Lt Gen Michael V. Hayden, USAF, Director, National Security Agency
Address to Kennedy Political Union of American University
17 February 2000

Good evening and thanks for coming. I'm excited to be here and at the same time a little apprehensive. It seemed natural to ask my staff to learn about the Political Union and its speakers in order to gauge my remarks towards your interests. After all, we're in the information gathering and assessment business so it should be easy for us to come up with something that would complement what you've heard from other speakers in the series.

…But when I heard that I was following Jerry Springer...well, I wasn't sure that I was going to meet your expectations. Despite what you've seen on television, our agency doesn't do alien autopsies, track the location of your automobile by satellite, nor do we have a squad of assassins…if we did, I guess that Springer wouldn't be such a tough act to follow.

I think that the best I can hope for now is to wipe away some of the mystique surrounding the National Security Agency so that you better understand us and how we add value to America.

Today, the world, our nation, and my agency are faced with new challenges and opportunities. I'd like to share my thoughts with you on the nature of those challenges and how they redefine national security, and leave you with some thoughts on how we at NSA intend to deal with them.

Let's begin with a little history lesson:

A memorandum from President Truman established NSA in 1952, stating that "the communications intelligence activities of the United States are a national responsibility."

Our charter, a Department of Defense document, creates "a unified organization structured to provide for the signals intelligence (SIGINT) mission of the United States and to insure secure communications systems for all departments and agencies of the U.S. government."

Our mission was clearly important, but those were 47 years and 28 years ago, respectively. Our most recent "founding document," an Executive Order from President Reagan, reaffirms both the importance of intelligence and the principles guiding its collection.

Please indulge me a moment while I quote chapter and verse; it speaks to the core of my point this evening: "accurate and timely information about the capabilities, intentions and activities of foreign powers, organizations, or persons and their agents is essential to informed decision making in the areas of national defense and foreign relations."

"Collection of such information is a priority objective and will be pursued in a vigorous, innovative and responsible manner that is consistent with the constitution and applicable law and respectful of the principles upon which the United States was founded."

Let me give you an example of the tenacity required to produce signals intelligence. The VENONA Project was a program to examine and if possible, exploit encrypted Soviet diplomatic communications.

Three years after a 1944 cryptanalytic breakthrough, Meredith Gardner, one of the VENONA analysts, was able to read two KGB messages revealing that someone inside the War Department general staff was providing highly classified information to the Soviets.

VENONA translations pointed to over 200 named or covernamed persons then present in the U.S. claimed by KGB and soviet military intelligence messages as clandestine assets or contacts. The messages disclose some of the clandestine activities of Julius and Ethel Rosenberg, Harry Gold, Klaus Fuchs, David and Ruth Greenglass, and others involved with atomic bomb espionage.

As for the importance of our mission to national decision making of the gravest nature, consider the role signals intelligence played in managing the Cuban Missile Crisis. NSA collected early indications of the arms buildup beginning in Cuba, exploiting Soviet communications concerning ships headed to Havana—ships whose cargo manifests were suspiciously blank.

As early as 1960, American intercept operators began hearing Spanish along with the usual Slavic languages coming from airfields in Czechoslovakia. Not long thereafter, intelligence sources got wind of state of the art fighter and light bomber deliveries to Cuba. Soon, Cuba had a fully functional Soviet-style air defense system, complete with the SA-2 surface-to-air missile which had downed U-2 pilot Gary Powers in 1960. What were they hiding?

After hazardous U-2 flights over Cuba confirmed the presence of Soviet offensive missiles, President Kennedy ordered a naval "quarantine" of the island to stop any further arms deliveries. In the tense situation that followed, it was signals intelligence that confirmed that Soviet ships would not challenge the Americans enforcing the quarantine.

These founding principles of SIGINT helped us to win the cold war. Competing priorities were not an issue with The Bear to focus our attention. Funding, in light of that clear threat to America, was vigorous and consistent. The environment has changed dramatically but our relevance has only increased. Let's talk about this environment a little...

We are an agency in change. In this new era, the global environment is no longer defined using a map. You of all people are aware that we're right in the middle of a technological revolution and it's that revolution which has made what I say true. To illustrate:

Twenty years ago, how many people outside of government or research used a computer—much less had one at home? Forty years ago there were 5,000 stand-alone computers, no fax machines and not one cellular phone. Today, there are over 180 million computers -- most of them networked. There are roughly 14 million fax machines and 40 million cell phones and those numbers continue to grow.

The telecommunications industry is making a $1 trillion investment to encircle the world in millions of miles of high bandwidth fiber-optic cable. They are aggressively investing in the future. As private enterprise transitioned from the Industrial Age to the Information Age, so must government. So far, the National Security Agency is lagging behind.

For example, you may have heard about the recent network outage at NSA. Due to a software anomaly, our aging communications infrastructure failed and our ability to forward intelligence data, process that data and communicate internally was interrupted for 72 hours. Thousands of man-hours and $1.5 million later, we were able to resume normal operations.

For others, technology is an enabler. It's an investment that makes their jobs easier. For NSA, technology is the foundation upon which all of our processes rest; it is not an option. The network outage was a wake-up call to our stakeholders and us that we can no longer afford to defer the funding of a new infrastructure. And the challenge doesn't stop there.

Advancements in telecommunications and particularly the Internet have highlighted a fundamental, but not necessarily new privacy issue. Simply put: how do we balance the need for foreign intelligence information with the responsibility to protect individual privacy rights? What standard do we use as a society to make that determination?

I would note here that all of us who deal with communications have to deal with privacy issues. The system administrator of your campus computer network has to deal with it, so must your Internet service provider, your telecommunications carrier, and law enforcement agencies. NSA, a signals intelligence (SIGINT) and information systems security (INFOSEC) agency, also has to deal with it. We deal with privacy issues in different ways depending upon the type and purpose of activity involved.

You've probably all read by now some of the recent press reports on NSA. The Washington Post and the New Yorker Magazine speculate 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

have also been referred to as, "a global spying network that can eavesdrop on every single phone call, fax, or e-mail, anywhere on the planet."

Those of us who have been around awhile recall hearing about the Church and Pike investigations of the mid-1970's. After lengthy investigations, the House and Senate committees concluded that NSA had not given appropriate weight to privacy considerations in conducting its signals intelligence mission.

As a result, Congress passed a law called the Foreign Intelligence Surveillance Act regulating electronic surveillance in the United States. Both houses of Congress established permanent intelligence oversight committees to ensure compliance. Moreover, President Ford issued an Executive Order which both authorized and set limits on the conduct of intelligence activities. As a result, the legal and policy context for intelligence activities was forever and dramatically changed.

Now, if you've seen "Enemy of the State" you might believe that the NSA's intelligence gathering mission offers the greatest threat to the privacy of network users. Like many people, you may not be aware of the laws and regulations under which the NSA operates, and the rigorous oversight applied to those operations to ensure our compliance.

So how do we reconcile the government's need for foreign intelligence information with the need to protect individual privacy rights? We do this through a series of procedures outlined in the Executive Order, approved by the Attorney General and the Secretary of Defense, and vetted with the Congressional intelligence oversight committees.

The procedures recognize two important facts: first, there are times when a government needs to collect information about its citizens. The circumstances under which this is allowed to occur either inside or outside the U.S. are extremely limited and well-regulated. Basically, there must be probable cause that a person is an agent of a foreign power and a court must issue a warrant authorizing the surveillance inside the U.S. The Attorney General, applying the same standard of probable cause, must authorize surveillance when the person is outside the U.S. For example, suppose that a foreign country has recruited a U.S. citizen to commit a terrorist act against the U.S. When that person travels abroad, he may be surveilled only if the U.S. government has demonstrated probable cause that he is a terrorist or is aiding and abetting terrorists. Under our legal system, probable cause means that you must have facts that would convince a reasonably prudent person that what you're saying is true.

The second fact that the procedures recognize is that it is inevitable that NSA will inadvertently acquire information about U.S. citizens in the course of its foreign intelligence collection activities. An example of this might be when we have intelligence of two foreign agents discussing the recruitment of a U.S. citizen. When that happens, the procedures require that NSA "minimize" the retention and dissemination of such information. In other words there are rules imposed upon us by law and regulation that

say, "NSA, you may only keep and disseminate such information under a very limited set of circumstances." Circumstances like when the life of the U.S. person is in danger; they are the target of a foreign power or the agent of a foreign power.

So, contrary to some articles written about the Agency, there are rules governing NSA activities. The Department of Justice, the Department of Defense, and the Congressional committees all participate in their formulation and oversight.

But the question remains, how can the American people be confident that we abide by the rules?

First, we train our employees to make sure they know them. Each year our Office of General Counsel conducts hundreds of training sessions specifically designed to maintain a legally sensitized work force -- to make sure our employees recognize privacy issues and know how to deal with them appropriately. If for whatever reason, an employee fails to make his or her annual training, his or her access to intelligence databases is automatically denied.

Second, there is an elaborate oversight process in place. The NSA General Counsel, the Inspector General, and a Senior Intelligence Oversight Board perform this function within the Agency. Within the Executive branch -- the Department of Defense, the Department of Justice and the President's Foreign Intelligence Oversight Board conduct oversight of NSA. On the legislative side, the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence scrutinize NSA's activities as the people's representatives to ensure compliance with the Constitution, law, and regulations.

The bottom line is we are responsible citizens. We know what the rules are and we abide by them. We try to maintain a steady heading. Ironically, at times, we are criticized for being too conservative. My philosophy is a simple one:

A) We can't be careless or risk takers where the privacy rights of U.S. citizens are involved. We have to do it right.
B) We have to behave in such a way that the American people can be confident that we are not abusing the tremendous power they authorize us to exercise.

Weapons of mass destruction — especially chemical and biological weapons — are becoming a threat to U.S. soil for the first time. The threat of cyber-attack, or information warfare by our adversaries now has the potential for mass disruption of our nation's infrastructure. At a time when our national security is at its most vulnerable, it would be more than irresponsible and illegal to take liberties with our authorities. We put at risk our legitimate intelligence mission and that means we put America at risk.

The information we collect and the information we protect is the ultimate opportunity cost. NSA employees do not simply decide on a daily basis how and what

they will collect and exploit. We are driven by requirements levied upon us by national level military and civilian decision-makers. Put yourself in their place...

- Do you want to understand the intentions of terrorist groups?
- Do you want to know these groups have an interest in gaining knowledge of the United States communications and utility infrastructure?
- Do you want to know the status of a rogue state's military capabilities?
- Do you want to guarantee our military command authorities secure communications regardless of their location?
- Do you want to stop a foreign intelligence officer from penetrating our government networks?

The price tag for new information capabilities is high, but the alternatives are unthinkable. The Director of Central Intelligence, George Tenet recently characterized the situation during his address at Georgetown by quoting Pogo – a comic strip by the late Walt Kelly – Pogo said, "we are faced with insurmountable opportunities."

Let me add that we don't just attack or acquire information. We also protect it, especially national security information. In addition, we cooperate with American industry in setting standards for commercial encryption so that your information is protected.

I noted earlier how much the world is changing. NSA is changing, too. Just look at the very fact of my presence here tonight. Our Agency benefited in the past from the high walls of security we placed around our activities during the cold war. However, we've paid a price. While security and secrecy kept critical information well protected inside, they also kept some important things on the outside from influencing our growth as an Agency. We can no longer afford to operate that way. The knowing few have always been well aware of the fact that NSA is a national treasure. At the same time, they are much less aware of the weight of our challenges at a time when our human and fiscal resources have declined in the past two decades. Moreover, the media and the public have some misperceptions about our business that do an injustice to the men and women who serve tirelessly in their efforts to protect and defend through their cryptologic disciplines.

We are at a historic decision point.

The 21st century represents unprecedented opportunities and more diverse and dispersed threats. Just as we organized to meet the challenges of the cold war, we must adapt to capitalize on the opportunities of the next millennium.

If we as a nation do not make serious, sustained investments in information security and intelligence over the next five to seven years, we may find that we have missed opportunities and foreclosed options that we will dearly wish we had left available (DCI, 18 Oct 99).

Isaac Asimov said, "it is change, continuing change, inevitable change, that is the dominant factor in society today. No sensible decision can be made any longer without taking into account not only the world as it is, but the world as it will be." He was right—to be successful, we have to be visionary, opportunistic and willing to manage risk as opposed to avoid it.

We need fresh, innovative and creative viewpoints. Viewpoints from people like you -- you all are part of the future for America. As you move into positions of influence in the private and public domains, I encourage you to challenge the status quo, become a champion for continuous improvement and learning, and to not allow personal and organizational precedence to govern your behavior.

I didn't mean to turn this into a recruiting pitch, but I would be remiss if I failed to mention that we will be aggressively hiring new talent in a variety of core skill areas as we begin a process of revitalizing our workforce. If you're thinking about public service and would like career opportunities which are challenging, exciting, and rather, well…very cool, I encourage you to examine these businesses we call SIGINT and INFOSEC at the National Security Agency.

Thank you for the invitation and the opportunity to share my thoughts. I'd be happy to take your questions.