): HEC R&D increased \$52 million to accelerate Black Widow and Eldorado system investments; a \$12 million reduction in HCSS investments helped offset this increase. The decrease in the HCSS budget is also due to a shift in reporting of \$14 million of investments to the new CSIA PCA.

Comparison of 2006 estimate (\$141 million) and 2007 request (\$118 million): With accelerated investments in 2006, Black Widow R&D will be largely completed, reducing funding required in 2007.

NASA

Comparison of 2006 request (\$74 million) and 2006 estimate (\$78 million): HEC I&A increased \$7 million due to Columbia high-end computing system costs being higher than initially estimated. A shift to agency-wide management of HEC investments adds an additional \$19 million of investments at Goddard Space Flight Center to HEC I&A. Reductions in HCI&IM, LSN, and HCSS are due to NASA's continuing transformation to focus on R&D aimed at implementing its Vision for Space Exploration.

Comparison of 2006 estimate (\$78 million) and 2007 request (\$82 million): NASA's budget remains relatively stable from 2006 to 2007.

AHRQ

Comparison of 2006 request (\$68 million) and 2006 estimate (\$62 million): AHRQ's LSN budget decreases due to reductions in research on privacy and security law, and in health information exchanges at the state level in support of large-scale exchanges of health information at regional and national levels.

Comparison of 2006 estimate (\$62 million) and 2007 request (\$57 million): Beginning in 2007, the HHS will take the lead on data standards interagency agreements, resulting in some of the \$10 million that AHRQ had budgeted for this work being reallocated to spending outside of the NITRD Program.

NIST

Comparison of 2006 request (\$42 million) and 2006 estimate (\$39 million): Reductions in HEC I&A and HCI&IM spending account for the decrease in NIST's budget. The addition of CSIA as a new PCA results in funding that had previously been reported under HCSS now being nearly equally divided between the CSIA and HCSS PCAs.

Comparison of 2006 estimate (\$39 million) and 2007 request (\$43 million): NIST's budget receives a \$4 million increase from 2006 to 2007, divided equally between the CSIA and HCI&IM PCAs.

DOE/NNSA

Comparison of 2006 request (\$114 million) and 2006 estimate (\$35 million): A portion of the reduction in DOE/NNSA's budget is due to decreases in the ASC Program budget. The bulk of the reduction does not correspond to changes in programmatic activities, but is due to new classification and characterizations of DOE/NNSA investments resulting from new business processes in use at the agency. The percentage of major technical efforts classified as R&D has been reduced in several instances, while investments in network infrastructure, legacy codes, infrastructure operations and maintenance, data management activities, storage procurements, and software tools development and licenses have been characterized as outside the scope of R&D

⁸ NSA's budget reporting includes unclassified funding from DTO (formerly ARDA).

activities. For comparison, had investments been classified per these new business processes last year, the previously reported 2006 request would have been \$39 million.

Comparison of 2006 estimate (\$35 million) and 2007 request (\$42 million): The main component of DOE/NNSA's budget increase is an increase of \$8 million in HEC R&D, to support participation as a mission partner in Phase III of DARPA's HPCS program, and to pursue a next-generation successor to the BlueGene/L high-end computing system.

NOAA

Comparison of 2006 request (\$20 million) and 2006 estimate (\$16 million): The decrease in NOAA's budget, mostly in HEC I&A, is due to Congressional action reducing NOAA's operations, research, and facilities budget.

Comparison of 2006 estimate (\$16 million) and 2007 request (\$23 million): The 2007 request restores funds cut in 2006 and includes additional increases, mainly to HEC I&A.

EPA

Comparison of 2006 request, 2006 estimate and 2007 request (all \$6 million): The NITRD Program budget for EPA remains level at \$6 million.

NITRD Program Budget Summary by PCA

A broad analysis of the NITRD Program budget by PCA, which summarizes the most substantial changes to PCA budgets in 2007, using 2006 estimated spending as a baseline, appears below. This section summarizes the more detailed information about significant changes within agency budgets provided above.

Because of the continuing priority placed on high-end computing by the Administration, the 2007 budget request for HEC I&A is \$884 million, an increase of \$59 million above 2006 estimated spending. The bulk of the new funding is requested by NSF and DOE/SC for procurements of and/or enhancements to leadership-class computing systems. Budget increases more than offset the reduction in OSD's HEC I&A budget, due to higher-level funding reallocations within DoD, primarily within the HPCMPO.

Also because of the budget emphasis on high-end computing, the 2007 budget request for HEC R&D is \$440 million, an increase of \$56 million above 2006 estimated spending. Most of the change is accounted for by budget increases for DOE/SC to enhance its SciDAC partnerships and for DARPA for Phase III of the HPCS program, a planned decrease in NSA's request due to the 2006 acceleration of Black Widow R&D, and an increase in DOE/NNSA's request.

As a new NITRD PCA, CSIA reports R&D in the NITRD Program Budget Supplement for the first time this year. The 2007 budget request for CSIA is \$176 million,⁹ an increase of \$14 million above 2006 estimated spending. This increase is mainly the result of a larger budget request at NSF due to an elevated emphasis on cyber security via the Cyber Trust program and related activities.

The 2007 budget request for HCI&IM is \$825 million, an increase of \$63 million above 2006 estimated spending. Budget request increases at NSF for R&D in scientific data management and at DARPA for its Learning, Reasoning and Integrated Cognitive Systems programs are the most substantial changes for this PCA.

The 2007 budget request for LSN is \$405 million, an increase of \$11 million above 2006 estimated spending. Increases in budget requests at DARPA for scaling up cognitive networking activities, and at DOE/SC for enhancements to ESnet to support management of petascale data from scientific facilities and high performance computing facilities, account for most of the change in this PCA. Budget increases more than offset the reduction in OSD's LSN budget, due to higher-level funding reallocations within DoD, primarily within the Army.

The 2007 budget request for HCSS is \$145 million, an increase of \$12 million above 2006 estimated spending. An increase in NSF's budget request for HCSS accounts for most of this difference.

The 2007 budget request for SEW is \$114 million, an increase of \$2 million above 2006 estimated spending. Funding for this PCA remains relatively stable.

The 2007 budget request for SDP is \$86 million, an increase of \$2 million above 2006 estimated spending. Funding for this PCA remains relatively stable.

⁹ Please see footnote 1 on page 19.

**National Science and Technology Council
Committee on Technology
Co-Chairs**

Richard Russell, Associate Director, OSTP
William A. Jeffrey, Under Secretary for Technology (acting), DOC

**Subcommittee on Networking and Information Technology Research and Development
Co-Chairs**

Peter A. Freeman, NSF
Simon Szykman, NCO

NSF <i>Representatives</i> Peter A. Freeman Thomas A. Weber <i>Alternates</i> Deborah L. Crawford C. Suzanne Iacono	DARPA <i>Representative</i> Anthony J. Tether DOE/SC <i>Representative</i> Michael Strayer <i>Alternates</i> Daniel A. Hitchcock Norman H. Kreisman NSA <i>Representative</i> George R. Cotter <i>Alternate</i> Candace S. Culhane	NASA <i>Representative</i> Walter F. Brooks <i>Alternate</i> Bryan A. Biegel AHRQ <i>Representative</i> J. Michael Fitzmaurice NIST <i>Representative</i> Cita M. Furlani <i>Alternate</i> Larry H. Reeker	DOE/NNSA <i>Representative</i> Robert Meisner <i>Alternate</i> Thuc T. Hoang NOAA <i>Representative</i> William T. Turnbull <i>Alternate</i> Michael Kane EPA <i>Representative</i> Gary L. Walter <i>Alternate</i> Val Garcia	OMB <i>Representative</i> David S. Trinkle OSTP <i>Representative</i> Charles H. Romine NCO <i>Representative</i> Simon Szykman <i>Alternate</i> Sally E. Howe
OSD <i>Representative</i> André M. van Tilborg <i>Alternate</i> Robert Gold NIH <i>Representative</i> Michael Marron <i>Alternates</i> Michael J. Ackerman Peter Highnam Karen Skinner				

Interagency Working Groups, Coordinating Groups, and Team Chairs

High End Computing (HEC) Interagency Working Group <i>Chair</i> John Grosh, OSD <i>Vice-Chair</i> Frederick C. Johnson, DOE/SC <i>Incoming Vice-Chair</i> José L. Muñoz, NSF	Large Scale Networking (LSN) Coordinating Group <i>Co-Chairs</i> Daniel A. Hitchcock, DOE/SC Wei Zhao, NSF LSN Teams: Middleware and Grid Infrastructure Coordination (MAGIC) Team <i>Co-Chairs</i> Mary Anne Scott, DOE/SC Kevin L. Thompson, NSF Joint Engineering Team (JET) <i>Co-Chairs</i> Douglas G. Gatchell, NSF George R. Seweryniak, DOE/SC <i>Vice-Chair</i> Paul E. Love, Internet2 Networking Research Team (NRT) <i>Co-Chairs</i> Thomas Ndousse, DOE/SC Guru Parulkar, NSF	High Confidence Software and Systems (HCSS) Coordinating Group <i>Co-Chairs</i> Helen D. Gill, NSF William Bradley Martin, NSA Social, Economic, and Workforce Implications of IT and IT Workforce Development (SEW) Coordinating Group <i>Co-Chairs</i> C. Suzanne Iacono, NSF Susan B. Turnbull, GSA Software Design and Productivity (SDP) Coordinating Group <i>Co-Chairs</i> Thuc T. Hoang, DOE/NNSA Michael Foster, NSF
---	---	---

Participation in Federal NITRD Activities

The following goals and criteria developed by the NITRD Program are intended to enable agencies considering participation to assess whether their research and development activities fit the NITRD structure.

NITRD Goals

- Provide research and development foundations for assuring continued U.S. technological leadership in advanced networking, computing systems, software, and associated information technologies
- Provide research and development foundations for meeting the needs of the Federal government for advanced networking, computing systems, software, and associated information technologies
- Accelerate development and deployment of these technologies in order to maintain world leadership in science and engineering; enhance national defense and national and homeland security; improve U.S. productivity and competitiveness and promote long-term economic growth; improve the health of the U.S. citizenry; protect the environment; improve education, training, and lifelong learning; and improve the quality of life.

Evaluation Criteria for Participation

Relevance of Contribution

The research must significantly contribute to the overall goals of the NITRD Program and to the goals of one or more of the Program's eight Program Component Areas (PCAs) – High End Computing Infrastructure and Applications (HEC I&A), High End Computing Research and Development (HEC R&D), Cyber Security and Information Assurance (CSIA), Human- Computer Interaction and Information Management (HCI&IM), Large Scale Networking (LSN), High Confidence Software and Systems (HCSS), Social, Economic, and Workforce Implications of Information Technology and Information Technology Workforce Development (SEW), and Software Design and Productivity (SDP) – in order to enable the solution of applications and problems that address agency mission needs and that place significant demands on the technologies being developed by the Program.

Technical/Scientific Merit

The proposed agency program must be technically and/or scientifically sound, of high quality, and the product of a documented technical and/or scientific planning and review process.

Readiness

A clear agency planning process must be evident, and the organization must have demonstrated capability to carry out the program.

Timeliness

The proposed work must be technically and/or scientifically timely for one or more of the PCAs.

Linkages

The responsible organization must have established policies, programs, and activities promoting effective technical and scientific connections among government, industry, and academic sectors.

Costs

The identified resources must be adequate to conduct the proposed work, promote prospects for coordinated or joint funding, and address long-term resource implications.

Agency Approval

The proposed program or activity must have policy-level approval by the submitting agency.

Glossary

- AFRL** - Air Force Research Laboratory
- AHRQ** - HHS's Agency for Healthcare Research and Quality
- ANL** - DOE's Argonne National Laboratory
- ARC** - NASA's Ames Research Center
- ARDA** - Advanced Research and Development Activity
- ARL** - Army Research Laboratory
- ARO** - Army Research Office
- ARSC** - Arctic Region Supercomputing Center
- ASC** - DOE/NNSA's Advanced Simulation and Computing program (formerly ASCI, for Accelerated Strategic Computing Initiative)
- BIRN** - NIH's Biomedical Informatics Research Network
- Black Widow** - NSA-supported next-generation (2007) system in the X1/X1e massively parallel, vector-processing system line
- BlueGene** - A supercomputing project dedicated to building a new family of supercomputers
- BlueGene/L** - Scalable experimental new supercomputing system being developed in partnership with DOE/SC and DOE/NNSA; expected to achieve 300-teraflops+ processing speeds
- BlueGene/P** - The next generation in the BlueGene line after BlueGene/L
- CaBIG** - NIH's cancer Biomedical Informatics Grid
- CAIDA** - Cooperative Association for Internet Data Analysis
- CAREER** - NSF's Faculty Early Career Development Program
- CENIC** - Corporation for Network Initiatives in California
- CENTCOM** - DoD's United States Central Command
- CG** - Coordinating Group
- CHEETAH** - NSF's Circuit-switched High-speed End-to-End Architecture network
- CIIP** - Critical Information Infrastructure Protection
- CIO** - Chief information officer
- CMS** - HHS's Centers for Medicare and Medicaid Services
- COPs** - Communities of practice
- CSIA** - Cyber Security and Information Assurance, one of NITRD's eight Program Component Areas
- CSTB** - Computer Science and Telecommunications Board of the National Research Council
- DARPA** - DoD's Defense Advanced Research Projects Agency
- DDDAS** - Dynamic Data Driven Applications Systems
- DETER** - NSF- and DHS-initiated cyber DEFense Technology Experimental Research network
- DHS** - Department of Homeland Security
- DLI** - DoD's Defense Language Institute
- DNS** - Domain Name System
- DOC** - Department of Commerce
- DoD** - Department of Defense
- DOE** - Department of Energy
- DOE/NNSA** - DOE/National Nuclear Security Administration
- DOE (OE)** - DOE's Office of Electricity Delivery and Energy Reliability
- DOE/SC** - DOE's Office of Science
- DOJ** - Department of Justice
- DOT** - Department of Transportation
- DRAGON** - NSF's Dynamic Resource Allocation (via GMPLS) Optical Network
- DTO** - Disruptive Technology Office (formerly ARDA); budget reported through NSA this year
- Eldorado** - NSA-supported multithreaded system
- EMIST** - NSF/DHS Evaluation Methods for Internet Security Technology project
- EPA** - Environmental Protection Agency
- ESCHER** - Embedded Systems Consortium for Hybrid and Embedded Research, a joint effort of DARPA and NSF
- ESMF** - Earth System Modeling Framework
- ESnet** - DOE/SC's Energy Sciences network
- ESSC** - DOE/SC's Energy Sciences network (ESnet) Steering Committee
- ETF** - Extensible Terascale Facility
- FAA** - DOT's Federal Aviation Administration
- FBI** - Federal Bureau of Investigation
- FDA** - HHS's Food and Drug Administration
- FISMA** - Federal Information Security Management Act
- FIU** - Florida International University
- FY** - Fiscal Year
- GALE** - DARPA's Global Autonomous Language Exploitation program
- GENI** - Global Environment for Network Investigations
- GEOSS** - Global Earth Observation System of Systems, a cooperative effort of 34 nations, including the U.S., and 25 international organizations to develop a comprehensive, coordinated, and sustained Earth observation system
- GMPLS** - Generalized Multi-Protocol Label Switching

GSA - General Services Administration
GSFC - NASA's Goddard Space Flight Center
HCI&IM - Human-Computer Interaction and Information Management, one of NITRD's eight Program Component Areas
HCSS - High Confidence Software and Systems, one of NITRD's eight Program Component Areas
HEC - High-end computing
HEC I&A - HEC Infrastructure and Applications, one of NITRD's eight Program Component Areas
HEC R&D - HEC Research and Development, one of NITRD's eight Program Component Areas
HECRTF - High-End Computing Revitalization Task Force
HEC-URA - HEC University Research Activity, jointly funded by multiple NITRD agencies
HHS - Department of Health and Human Services
HPC - High-performance computing
HPCMPO - OSD's High Performance Computing Modernization Program Office
HPCS - DARPA's High Productivity Computing Systems program
HRI - Human-robot interaction
INCITE - DOE/SC's Innovative and Novel Computational Impact on Theory and Experiment program
Infiniband - A high-speed serial computer bus, intended for both internal and external connections
I/O - Input/output
IP - Internet Protocol
IPsec - IP security protocol
IPv6 - Internet protocol, version 6
IRS - Internal Revenue Service
ISI - Information Sciences Institute
IT - Information technology
ITR - NSF's Information Technology Research program
IT R&D - Information technology research and development
IU - Indiana University
IWG - Interagency Working Group
JET - LSN's Joint Engineering Team
JETnets - Federal research networks supporting networking researchers and advanced applications development
JPEG - An image file format developed by the Joint Photographic Experts Group
LANL - DOE's Los Alamos National Laboratory
LBL - DOE's Lawrence-Berkeley National Laboratory
LCF - DOE's Leadership Computing Facility
LSN - Large Scale Networking, one of NITRD's eight Program Component Areas
MAGIC - LSN's Middleware and Grid Infrastructure Coordination team
MAN - Metropolitan area network
MAX - Mid-Atlantic eXchange
MCNC - Microelectronics Center of North Carolina
MIDAS - NIH's Modeling of Infectious Disease Agents Study
MPEG-7 - Moving Picture Experts Group's multimedia content description interface, release 7
MPI - Message-passing interface
MTU - Maximum transmission unit
MURI - Multidisciplinary University Research Initiative
MW - Middleware
NARA - National Archives and Records Administration
NASA - National Aeronautics and Space Administration
NationalLambda Rail - Consortium of organizations working to provide an optical network for research
NCAR - NSF-supported National Center for Atmospheric Research
NCBC - NIH's National Centers for Biomedical Computing
NCS-A - DOE/SC NERSC new computer system-A
NCS-B - DOE/SC NERSC 7-TF new computer system-B
NCSA - NSF-supported National Center for Supercomputing Applications
NERSC - DOE/SC's National Energy Research Scientific Computing Center
NERSC-4 - DOE/SC center's 9-TF SP3 computing platform
NERSC-5 - DOE/SC center's planned next-generation (100-150 TF) platform
NIH - HHS's National Institutes of Health
NIST - DOC's National Institute of Standards and Technology
NITRD - Networking and Information Technology Research and Development
NLANR - NSF-supported National Laboratory for Applied Network Research
NLM - NIH's National Library of Medicine
NNSA - DOE's National Nuclear Security Administration
NOAA - DOC's National Oceanic and Atmospheric Administration
NRT - LSN's Networking Research Team
NSA - National Security Agency
NSF - National Science Foundation
NSTC - National Science and Technology Council

NVLAP - National Voluntary Lab Accreditation Program, supported by NIST and NSA

ODDR&E - OSD's Office of the Director, Defense Research and Engineering

OMB - White House Office of Management and Budget

OMNInet - Large-scale metro optical network testbed supported by national labs, universities, Canadian organizations, and vendor partners

ONR - Office of Naval Research

ONT - Optical networking testbed

OptiPuter - NSF-funded five-year project to interconnect distributed storage, computing, and visualization resources using photonic networks

ORNL - DOE's Oak Ridge National Laboratory

OS - Operating system

OSD - Office of the Secretary of Defense

OSTP - White House Office of Science and Technology Policy

PCA - Program Component Area

PDA - Personal digital assistant

PET - OSD (HPCMPO)'s Programming Environment and Training program

PI - Principal investigator

PITAC - President's Information Technology Advisory Committee

PNL - Pacific Northwest Laboratory

PSC - Pittsburgh Supercomputing Center

Purple - DOE/NSA ASC's 100-TF SMP supercomputing platform under development, in tandem with Blue Gene/L, at LLNL

QoS - Quality of service

R&D - Research and development

RDE - Real-time, distributed, embedded

ROM - Read-only memory

RTOS - Real-time operating system

SAPIENT - DARPA's Situation-Aware Protocols in Edge Network Technologies program

SBIR - Federal government's Small Business Innovation Research program

SC - DOE's Office of Science

SCADA - Supervisory control and data acquisition

SciDAC - DOE/SC's Scientific Discovery through Advanced Computing program

SDP - Software Design and Productivity, one of NITRD's eight Program Component Areas

SDSC - San Diego Supercomputer Center

SEW - Social, Economic, and Workforce Implications of IT and IT Workforce Development, one of NITRD's eight Program Component Areas

SoD - NSF's Science of Design program

SP3 - 7-TF scalable parallel platform at NERSC

StarLight - NSF-supported international optical network peering point in Chicago

State - Department of State

TF - Teraflop(s), a trillion floating point operations (per second)

TIDES - DARPA-funded Translingual Information Detection, Extraction and Summarization program

Treasury - Department of the Treasury

TREC - Text REtrieval Conference

TRUST - NSF's Team for Research in Ubiquitous Secure Technology

TSWG - Technical Support Working Group

UCAR - University Corporation for Atmospheric Research

UIC - University of Illinois at Chicago

UIUC - University of Illinois at Urbana-Champaign

UltraScience Net - DOE/SC's experimental research network

UMd - University of Maryland

UNC - University of North Carolina

USGS - United States Geological Survey

USASMDC/ARSTRAT - U.S. Army Space and Missile Defense Command/Army Forces Strategic Command

UW - University of Washington

UWisc - University of Wisconsin

VA - Department of Veterans Affairs

V&V - Verification and validation

VM - Virtual machine

VPN - Virtual private network

WAN - Wide area network

Wi-Max - Worldwide interoperability for microwave access, a set of wireless standards

WLAN - Wireless local area network

WRF - Weather Research and Forecasting model, a next-generation mesoscale numerical weather prediction system developed collaboratively by Federal agencies

X1 - Scalable, hybrid scalar-vector high-end computing system developed with support from NSA and ODDR&E

X1e - follow-on to the X1 (see Black Widow)

XT3 - Third generation of massively parallel processor (MPP) systems, following predecessors T3D and T3E

National Coordination Office (NCO) for Networking and Information Technology Research and Development (NITRD)

Simon Szykman, Ph.D.
Director

Sally E. Howe, Ph.D.
Associate Director
Executive Editor, FY 2007
NITRD Budget Supplement

Martha K. Matzke
Editor, FY 2007
NITRD Budget Supplement

Suite II-405
4201 Wilson Boulevard
Arlington, Virginia 22230
(703) 292-4873
FAX: (703) 292-9097
nco@nitrd.gov

NCO Web Site
<http://www.nitrd.gov/>

Acknowledgements

Developing the content for the FY 2007 Supplement in a timely fashion required technical information and support by a large number of Federal agency representatives involved in NITRD Program activities and by NCO technical and administrative staff. The editors extend sincerest thanks and appreciation to all.

Contributors

Nekeia Bell, NCO	Cray J. Henry, HCPMPO	Piyush Mehrotra, NASA
Bryan A. Biegel, NASA	Martin Herman, NIST	Robert Meisner, DOE/NNSA
Paul E. Black, NIST	Peter Highnam, NIH	Grant Miller, NCO
Robert B. Bohn, NOAA	Daniel A. Hitchcock, DOE/SC	Paul Miner, NASA
Raymond A. Bortner, AFRL	Thuc T. Hoang, DOE/NNSA	William Miner, NCO
Walter F. Brooks, NASA	C. Suzanne Iacono, NSF	Virginia Moore, NCO
Martin Burkhouse, DOJ	Alan S. Inouye, NCO	José L. Muñoz, NSF
Robert Chadduck, NARA	Donald Jenkins, NIH	Thomas Ndousse, DOE/SC
Leslie Collica, NIST	Paul Jones, FDA	William Newhouse, NSA
George R. Cotter, NSA	Frederick C. Johnson, DOE/SC	Guru Parulkar, NSF
Deborah L. Crawford, NSF	Rodger Johnson, DREN	Perry Pederson, TSWG
Candace S. Culhane, NSA	Michael Kane, NOAA	Mark Powell, FAA
Warren Debany, AFRL	Frankie D. King, NCO	Larry H. Reeker, NIST
David Ferraiolo, NIST	Steven King, OSD	Stephen Roznowski, NSA
J. Michael Fitzmaurice, AHRQ	Rita Koch, NSF	Jean C. Scholtz, (formerly NIST)
Michael Foster, NSF	Carl Landwehr, DTO (formerly NSF)	Mary Anne Scott, DOE/SC
Simon Frechette, NIST	Annabelle Lee, DHS	William J. Semancik, NSA
Kenneth Freeman, NASA	Sander L. Lee, DOE/NNSA	George R. Seweryniak, DOE/SC
James C. French, NSF	Tsengdar Lee, NASA	David Su, NIST
Cita M. Furlani, NIST	Karl Levitt, NSF	Denise Sumikawa, LLNL
Helen Gigley, CIA (formerly ONR)	Ernest R. Lucier, FAA	Judith D. Terrill, NIST
Helen Gill, NSF	Peter Lyster, NIH	Anthony J. Tether, DARPA
Robert Gold, OSD	Stephen R. Mahaney, NSF	Diane R. Theiss, NCO
Robert B. Graybill, DARPA	Paul Mansfield, NSA	Susan B. Turnbull, GSA
John Grosh, OSD	Michael Marron, NIH	William T. Turnbull, NOAA
Kevin Harnett, DOT	Wendy Martinez, ONR	Gary L. Walter, EPA
Vivian Harris, NCO	William Bradley Martin, NSA	Robert Wright, FBI

Copyright Information

This is a work of the U.S. Government and is in the public domain. It may be freely distributed and copied, but it is requested that the National Coordination Office for Networking and Information Technology Research and Development (NCO/NITRD) be acknowledged.

To Request Additional Copies

To request additional copies of this Supplement to the President's FY 2007 Budget or other NITRD Program publications, please contact: National Coordination Office, Suite II-405, 4201 Wilson Boulevard, Arlington, Virginia 22230; (703) 292-4873; fax: (703) 292-9097; e-mail: nco@nitrd.gov. Electronic versions of NITRD documents are also available on the NCO Web site: www.nitrd.gov.