JOHN M. POINDEXTER
[redacted]

12 August 2003

Dr. Anthony Tether
Director
Defense Advanced Research Projects Agency
[redacted]

Dear Tony:

After the horrific attacks against the United States on 9/11, I felt compelled to do what I could to make sure that never happened again. I had been thinking of how to combat terrorism for some 20 years. I was not anxious to come back into government, but in discussions with you and others concluded that was probably the best way to explore research and development of information technologies and concepts to help solve the enormous problems of combating terrorism. So I agreed to accept an appointment for a limited period of time to start a new office within DARPA specifically focused on imaginative uses of new information technology tools to help in the war against terrorism. Now I have decided it is time for me to step down.

Some of the research and development programs that we have been working on have become controversial and I want to take this opportunity in an open letter to you to put these controversies in perspective. Although we have tried to be very open about our work there is still a great deal of misunderstanding.

Many people do not understand the Defense Advanced Research Projects Agency (DARPA). After the Soviet Union launched Sputnik in 1957 the United States was facing a significant threat in the Cold War. President Eisenhower established a new agency in the Department of Defense charged with imagining and developing new innovative technology solutions to difficult national security problems. It was called Advanced Research Projects Agency (ARPA). In later years Defense was added to the title. ARPA/DARPA has had many successes including the development of rockets to give the United States access to space, Stealth technology to make vehicles more immune to detection by radar, various unmanned vehicles such as Predator and Global Hawk, and of course ARPAnet (the predecessor to the Internet), plus many other technologies too numerous to mention. DARPA is respected world-wide for its preeminence in research and development. The reasons that DARPA has been successful in my view are three-fold. Program Mangers are given the freedom to think "outside the box" and even draw new boxes to come up with solutions that others might not think possible. Congress has always provided substantial funding to explore many ideas – some of which are successful and others are not. DARPA does not do the research itself, but instead harnesses the incredible creativity of the American people, universities, and industry.

DARPA is a tool builder and not a tool user. Technology solutions are developed and shown to work. It is then up to user agencies and Congress through the normal authorization and appropriations process to decide whether the technology solutions will be implemented and under what conditions. DARPA is not the eventual user of the technologies that are developed.

In the research and development process DARPA routinely works with user agencies of the DOD, the Intelligence Community, and other agencies of the government on national security problems to test and experiment with the technology solutions to prove that they work before transition to an acquisition program and operational implementation takes place. This is certainly the case with the programs of my office.

The national security problem of terrorism, which we sometimes call the asymmetric threat since it pits the United States and other friendly countries of the world -- not against another state -- but against a confederation of terrorist groups who have no national boundaries, began to be a problem in the last two decades of the last century. However the consequences of the terrorist attacks are rapidly becoming more severe and intolerable as demonstrated by the attacks of 9/11 and the bombings in Saudi Arabia, Indonesia and elsewhere throughout the world. It is a world-wide problem. The attacks on the World Trade Center and the Pentagon brought the war to our home; giving us a war on two fronts – at home and abroad. There have been numerous reports and commentaries about what went wrong in preventing the government from detecting the attack planning and thus stopping the attacks. Some planning and preparation activity took place overseas and some took place here in the U.S. This greatly complicates a solution to the problem since it involves a better interface between foreign and domestic intelligence organizations of our government.

For good and sufficient reasons, we have kept these organizations separate, but if we are going to be successful in the future we must find a way for them to work together within a framework that is effective and at the same time preserves the essential character of our republic. More than half of the foreign intelligence activities are in the Department of Defense and report to both the Secretary of Defense for resources and Director of Central Intelligence for tasking. The DOD clearly has a significant foreign intelligence role and it is appropriate that DARPA be involved in looking for technology solutions. DARPA is in a position to take a fresh look at the problem with no vested bureaucratic interests in coming up with an integrated solution. The technology and tools to be developed for the foreign part would be just as applicable to the domestic part; however if and when it comes to implementation the foreign intelligence activities of the DOD, CIA and others would apply the tools against foreign intelligence data and domestic intelligence activities, such as the FBI, would apply them against domestic intelligence in accordance with the laws and polices. In no case would DARPA be applying the tools. There are extensive Congressional oversight provisions for the foreign and domestic intelligence activities to detect any potential abuses.

As you know as our research has evolved we have had basically two research paths – each in the context of a premise. The first premise is that the U.S. government has all of the data it needs to find information that would allow us to detect foreign terrorists and their plans and thus enable the prevention of attacks against U.S. interests. The problems here are a matter of sharing this information amongst the various agencies involved and providing better ways of finding information more rapidly, tools to aid in conducting faster and better analyses and decision support tools to enable better decisions. The massive amounts of data that are presently available under existing laws and policies far exceed the capacity of the humans in the system to analyze these data without tools to aid them . In fact these are exactly the problems identified by the Congress in their reports on the events surrounding the attacks of 9/11. On this first research

path we created an experimental network called TIA and partnered with nine foreign intelligence, counter-intelligence and military commands for testing experimental tools using foreign intelligence data that is currently available to them. Because of the urgency of the problems we did not want to develop the tools in a sterile laboratory environment, but instead place them in the real world where they could be tested by real users working on real problems. We held our first TIA Users Conference with the agencies and commands that are participating in the experiments a few weeks ago and there was enthusiastic support and excitement about the potential value of our work in solving the difficult problems they face in combating the terrorist threat. The work under this premise should not be controversial in the U.S. since the tools are being applied using foreign intelligence data and as I have said is completely responsive to the problems the Congress has raised with respect to 9/11. A recent experiment with TIA indicates analyses can be conducted in less than $1/10^{th}$ the time with a much greater percentage of the time spent on actual analysis (the thinking part) and less percentage spent on finding the information and producing the reports. With people who are willing to take the time to understand what we are doing and have accomplished, there is nearly unanimous support for our work. The research and development along this path is distinct from that of a second path which I describe next.

If we are wrong on the first premise and the U.S. government does not have all of the data it needs to find the terrorists and prevent their attacks, we felt it prudent to explore a second research path. This is the controversial one. In terms of the recent flap over FutureMap – did we want to bet the safety of thousands if not millions of Americans that our first premise was correct? Since we didn't want to make that bet, we devoted a relatively small portion of the funds that had been made available to us to this second research path. There is another community of people who believe that all the data necessary to effectively counter the terrorism threat is not entirely in government databases. Instead, there may be more information in the greater information space that might prove valuable for the government to exploit in its counterterrorism operations, but currently this data is not used due to legal or policy restrictions. This research path is testing the hypothesis that when terrorist organizations engage in adverse actions against the United States, they make transactions in support of their plans and activities, and those transactions leave a signature in the information space. Those transactions will likely span government, private, and public databases.

The challenges for the supporting TIA programs in this second research path are twofold: First, is the signature detectable when embedded within a world of information noise? Second, in what part of the information space does that signature manifest itself? Ultimately, our goal within this thread is to understand the level of improvement possible in our counterterrorism capabilities if the government were able to access a greater portion of the information space, while at the same time considering the impact—if any—on information policies like the right to privacy, and then mitigate this impact with privacy protection technology. If our research does show an improvement in the government's ability to predict and preempt terrorism, then it would be up to the policymakers, Congress, and the public at large—not DARPA—to decide whether to change law and policy to permit access to such data. Because the government today does not access some types of transactional data that may prove meaningful, all of this research is being done with synthetic, simulated data. Recent results from the preliminary testing with the synthetic data are encouraging that we will be able to find patterns of transactions that are indicative of terrorist planning and preparations.

We knew from the beginning that this second research path would be controversial and if the research proved successful, we would have to solve the privacy issue if it were ever to be deployed. We did not want to make a trade off between security and privacy. It would be no good to solve the security problem and give up the privacy and civil liberties that make our country great. The privacy issue is not just a U.S. issue. Many of our friends and allies also have strict privacy laws and if a wider array of transaction data was to be searched in foreign data, the problem for them would also have to be solved. There is also the question of privacy for sensitive intelligence sources and methods if more and more information is to be shared amongst the agencies. We needed to find a solution for all three concerns: privacy of US citizens, privacy of foreign citizens and privacy of sources and methods.

In early 2002, shortly after the new office was formed, we began a study called Security with Privacy to imagine ways technology could be developed to preserve the privacy of individuals and still search through data that is not currently available to the government looking for specific patterns of activity that are related to terrorist planning and preparation activities. The problem here is that because of our free societies, which we rightfully cherish and want to preserve, the terrorist has been permitted to come amongst us. Their activities take place amidst all of the innocent activity of everyday life. We don't always have the identities of these terrorist and so there will always be the possibility of "sleeper cells". The only way to detect them is by looking for patterns of specific activities that have proven in the past or estimated for the future to be indicative of terrorist planning. We never contemplated spying and saving data on Americans. We only wanted to find specific patterns of activities that would lead us to foreign terrorists. To conduct the research under this premise we have been using synthetic data that is representative of the real world.

The Security with Privacy Study, which was completed in the fall of 2002, produced some very interesting, imaginative ideas and we contracted with researchers to pursue innovative techniques to protect the privacy of innocent people as well as technologies to provide an effective method of oversight to deter abuse. Since that time we have identified other techniques that, if developed, might enable machine searches through data in such a way that the identity of people would be concealed until a proper case was made and presented to the appropriate authorities. Only then would the identity of the people in question be revealed.

From the beginning we decided to be very open about our vision and research – not secretive. In January 2002, I came back into government and we established the Information Awareness Office. In March 2002, only 6 months after the attacks, we issued a public announcement asking for research ideas in the areas of our interest. In May 2002 we opened an Internet Web site to the public which explained our objectives. In August 2002 I spoke to a conference of about 2000 researchers and trade press and explained our vision and the directions of our work. All of these things are on the record. In November 2002 after our work had been badly mis-represented in the major media, it was decided that I should not speak publicly to provide a defense and explanation of our work since I was such a "lightning rod" (not my words). In May 2003 we prepared a 100 page "Report to Congress Regarding the Terrorism Information Awareness Program" which Secretary Rumsfeld sent to the Congress after coordinating with the

Director of Central Intelligence and the Attorney General. This report even explained FutureMap, which was most recently distorted in press conferences and the media. Admittedly one of the contractors made this distortion possible by using some extremely bad examples that had not been approved. In the highly charged political environment of Washington positions on highly complex issues are taken and debated using glib phrases, "sound bites" and symbols. I doubt that many people have read our Report to Congress to get a balanced view of what we have been trying to do.

As you know I have wanted to step down for months now, but at your request agreed to stay on for a while longer to shepherd the research and development programs toward greater maturity. We have made significant progress with the TIA experimental network under the first premise that the government today has access to all the information it needs. The user agencies and commands are finding the tools and concepts valuable. There is a long way to go yet, but progress has been made. The work under the second premise is very much still in the research phase and obviously still controversial. I regret we have not been able to make our case clear and reassure the public that we do not intend to spy on them. I think I have done all that I can do under the circumstances and therefore request that you accept my resignation from government effective August 29, 2003. This will provide time for a smooth transition of my responsibilities.

In closing I want to thank you personally for the opportunity and support to pursue my ideas about how the United States can combat terrorism more effectively. DARPA traditionally takes on very hard problems (what we call DARPA-hard) and often comes up with imaginative, independent, fresh approaches to solving very difficult problems for the national security community. Sometimes these solutions are not without controversy. When DARPA was developing the Stealth technology, I can recall from my White House years that the Air Force wanted to quit buying the first version of the aircraft before it was publicly acknowledged we had such a radar-avoiding capability. It was too much of a radical change. Fortunately we did not stop.

The United States and free-world continue to face an enormous threat to our freedom and way of life by those who choose to use terrorism to destroy what we cherish – the ultimate threat to our privacy. The Senate version of the Defense Appropriations Bill going into conference with the House on September 2 eliminates funding for most of the counter-terrorism programs of my office – both the non-controversial as well as the controversial. I hope a compromise can be reached that will permit a continuation of at least the non-controversial parts. It is my sincerest hope that our country's children and grandchildren can understand that, in my opinion, the complex issues facing this nation today may not be solved using historical solutions and rhetoric that has been applied in the past, and that it may be useful to explore complex solutions that sometimes involve controversial technical concepts in order to rediscover the privacy foundations of this nation's strength and the basis for its freedoms.

Very respectfully,