Center for National Security Studies
Protecting civil liberties and human rights

Statement of the Center for National Security Studies

by Kate Martin, Director, and Lisa Graves, Deputy Director

"Constitutional Failings of the Foreign Intelligence Surveillance Modernization Act"

Before the Senate Select Committee on Intelligence

May 1, 2007

On behalf of the Center for National Security Studies, we thank Chairman Rockefeller for the invitation to submit our views regarding the Foreign Intelligence Surveillance Act (FISA) and the administration's proposal to amend it via the "Foreign Intelligence Surveillance Modernization Act" (FISMA).

The Center has worked on issues concerning FISA since its birth, and we are pleased to be invited to share our views with the distinguished Members of this Committee who are charged with shared oversight of US intelligence-gathering operations. For more than 30 years, the Center has worked to ensure that civil liberties and human rights are not eroded in the name of national security. We are guided by the conviction that our national security can and must be protected without undermining the fundamental rights of individuals guaranteed by the Bill of Rights. In our work, we begin with the premise that both national security interests and civil liberties protections must be taken seriously and, that by doing so, solutions to apparent conflicts can often be found without compromising either.

***Summary*.** We strongly oppose the administration's proposal and urge the Committee to reject it because its complex changes to FISA would severely undermine the fundamental privacy rights of Americans. It would authorize the Executive Branch to conduct unconstitutional searches of Americans' private conversations. It would permit the government intentionally to acquire billions and billions of Americans' international phone calls and e-mails without a warrant, so long as it vacuumed up the contents of these communications en masse, rather than targeting for initial acquisition the communications of a particular individual in the United States. And it would permit the government to then sort and analyze all those

1120 19th Street, NW, Suite 800, Washington, DC 20036
(202) 721-5650 fax: (202) 530-0128 cnss@cnss.org www.cnss.org

communications and listen to and distribute whichever ones it chose, in secret, with no warrant or meaningful individualized oversight whatsoever. This would be a dramatic and drastic change to statutory law. Under the guise of "tech neutrality," the proposal would neutralize the key protections in current law and authorize warrantless surveillance of virtually all communications in any form by Americans with anyone, including other Americans, located overseas. The administration's proposal attempts to make public law sanction federal government acquisition and mining of vast amounts of private, personal information on Americans residents, preying on fears about terrorism and exploiting new technologies that make such invasions of the private calls and e-mails of American residents easier than ever before.

The administration has tried to cast its proposal as merely "modernization," even though FISA has been repeatedly modernized including four significant changes since September 11th. In each instance, Congress has kept the basic structure of individualized judicial checks for communications to or from people in the US, and rightly so. As General Hayden testified to the House Permanent Select Committee on Intelligence in 2000, the reality is that FISA's "privacy framework is technology neutral and does not require amendment to accommodate new communications technologies." Notably, he gave this assurance after calling reports that the NSA operated a program called "Echelon" to monitor all international communications, "false and misleading," yet the administration's FISMA tries to give legal license to such activities directed at streams of American communications. The changes being proposed would not be mere accommodations of new technologies in order to keep the legal framework current but would work a fundamental change to the structure of law and substantially weaken civil liberties protections. Indeed, the fact that more human thought and speech than ever before is now transcribed into electronic signals and transmitted by phone calls or e-mails requires greater protections for privacy and freedom of speech, not fewer.

The Administration seeks to legalize massive warrantless surveillance of Americans, far beyond the surveillance it has admitted to in the "Terrorist Surveillance Program."

We now know that since shortly after the 9/11 attacks the administration has claimed the power to listen to Americans' conversations and read their e-mails without warrants and in violation of FISA's protections for the privacy of people in the US in both their international and domestic communications. We do not yet know how broadly they exercised that power for the duration of the program, although they have admitted to warrantless surveillance of some

international communications of persons in the US, all the while the President and others in the administration claimed publicly, until late 2005, that they obtained warrants to monitor people here. There is also evidence that they have sought addressing information of all communications presumably in order to conduct traffic analysis of billions of communications by Americans.

The administration argued when the warrantless surveillance was first revealed, that the President has "inherent" powers as commander-in-chief to set aside the requirements of FISA, if he believes it necessary. This argument ignored the first Article of the Constitution, which expressly commits to Congress shared powers over war and national defense and the system of separated but shared powers described by the Supreme Court in the steel seizure case, even in times of war. So, the administration also contended that the Authorization for the Use of Military Force in Afghanistan constituted an implicit amendment to FISA authorizing warrantless surveillance of people in the US. After much scholarly and bipartisan rejection of these arguments, the administration apparently pressed for a creative interpretation of the law by the FISA court to authorize some part of the most current iteration of such surveillance. The purpose of the administration's proposed amendments is illuminated when set in this context. While the administration has not disavowed its claims of executive power to override the law, it is now pressing for statutory changes to achieve the same end, *i.e.*, unchecked secret power to conduct electronic surveillance on millions of Americans.

*** The bill would permit the vacuuming of all international communications of Americans.** The bill would allow the warrantless seizure of all international calls and e-mails of American residents and businesses, without any link to al Qaeda—a sweep far broader than the secret program President Bush publicly acknowledged on December 17, 2005. It would change the definition of "electronic surveillance" to allow Americans' international calls and e-mails to be scooped up en masse through any technological means (*i.e., "tech neutral")* so long as a particular American was not targeted in the *initial* "acquisition" or surveillance.[1] Once

[1] This radical change is buried in the technical amendments to the sophisticated definition of "electronic surveillance" in FISA, which can be unpacked as follows. Current FISA law bars the warrantless "acquisition" of the content of domestic communications--whether they occur by *wire or radio*--as well as "information," if it is intentionally acquired through other means, such as "bugging" or video surveillance devices, where a person has a reasonable expectation of privacy. FISA also bars warrantless "acquisition" in the US of the contents of *wire* communications "to or from a person in the United States," meaning domestic or international, whether a known US person is the target of the acquisition or not. It also bars the surveillance of

Americans' international communications were acquired without a warrant, the government would be free to analyze and listen to any private personal or business conversations or data, without ever having obtained any judicial warrant. The "Fact Sheet" issued by the Department of Justice omits any mention of this and the other extraordinary changes that would be made by the bill. No administration official has explained to the American people that this is the power they are seeking.

* **The bill would also apparently authorize warrantless access to some number of purely domestic cell phone and e-mail content**, with a new statutory basis to claim that the government does not know and need not ascertain if the sender and all recipients are in the US.

*** It would permit unlimited access without court oversight to all international and some domestic call records**, allowing the tracing of the social networks of American residents, including journalists as a routine part of foreign intelligence monitoring here.

*** The changes to FISA's definitions would also create a loophole for surreptitious video surveillance of private spaces without a warrant for foreign intelligence purposes.**

* **The administration's bill also replaces the narrow exception to the warrant requirement for certain communications of embassies in the US with broader authority to acquire communications in the US without a court order**, simply based on the Attorney General's certification or directive. For example, section 102 of FISA would be changed to eliminate the narrow exception that a warrant is not required if the surveillance is directed "solely" at the communications of foreign governments in the US, and it deletes the bar on such warrantless surveillance even when there is a "substantial likelihood" Americans' conversations will be swept in. That is, the Attorney General could order warrantless surveillance directed toward a foreign government here even if such surveillance was likely to sweep in Americans' conversations. And the bill strikes the statutory protections for American conversations obtained

---

the contents of the *radio* communications to or from a known US person in this country by intentionally "targeting" that person. (The statute is silent about acquiring international *radio* communications without intentionally targeting a particular US person, although at the time FISA was passed Congress recognized that Americans do have Fourth Amendment rights in the privacy of the content of such communications.) By repealing or modifying these statutory prohibitions, the bill would suddenly allow the warrantless acquisition of the content of all international telephone, e-mail or other communications sent by any technology to or from Americans so long as it is acquired en masse rather than by *initially* targeting a particular US person's communications.

inadvertently in this way without warrants, by eliminating FISA's requirement in 50 USC 1801(h)(4) that such conversations be deleted within three days of acquisition unless the government obtains a FISA court order or if there is a threat to life or threat of bodily injury.

It is quite likely that any power granted to gather information will be used to the maximum extent, and the powers proposed to itself by the administration would be used to sweep up conversations and communications involving millions of innocent people. As Mark Twain said, "to a man with a hammer, everything looks like a nail." These proposals strike at the heart of Americans' reasonable expectations of privacy against government surveillance.

The Bill would violate the Fourth Amendment.

The warrantless surveillance of Americans' conversations that would be authorized by FISMA fundamentally violates the Constitution because:

- The Fourth Amendment requires warrants, and there is a FISA court available to issue such warrants;
- It requires an individualized determination of probable cause before seizing private communications;
- and the massive surveillance that would be authorized by this bill would be unreasonable, under any fair interpretation of the Fourth Amendment.

In addition, the administration is simply wrong that, contrary to the language and legislative history of FISA, Congress intended to allow virtually unlimited monitoring of the content of Americans' international communications or believed that such acts would be constitutional.

Faithful enforcement of the Fourth Amendment's protections are in some ways even more critical for intelligence surveillance than for criminal investigations because intelligence surveillance is likely to remain secret. On this point, the bipartisan Church Committee recorded what can happen, even with he best of intentions of protecting the country, when warrants are not required. Unchecked secret government power intended to protect the national security:

> may become a menace to free government and free institutions because it carries with it the possibility of abuses of power which are not always quickly apprehended or understood.... Our investigation has confirmed that warning. We have seen segments of our government, in their attitudes and actions, adopt tactics unworthy of a democracy.... *We have seen a consistent pattern in which programs initiated with limited goals,* such as preventing criminal violence or identifying foreign spies, were *expanded to what witnesses characterized as "vacuum cleaners," sweeping in information about lawful activities of American citizens.*

Final Report of the Senate Select Committee, Book II, April 26, 1976 (emphasis added).

Notably, the Defense Department has agreed with this assessment:

> In the early and mid 1970s several Congressional committees, including the Church, Pike, and Ervin committees, conducted investigations and public hearings. After three and a half years of investigation, these committees determined that what had occurred was a classic example of what we would today call "mission creep." What had begun as a simple requirement to provide basic intelligence to commanders charged with assisting in the maintenance and restoration of order had become a monumentally intrusive effort. This resulted in the monitoring of activities of innocent persons involved in the constitutionally protected expression of their views on civil rights or anti-war activities. The information collected on the persons targeted by Defense intelligence personnel was entered into a national data bank and made available to civilian law enforcement authorities. This produced a chilling effect on political expression by those who were legally working for political change in domestic and foreign policies. Senator Ervin concluded "the collection and computerization of information by government must be tempered with an appreciation of the basic rights of the individual, of his right to privacy, to express himself freely and associate with whom he chooses." As a result of these investigations, DoD imposed severe restrictions on future surveillance of U.S. persons, required that information already in DoD files be destroyed, and established a structure to regulate future DoD intelligence collection.

Available at: http://www.dod.mil/atsdio/. Unfortunately, over the past six years, we have seen frequent reports of deliberate, secret departures from these and other protections, some of which have been reportedly abandoned only last month, as with the TALON database.

On electronic surveillance, only the most extreme proponents of unchecked presidential power argue that warrantless surveillance conducted in violation of FISA's prohibitions is legal. But eliminating FISA's statutory prohibitions will not cure the constitutional infirmity of such surveillance. The Fourth Amendment is clear that a judicial warrant is required to seize or search an Americans' private papers or the equivalent and plainly such warrants must be based on individualized probable cause of wrongdoing, such as conspiring with foreign nationals to commit acts of terrorism.

The Fourth Amendment protects the privacy of the people of the United States and requires warrants before listening to conversations. *Katz v. United States*, 389 U.S. 347 (1967). Notably, in a case involving warrantless wiretapping in the name of national security, the Supreme Court stressed that "Fourth Amendment freedoms cannot properly be guaranteed if domestic surveillance may be conducted solely within the discretion of the Executive Branch." *United States v. United States District Court*, 407 U.S. 297, 324 (1972). While the Court

reaffirmed that "prior judicial approval is required for the type of domestic surveillance" in that case, it invited Congress to create standards for domestic and foreign intelligence gathering to protect constitutional rights. *Id.* In passing FISA after both a complete committee investigation and extensive public hearings, the Senate noted that the statute "was designed . . . to curb the practice by which the Executive Branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it." S. Rep. No. 95-604(I), at 7, 1978 U.S.C.C.A.N. 3904, 3908. There is no Fourth Amendment exception for the seizure of Americans' international calls, whether made from a landline, cordless phone or cell phone, or written in e-mails, although that is what the bill attempts to create. And there is no emergency exception to the Fourth Amendment that could accommodate what the administration desires.

When the government wants to monitor the communications of a person in the US, then the Constitution as reflected in FISA requires that there be judicial scrutiny. And, Congress has established the FISA court as a workable mechanism for issuing classified judicial warrants. Nevertheless, in a departure from these norms, the Department of Justice has cited three cases allowing warrantless surveillance while neglecting the fact that each of these cases dealt with pre-FISA surveillance before Congress either made detailed findings that the unchecked regime of warrantless surveillance was a violation of the Fourth Amendment or created the FISA court. *See United States v. Truong*, 629 F.2d 908, 916 (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). The administration also often ignores contrary precedent such as *Zweibon v. Mitchell*, 516 F.2d 594 (D.C. Cir. 1975) (en banc), where a plurality of the D.C. Circuit rejected the notion that electronic surveillance for foreign intelligence activities can be conducted without a warrant. (Nor is the dicta about supposed inherent authority in the 2002 FISCR decision binding or persuasive authority in the face of Congress' explicit enactments.) Congress passed FISA because of the absolute imperative to "provide the secure framework by which the executive branch may conduct legitimate electronic surveillance for foreign intelligence purposes within the context of this nation's commitment to privacy and individual rights." S. Rep. No. 95-604, pt. 1, at 15 (1977) (noting that courts had "held that a warrant must be obtained before a wiretap is installed on a domestic organization that is neither the agent of, nor acting in collaboration with, a foreign power").

Even if FISA's warrant requirements were recklessly repealed and warrantless electronic surveillance of Americans were not confined by statute, the Fourth Amendment would still require that the Attorney General (or a comparable high-level official) personally determine there is probable cause that the target of the surveillance is an agent of a foreign power who is engaged in espionage or terrorism-related activities. *See United States v. Truong*, 629 F.2d 908, 916 (4th Cir. 1980). In that case, the Attorney General made no such determination, the search was held unconstitutional and the court suppressed evidence from the search.

The administration's proposal would authorize massive surveillance of Americans with no warrant and not even any individualized determination of probable cause by the Attorney General. Perhaps the administration will argue that because the bill would only allow the "untargeted" surveillance of thousands or millions of Americans, the requirement of individualized probable cause is inapplicable, although privacy would still be warrantlessly invaded. And, by any reasonable estimate of the number of actual suspected al Qaeda operatives in contact with the US, the volume of innocent communications of Americans that would be swept up in a nation of 300,000,000 people creates a ratio exponentially smaller than even the so-called one percent doctrine of the Vice President. Statistically, the proportion of innocent international calls and e-mails that would be statutorily allowed to be vacuumed under this proposal would be on the order of 99.999+ innocent--and, at what cost in both privacy and money? There is no such exception in the Fourth Amendment. The Constitution does not permit the seizure of millions or billions of conversations or e-mails of Americans to look for a few.

The administration's proposal would repeal a major protection in FISA.

Since the enactment of FISA, no administration has ever explained to the American people that despite the law, there is no privacy in their international communications against seizure or search by the federal government, should they happen to be carried wirelessly. Nor has this administration explained that such is its view. Nevertheless, the administration now argues for a proposal to effectuate such a result, on the ground that it is simply "updating" FISA in light of technological developments.

But allowing such warrantless vacuum cleaner surveillance would be a major repeal of FISA's protections. The plain language of FISA bars the acquisition of the contents of calls "to or from Americans" without a FISA warrant through tapping wire communications in the US. This command plainly was intended to protect against the wiretapping of Americans'

international and domestic calls and telegrams. As the Church Committee noted, the fact that the NSA's "Operation Shamrock" gathered all international telegrams of Americans without initial targeting was of little consolation to those Americans whose private correspondence was seized and analyzed. FISA forbids the government from warrantlessly tapping wires in the US, whether they are telephone lines strung from city to city or trans-oceanic cables departing the coasts. These protections defined in 50 USC 1801(f)(2), bar warrantless acquisition whether a particular person is targeted or whether no one or everyone is targeted. It bars "sitting on the wire." This section would be deleted in its entirety by the administration's bill.

In place of (f)(2), the administration proposes to make 1801(f)(1) "technologically neutral," but does so in a way that eliminates the bar on blanket acquisition of international calls to or from Americans via warrantless wiretapping. Under the administration's revision, there would be no bar on acquisition of all international communications, by sitting on a wire/cable in the US and seizing all such communications of Americans.

The administration's claim that Congress intended to allow it virtually unfettered access to all Americans' international communications unless a person were targeted initially is contradicted by the legislative history. While the so-called "radio exception" in (f)(1) excludes non-targeted international radio transmissions from FISA, Congress made clear that exclusion of some surveillance of Americans from FISA's definitions "should not be viewed as congressional authorization of such activities as they affect the privacy interests of Americans," noting that in any case, "the requirements of the Fourth Amendment would, of course, continue to apply to this type of communications intelligence activity," regardless of FISA. *See* H. REP. NO. 95-1283(I) (June 5, 1978).

Moreover, Congress made clear that when it barred the intentional "targeting" of radio transmissions of Americans, beyond barring the warrantless wiretapping of calls to or from people in the US, that it would not brook the very scenario implied by the administration's interpretations this past year: initial, untargeted acquisition, followed by targeted searches of Americans' acquired conversations. Specifically, the administration suggested in the course of its work on the Wilson and Specter bills that it did not believe FISA placed any limits on the use of devices that analyze communications "lawfully" acquired, such as through its warrantless surveillance of Americans that it has argued is lawful. While FISA did not settle rules for the monitoring of foreign nationals outside the US, it was focused on securing the rights of people in

the US against invasions of privacy, including drilling down in radio signals to monitor frequencies containing channels of American transmissions, and this is reflected in both the legislative history and in long-standing internal directives to NSA operators in the field against intentionally monitoring Americans, even if not known by name, at least before this administration took over.

Telecommunications history also does not support the administration's claims.

The administration's fall back argument is the assertion that in 1978 most international communication was via radio and most domestic communication was via wire but now the situation is reversed—meaning they claim that technological changes are denying them easy access to most international communications of Americans that they claim to be *entitled* to. Beyond the legal history and language in FISA against that interpretation, even a general examination of telecommunications history reveals that the scenario they posit claiming that virtually all international calls of Americans were via satellite radio and therefore intended to be obtained by the government is not accurate. While satellites were increasingly used in the 1970s for television broadcasting and some telecommunications, American telephone companies were continuing to rely on trans-oceanic cables for international calls, with newer transatlantic cables sunk even the year after FISA passed, followed by newer Pacific cables in the early 1980s, which were then replaced in the late 1980s by fiber optic cables that made calls easier to hear and faster. These historic facts are undeniable and anyone old enough to have made international calls in the late 1970s and early 80s undoubtedly remembers the effect of those wire cables: international phone calls sounded a bit like a tunnel and there was a slight delay in response. That is not to say that US calls were transmitted exclusively by wire; in fact, regional domestic calls at the time FISA was passed were often transmitted in part by microwave radio towers, and now they may be transmitted wirelessly by cellular towers and by domestic fiber optic cable.

A more accurate statement than the administration's description would be that for past 29 years, US telecommunications has relied on both wire and radio technology for domestic and international calls. From the beginning, FISA was written to accommodate that reality. There are some conceptual differences between radio and wire communications, for example with the use of satellites for television and radio broadcasts to the public or the necessity of SIGINT regarding the radio communications of navy ships or submarines. But the American people did not, and do not, believe the government has a right or was given statutory authority to monitor all

international communications of Americans in the aftermath of documented abuses by the NSA and other intelligence agencies through secret programs, such as Operation Shamrock and Operation Minaret. There is no evidence that Congress intended, or that the NSA has for the past 30 years, indiscriminately seized millions of conversations and communications of people in the US for analysis. On the contrary, the NSA's own guidance in USSID 18, even provided protections for the content of the communications of Americans abroad.

FISA also bars the government from intentionally acquiring the purely domestic radio communications of Americans when there is a reasonable expectation of privacy because Americans do not lose their constitutional right to privacy merely because telephone companies beam their domestic calls beam them to or from microwave towers. But current law does not bar the government from hearing short-wave radio broadcasts or from listening to embassy communications that are unlikely to include Americans communications or monitoring foreign-to-foreign communications beyond the reach of the Fourth Amendment. But improvements in electronic communications, such as the use of fiber optic cables or the advent of the Internet, simply do not justify fewer protections for privacy as this bill proposes.

The massive surveillance that would be permissible under the bill is not reasonable under the Fourth Amendment, let alone consistent with the warrant requirement.

Even the administration concedes that seizure of the contents of Americans' private communications must be reasonable, while claiming that their actions are reasonable. But the massive surveillance that would be allowed by this bill is manifestly unreasonable. The core of the Fourth Amendment is protection against unreasonable "general searches," especially of individual's private thoughts and communications. The administration, in essence, claims that Americans have no reasonable expectations of privacy in any of their international communications by phone or e-mail, as long as the government does not target them individually. Instead of offering facts and evidence that allowing the unchecked acquisition of virtually all international communications by Americans is the only way to protect against acts of terror in the US, the administration retreats to its standard mantra of national security justifications that, as former National Security Advisor Zbigniew Brzezinski pointed out, is counter-productive fear-mongering. Zbigniew Brzezinski, "Terrorized by 'War on Terror,'" *The Washington Post*, March 25, 2007.

The American people are entitled to know the basis for the claim that such massive invasions of Americans' private calls and e-mails is likely to be effective, much less necessary and proportionate. Generalizations based on a few extrapolations are not enough, claims of past successes must be examined as to whether the same result could have been achieved differently with less cost to civil liberties. There needs to be a thorough examination and analysis of the following: What is the range of the likely threat from individuals in this country, including Americans? How many international communications would be subject to surveillance, presumably millions every day for years to come? What is the likely number of communications that would yield useful intelligence, presumably a very small fraction of the communications actually seized? What are the costs of such a program, in terms of dollars and resources, such as translators allocated to this and therefore unavailable for other more focused, counterterrorism measures? What is the present and future risk to individual liberties from giving the government unchecked power to seize and listen to the private communications of millions of Americans? What is the cost in terms of loss of public trust in democratic and accountable government? What are the opportunity costs in terms of other security measures that could be funded to greater effect or without eroding core privacy rights of a free people?

These are difficult questions and some of the details underlying the answers are properly secret. But this administration has demonstrated time and again that its public statements on this and other intelligence issues are not credible and that it keeps facts secret that contradict its public assurances. The Congress cannot, consistent with its constitutional responsibility, legislate on this proposal without a much fuller public record and debate. Such a searching probe is essential to the preservation of the Constitution, no matter who is in the White House because, as the framers understood and provided against, over-reaching represents the fundamental tendency of individuals and factions in power, especially in times of national threat.

On Warrantless Access to Foreign-to-Foreign Communications.

The DOJ's Fact Sheet on the bill claims that it "would . . . protect civil liberties and privacy interests and improve our intelligence capabilities by focusing FISA on people located in the US. Revolutions in telecommunications technology have brought within FISA's scope communications that Congress did not intend to be covered—and, as a result, extensive resources are now expended obtaining court approval for acquiring communications that do not directly or substantially involve the privacy interests of Americans." But, as outlined above, the

administration would expressly delete long-standing privacy protections for the millions of people in the US by *exempting* the acquisition and later analysis of all international conversations from FISA. We would agree, however, that in crafting FISA Congress did not intend to place rules on the monitoring of what has been called "foreign-to-foreign" communications. That is why we support the tailored fix in Senator Feinstein's, S. 1114, which would deal with the new situation, in which the communications of two people outside the US who are not US persons are routed through US switches, by making clear no warrant is needed for that. The administration's proposed language goes way beyond that fix.

Similarly, if the government does not have enough resources to process FISA warrants for searching Americans' conversations or homes in order to protect both security and privacy, it should endorse Senator Feinstein and Congresswoman Harman's proposals to provide more resources for the FISA process.

All three branches must act to safeguard civil liberties consistent with the needs of national security and there must be a public debate.

Having seen that executive branch rules and congressional oversight were insufficient to protect civil liberties and national security without statutory rules, Congress enacted FISA. It also reiterated that public debate is necessary for a proper resolution of the terms of such laws.

> This evidence alone should demonstrate the inappropriateness of relying solely on executive branch discretion to safeguard civil liberties . . . . Even the creation of intelligence oversight committee should not be considered a sufficient safeguard, for in overseeing classified procedures the committees respect their classification, and the result is that the standards for and limitations on foreign intelligence surveillances may be hidden from public view. In such a situation, the rest of the Congress and the American people need to be assured that the oversight is having its intended consequences–the safeguarding of civil liberties consistent with the needs of national security. **While oversight can be, and the committee intends it to be, an important adjunct to control of intelligence activities, it cannot substitute for public laws, publicly debated and adopted, which specify under what circumstances and under what restrictions electronic surveillance for foreign intelligence purposes can be conducted.** Finally, the decision as to the standards governing when and how foreign intelligence electronic surveillance should be conducted is and should be a political decision, in the best sense of the term, because it involves the weighing of important public policy concerns–civil liberties and national security . . . . Under our Constitution legislation is the embodiment of just such political decisions.

H. REP. NO. 95-1283, at 21-22 (emphasis added). We firmly believe that the administration's proposal would circumvent the purpose of FISA through clever re-definition of what is governed

by FISA's warrant requirements, even though the statute "was designed . . . to curb the practice by which the Executive Branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it." S. Rep. No. 95-604(I), at 7, 1978 USCCAN 3904, 3908. The administration's proposal would resurrect that practice and seeks to do so without any informed public debate about its intention. We commend the Committee for its oversight and inquiry thus far. Changes this far-reaching *require* extensive public debate.

Conclusion. In FISA, Congress recognized since the beginning of the digital revolutions that emerging technology requires more protections for privacy rather than fewer, as more and more human thought and speech is committed to electronic documentation. As Senator Sam Ervin, the chief architect of the Privacy Act, which was intended to prevent computerized government dossiers, put it:

> [D]espite our reverence for the constitutional principles of limited Government and freedom of the individual, Government is in danger of tilting the scales against those concepts by means of its information gathering tactics and its technical capacity to store and distribute information. When this quite natural tendency of Government to acquire and keep and share information about citizens is enhanced by computer technology and when it is subjected to the unrestrained motives of countless political administrators, the resulting threat to individual privacy makes it necessary for Congress to reaffirm the principle of limited, responsive Government on behalf of freedom . . . . Each time we give up a bit of information about ourselves to the Government, we give up some of our freedom. For the more the Government or any institution knows about us, the more power it has over us. When the Government knows all of our secrets, we stand naked before official power. Stripped of our privacy, we lose our rights and privileges. The Bill of Rights then becomes just so many words.

Senator Ervin, on June 11, 1974, *reprinted in* LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974, S.3418, at 157 (Public Law 93-579)(Sept. 1976).

The Center for National Security Studies appreciates the Committee and its staff for considering these vitally important issues. We have set forth our request for additional public hearings on these matters, in a joint letter with other organizations submitted to the Chairman. We have also transmitted for the record a rebuttal of additional arguments made by the administration in its press relations regarding this proposed legislation (such as relating to data-mining, immunity, and other serious concerns we have regarding the bill). We hope this is the beginning of many public hearings on these matters, and we thank you for considering our views on this proposal.