Testimony of

General Michael V. Hayden

July 26, 2006

Testimony to the Judiciary Committee of the US Senate
By General Michael V. Hayden,
Director, CIA

26 July 2006

Mister Chairman, Senator Leahy, thank you for the opportunity to speak before your committee today. The work that you and we have before us is truly important: how dowe best balance our security and our liberty in the pursuit of legitimate foreign intelligence. Let me congratulate the Committee for taking on the task of examining and--where appropriate--amending the Foreign Intelligence Surveillance Act.

This task of balancing liberty and security is one that those of us in the intelligence community take very seriously and one to which we constantly turn our attention.

I recall that within days of the 9-11 attacks 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: right now a quarter billion Americans wished they had your job. I ended the talk by trying to give perspective. 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."

This was not an easy challenge. The Joint Inquiry Commission (comprised of the House and Senate Intelligence Committees) would summarize our shortcomings in the months and years leading to the September 11th attacks. The Commission harshly criticized our ability to link things happening in the United States with things that were happening elsewhere.

Let me note some of JIC's Systemic Findings (Joint HPSCI-SSCI, from abridged findings and conclusions)

"...NSA's cautious approach to any collection of intelligence relating to activities in the United States" (finding 7)

"There were also gaps in NSA's coverage of foreign communications and the FBI's coverage of domestic communications" (Finding 1, p 36, tab 4)

"...NSA did not want to be perceived as targeting individuals in the United States." (Finding 1, p 36, tab 4)

"[in talking about one end US conversations]...there was insufficient focus on what many would have thought was among the most critically important kinds of terrorist related communications, at least in terms of protecting the homeland." (Finding 1, p. 36, tab 4)

For NSA the challenge was especially acute. 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 very difficult. The explosion of modern communications in terms of its volume, variety and velocity threatened to overwhelm the Agency.

The September 11th attacks exposed an even more critical fault line. The laws of the United States do (and should) distinguish between the information space that is America and the rest of the planet.

But modern telecommunications do not so cleanly respect that geographic distinction. We exist on a unitary, integrated, global telecommunications grid in which geography is an increasingly irrelevant factor. What does "place" mean when one is traversing the World Wide Web? There are no area codes on the Internet.

And if modern telecommunications muted the distinctions of geography, our enemy seemed to want to end the distinction altogether. After all, he killed 3000 of our countrymen from within the homeland.

In terms of both technology and the character of our enemy, "in" America and "of" America no longer were synonymous.

I testified about this challenge 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 some 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.

The legal regime under which NSA was operating--the Foreign Intelligence Surveillance Act--had been crafted to protect American liberty and American security.

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 was optimized to deal with a 9/11 or to deal with a lethal enemy who likely already had combatants inside the United States.

Because of the wording of the statute, the government looks to four factors in assessing whether or not a court order was required before NSA can lawfully intercept a communication: who was

the target, where was the target, how did we intercept the communication, and where did we intercept the communication.

The bill before the committee today effectively re-examines the relevance of each of these factors and the criteria we want to use with each.

Who is the target?

The FISA regime from 1978 onward focused on specific court orders, against individual targets, individually justified and individually documented. This was well suited to stable, foreign entities on which we wanted to focus for extended period of time for foreign intelligence purposes. It is less well suited to provide the agility to detect and prevent attacks against the homeland.

In short, its careful, individualized processes exacted little cost when the goal was long term and exhaustive intelligence coverage against a known and recognizable agent of a foreign power. The costs were different when the objective was to detect and prevent attacks, when we are in hot pursuit of communications entering or leaving the United States involving someone associated with al Qa'ida.

In this regard, extending the period for emergency FISA's to seven days and allowing the Attorney General to delegate his authority to grant emergency orders is also very welcome and appropriate.

Where is the target?

As I said earlier, geography is becoming less relevant. In the age of the Internet and a global communications grid that routes communications by the cheapest available bandwidth available each nanosecond, should our statutes presume that all communications that touch America should be equally protected?

As the Chairman noted earlier this week, we do not limit our liberties by exempting from FISA's jurisdiction communications between two persons overseas that gets routed through US facilities.

Our limited government resources should focus on protecting US persons, not those entities who get covered as a result of technological changes that extend the impact--and protection--of FISA far beyond what its drafters intended.

I know that Senator DeWine among others has been very concerned about allocations of these resources and FISA backlogs. As Director of CIA I share his concerns in allocating my resources and hope that this legislation will help properly focus resources on protecting the legitimate privacy rights of US persons.

How did we intercept the communication?

For reasons that seemed sound at the time, current statute makes a distinction between collection "on a wire" and collection out of the air. When the law was passed, almost all local calls were on

a wire and almost all long haul communications were in the air. In an age of cell phones and fiber optic cables, that has been reversed...with powerful and unintended consequences for how NSA can lawful acquire a signal. Legislators in1978 should not have been expected to predict the future of global telecommunications. Neither should you. The statute should be technology neutral.

Where we intercept the communication?

A single communication can transit the world even if the communicants are only a few miles apart. And in that transit NSA may have multiple opportunities to intercept it as it moves and changes medium. As long as a communication is otherwise lawfully targeted, we should be indifferent to where the intercept is achieved. Signals intelligence is a difficult art and science, especially in today's telecommunication universe. Intercept of a particular communication--one that would help protect the homeland, for example--is always probabilistic, not deterministic. No coverage is guaranteed. We need to be able to use all the technological tools we have.

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. And so why should our laws make it more difficult to target the al Qa'ida communications that are most important to us--those entering or leaving the United States!

Because of the nature of global communications, we are playing with a tremendous home field advantage and we need to exploit this edge. We also need to protect this edge and those who provide it. The legislative language requiring compulsory compliance from carriers is an important step in this regard.

After 9/11, patriotic Americans assisted the Intelligence Community in ensuring that we have not had another attack on our soil since that awful day. And prior to 9/11, we received critical assistance across the IC from private entities. As Director of NSA, Deputy DNI, and now Director of the CIA, I understand that government cannot do everything. At times, we need assistance from outside the government.

Whatever legal differences and debates may occur about separation of powers, Article 2, and so on, those people who provide help to protect America should not suffer as a part of this debate. I would urge the committee to recognize the importance of the efforts of these Americans and provide appropriate protection.

One final--and very important--point. Many of the steps contained in the proposed legislation will address the issue raised by the Congress' Joint Inquiry Commission: one end US conversations, communications that the JIC characterized as "among the most critically important kinds of terrorist related communications, at least in terms of protecting the homeland."

That means NSA will bump up against information to, from or about US persons. Let me stress that NSA routinely deals with this challenge and knows how to do this while protecting US privacy. The draft bill contains quite a bit of language about minimization--the process NSA uses

to protect US identities. The same rules of minimization that NSA uses globally, rules approved by the Attorney General and thoroughly briefed to Congress, will be used.

Let me close by saying that we have a great opportunity here today. We can meet the original intent of the FISA Act to protect our liberty and our security by making the legislation relevant to both the technologies and the enemies we face.

Thank you.