NATIONAL ACADEMY OF SCIENCES

COMMITTEE ON A NEW GOVERNMENT-UNIVERSITY PARTNERSHIP FOR SCIENCE AND SECURITY

NORTHEAST REGIONAL MEETING

May 16, 2006

Massachusetts Institute of Technology
70 Memorial Drive
Cambridge, Massachusetts

NOTE: This is an unedited verbatim transcript of the workshop on a New Government-University Partnership for Science and Security held at the Massachusetts Institute of Technology on May 15-16, 2006. It was prepared by CASET Associates and is not an official report of The National Academies. Opinions and statements included in the transcript are solely those of the individual persons or participants at the workshop, and are not necessarily adopted or endorsed or verified as accurate by The National Academies.

Proceedings By:

CASET Associates, Ltd.
10201 Lee Highway, Suite 180
Fairfax, Virginia 22030
(703)352-0091

List of Participants:

Jacques S. Gansler

Alice P. Gast

Sheila S. Jasanoff

George Church

Judith Reppy

Sue E. Eckert

Suzanne Berger

Debra W. Stewart

Timothy Bereznay

Eugene B. Skolnikoff

Charles M. Vest

NOTE: This is an unedited verbatim transcript of the workshop on a New Government-University Partnership for Science and Security held at the Massachusetts Institute of Technology on May 15-16, 2006. It was prepared by CASET Associates and is not an official report of The National Academies. Opinions and statements included in the transcript are solely those of the individual persons or participants at the workshop, and are not necessarily adopted or endorsed or verified as accurate by The National Academies.

TABLE OF CONTENTS

NOTE: This is an unedited verbatim transcript of the workshop on a New Government-University Partnership for Science and Security held at the Massachusetts Institute of Technology on May 15-16, 2006. It was prepared by CASET Associates and is not an official report of The National Academies. Opinions and statements included in the transcript are solely those of the individual persons or participants at the workshop, and are not necessarily adopted or endorsed or verified as accurate by The National Academies.

P R O C E E D I N G S (8:55 a.m.)

DR. GANSLER: If you will take your seats, since we have a lot of academics we are starting ten minutes late, but that's enough, I think. We are still missing two of our panelists, but we are going to get started anyhow, and they will join us as they drift in.

Let me again thank all of you, both the committee and the audience, for attending what we think is a very, very important program. What we want to do first is simply repeat some of the administrative stuff that Alice mentioned yesterday. I'm Jack Gansler. Alice and I are the co-chairs of this committee. Yesterday Alice introduced all of the committee members who are sitting along the front row here. We also thanked our sponsors, NIH and NSF, and the encouragement that we received for this from the House Science Committee and OSTP. So there is a lot of interest around.

In fact, some of you may have seen in the paper this morning, they announced that a decision had been made by the White House on the deemed export controls, to delay for a year any implementation of that, and to try to take a more reasoned approach to it, bringing in advisors to meet

and get together between the government and universities to resolve this in a more thoughtful way.

I want to also remind you that this is an open session. It is being recorded. We will have an unedited transcript available on the website in a few weeks. When you do take part and I want to encourage you to take part, just introduce yourself by name and association so that we have that in the transcript.

Finally, I want to remind you that we have two more of these site visits planned, as required in our charter. We are going to be at Georgia Tech on June 5-6, and we are going to be at Stanford on September 27-28. Following those, the committee will then put together a proposed set of actions and findings, and we will then have a colloquium in Washington early next year. That is the overall plan for the activities.

This is a fact-finding session, so we want to greatly encourage people, not just on the panel but also in the audience to take part. Based on yesterday, we discussed last night the fact that to the extent we can, we want to encourage the panel and the audience to start moving in the direction of specific recommendations that

you might have, rather than simply describing the problem. I think we want to hear the problem, we want to understand the problem, and then we want to try to move towards a set of recommendations as this evolves in our various meetings.

So with that, I am going to turn it over to Sheila to both introduce herself to the panel and get us started.

Agenda Item: Panel: Concerns of the Academic Community

DR. JASANOFF: Thanks, Jack. My job will be to make sure that the panel does conform to that request. I think the panelists will begin with their opening statements, which may or may not be pushing us towards solutions. We will see how the discussion proceeds from there on out.

I am Sheila Jasanoff. I am professor of science and technology studies at the Kennedy School. I am happy to see the usual bimodal distribution of the audience that always seems to happen when I come to MIT. One has to develop peripheral vision to make sure that one sees everybody. I am glad to see as well that the panel is now complete.

George, is it okay if we do in fact go in the order of listing, or do you want to catch your breath a bit?

DR. CHURCH: Maybe I should catch a breath.

DR. JASANOFF: In that case, we will present with a slightly altered lineup of presenters, and begin with my very good friend Judith Reppy, with whom I was for a long time colleagues in the Cornell Department of Science and Technology Studies. You will find detailed biographies of all of our presenters in the booklets; I won't waste much time by going over that in detail.

Judith, please lead us off this morning.

DR. REPPY: Thank you. I have just recently converted to PowerPoint, so I am going to go stand over there so I can control the pointer.

I would like to start by making a few general remarks. MIT is obviously a great place to consider the question of government-university partnership in issues around science and security, because it was here in the years after the Second World War that a new relationship between the federal government and the scientists in the university was constructed.

That relationship is usually described in the language of a social compact, in which the university provided funds for R&D with very few strings attached, in the expectation that the results of the research would benefit both national security and the economy.

Academic freedom and open exchange of information were seen as absolutely essential to the vitality and productivity of the scientific enterprise, so the university was a natural site for basic research programs.

Fast forwarding, I would say that over time, people generally agree that the social compact has eroded. Following the Vietnam War, many academic scientists were less willing to work on security weapons related work, and the Defense Department became less likely to fund basic research. Cases of scientific fraud which called into question the integrity and trustworthiness of science and scientists led to increased government monitoring of scientific activities that were funded by the federal government. The growth in corporate-university partnerships has created potential conflicts of interest for scientists and to some extent further undermined their claims to operate free of oversight, because they may no

longer be seen as so disinterested.

I think other changes in the world have been very important, too. The ability of the state to monitor information flows across its borders has decreased with increase in globalization. Then of course, the subject of the Fink Committee on which I served, new areas of science and biotechnology have become newly relevant to national security. This has taken place without the benefit of an established relationship between the scientists and the security community which the physical and engineering sciences have enjoyed.

The governmental response to this change has been an increase in oversight and regulation of research, and that is what we are here to discuss. At least, that is my topic. In many cases, these new regulations have been implemented with very little regard for the core values of the university, namely, the free and open exchange of information and non-discrimination in treatment of students, faculty and staff. These problems have been exacerbated in times of crisis such as followed the 9/11 attacks and again, I think that is why we are here today.

There was a previous period in which it was seen

that there was a crisis. That was of course in the 1980s. At that time, President Reagan was persuaded to issue the national security Decision Document 189, which had this very important language in it. I am not going to read it to you, you can read it yourself, but basically it provided an exception for fundamental research from many of the regulations that had been put in place to govern export of technical information.

The FRE has been absolutely crucial in making the regulatory burden tolerable for universities. In fact, it was reaffirmed in November 2001 following 9/11 in a statement from Condi Rice to -- I have forgotten to who it was, but she wrote and said, yes, this is still the law of the land, and today it is still the rule. But the recent interpretations of the regulation have tended to chip away at the exemption, so this is a problem that universities are facing.

I would say that the most serious issues are still those concerned with the government's attempt to regulate information flows. I presume that this has already been discussed to some extent; I'm just going to mention the most important ones in my view: Contract

language that invokes the secret but unclassified idea which is so problematic for so many reasons; requirements on co-authorship controlling the OFAC, the Office for Foreign Assets Control and the Department of Treasury regulating co-authorship of papers with foreign nationals from countries that are on their list of regulated or banned list, and restrictions on the web-based distribution of information to participants in international collaborations, so you can't just put up a protocol for your experiment and hope that your colleagues in another country can get it off the web. There is also of course the requirements for prior review of publication, which has been extremely -- go along with the SBU concept.

I'm not going to say very much about deemed exports, because that is Sue Eckert's topic. But the fact is that these changes that we just heard are going to be deferred. When they were proposed, they caused a great deal of anxiety, and I guess the good news is that the government has listened to that anxiety, because they were going to create a huge regulatory burden for universities, and if they go ahead after a comment period and decide to implement them, it will do that. They are going to

severely restrict the reach of the fundamental research exemption.

Moving on, I would say that a separate related issue is the restriction on foreign graduate students from certain countries. If you go to changing the rule for identifying foreign researchers from the country of permanent residence to the country of birth, which has been proposed, you expand the net enormously. You can take an Iranian scientist who probably left Iran for political reasons and settled in Canada and became a permanent resident, and he would be barred from working in the United States. That is just a sample of the problem.

With respect to the students on campus, the proposal is to stigmatize them in some sense by requiring them to wear special identification and to have special controls on access to the laboratories.

So these run directly counter to the principle of non-discrimination in universities. There is no way to enforce them without creating a second-class status for these particular students.

Finally, I think this is always key, implementation. If different agencies interpret the rules

differently, or decide to play it safe by invoking every possible protection, the situation quickly becomes unworkable.

I think you can measure the cost of the regulatory burden which has already been incurred by universities in responding to regulation by the need to staff these new compliance bureaucracies. I know some of you are here in the audience today, and I am conscious of the size of the office at Cornell. So that is a direct cost in the university. Then there are the unmeasurable costs, or the less easy to measure costs, which is the chilling effect on researchers when they face this kind of reporting requirements, and the very strong disincentives for international collaboration because of the barrier for participation.

And of course, another cost is that the United States becomes less attractive to foreign students. We have seen that for a variety of reasons. I gave a talk in Cornell engineering school earlier this semester on deemed exports. I started to explain what they were, and I could see the students in the audience just turning and staring at each other, because 90 percent of them are from other

countries, and they had no idea that these regulations were there and that they were potentially going to affect them.

It is true that these issues affect different scientific fields in different levels of intensity, but none escape some impact.

On the Fink Committee, we looked at the historical experience of two different scientific fields directly relevant to national security, nuclear weapons work and cryptography, in order to compare them to the situation in the biological sciences. Unlike biology, both of these fields have strong ties to national security agents, and both are quite small in size. This has facilitated government controls of material and of information flows. For example, in biology you have tens of thousands of journals. In cryptography there are only on the order of about 200 published papers a year in professional journals.

If you turn to the nuclear weapons complex, you find that it is not even an issue in the university for the most part, because we have a large system of national labs, and because most universities simply don't do classified research, so they are not involved in that particular part

of the research program.

The issues in cryptography over publication and deemed exports have been more difficult, but the small size of the community seems to have facilitated a kind of modus vivendi, in which there has been voluntary cooperation in review of papers in exchange for no government restrictions on the professional conference sessions. But I would say that neither of these solutions is practical for the biological sciences, because of the structural differences, the size of the field, the number of journals, and the fact that there is so much going on that has never before been connected to security, so nobody -- they don't know who to talk to. They don't have a Rolodex. The Rolodex has about five names in it, as far as I can tell.

So the question is, what is to be done?. I think that if we are going to talk about a government-university partnership, we have to first consider whether or not that is the right language. I adopt it because that is the title of this symposium. I think it is actually somewhat misleading. I think what we have is a principal agent relationship in which the federal government hopes that the universities will produce that new science, the new

scientific advances that they want, and they think that the best way to get that is to delegate basic research to these universities, a large part of it. But when it comes to national security, there is an unavoidable conflict between some parts of the culture and goals of the university and the goals of the government. So the trick is to manage the tension in ways that are acceptable to both sides.

If we want to get beyond this rhetorical flourish, we need to do things to develop mutual trust between academia and the government. Of course, I come out of the peace studies program and arms control activity, so I turn to this idea of confidence building. Jack will be happy that I have a proposal.

We do have regular meetings to discuss the issues. I'm quite sure that many people in this audience participate in those, but you have to think about it on a field by field basis.

In biology now, some of this is happening through ENSAB. If you are familiar with the ENSAB, you know that it is a fairly unwieldy organization at this point and has not really developed a way of working, so I would say that the jury is out, whether that is going to turn out to be seen

by the biology community of scientists as representing their interests effectively, or whether it is simply going to be a rubber stamp for government proposals.

Another rule of thumb for building trust that we can learn from international relations is this idea of transparency. Transparency in some sense is built into our system because of the regulatory process, so that is one of the things the United States is famous for if you compare it to other countries.

But in practice, the regulations in this area are so complex that they can only be understood by specialists, which is why we have these new bureaucracies. The rules as they are written and I have read them are really arcane for any normal person. I think the real problem here though is one of consistency.

I think that is the single thing that could help build more trust. As long as you have the variability in definitions in key terms and in enforcing the regulations, there is going to be instability in this relationship, and there is going to be continued suspicion on both sides.

So I would say if the government wants a cooperative relationship with the university community, it

needs to simplify the regulatory regime and adopt consistent rules, and it has to adopt consistency.

That's it.

DR. JASANOFF: Thanks for that, Judith, and also for not just stating the issues, but moving on to solutions and getting us pointed in that direction.

George, would you like to pick up now? Our next speaker will be George Church, who is professor of genetics and the Director of the Center for Computational Genetics at the Harvard Medical Center.

DR. CHURCH: First of all, I'm sorry that I was late. I was ridiculously early yesterday, and somehow I compensated today.

What I would like to address is the biological revolutions that are occurring and how that impacts the way we are dealing with the government-university partnerships in science and security. In particular what we are dealing with are exponential curves in three fields. One is computing, which was discussed here, and the other two are analytical and synthetic chemistry and biology. We can analyze DNA and synthesize DNA at alarming rates compared to what was possible in the past, alarming if you are an

alarmist, and we can compute on these things at exponentially increasing rates.

The technology is changing to the point where when just a little while ago when I was starting my laboratory, starting in research rather, it was relatively trivial to type in all the DNA sequences that were known. I did this myself. There are now 100 billion such DNA ACG's and T's, and I wouldn't attempt to do that.

Similarly, synthesis at the time when I started, it was very difficult to synthesize ten nucleotides, a little thing that is almost quite useless. Now we are synthesizing things on a genomic scale. On a single chip you can now synthesize chemicals on chips the same way that you can for consumer electronics. On a single chip you can fit millions of oligonucleotides for hundreds of dollars.

So now people have made synthetic viruses. In fact, it is fairly routine in the virology field to do this for research purposes, and it becomes feasible to make rather drastic changes. Some people say that this is enabling smaller and smaller groups to do mischief. That is, what used to be something you would worry about a superpower doing becomes something a small country can do

or a small subset of a country or a company or even a group of people in a garage. That is one of the problems with the exponential technologies.

When we address the issue of controlling information, this is very difficult to do, not just because biology has a thousand journals, but because of the Internet. Now anything that gets in any public domain, or even private, it gets spread very quickly. Things that presumably are not in the public domain like the latest blockbuster film is present in DVDs all over Asia and the world. So I think it is not so much that it is a burden on academia as that it is not practical. Many things that we think are safe today are less safe in a new context tomorrow.

We can continue to raise questions and problems, but there are some proposals that are floating around which I think are interesting. There are some important traction that we are getting in terms of committees that are putting together very solid documentation of where we stand and where we can go.

The previous speaker just mentioned ENSAB, which I think is important. There is a Sloan Foundation funded

committee that is meeting four times at MIT and Ventura Institute and CESIS, and there is Synthetic Biology 2.0 which will be meeting May 22, where there will be the coming together of a couple of bicoastal town meetings, ending in a vote on various things that we can voluntarily do to improve the security. We are talking now here international security, not national security.

For example, one of the proposals that has been floating around since well before 2004 when I put a white paper out is the idea of surveillance of the whole stream of chemicals from precursors which are unique to oligonucleotides to synthetic genes to instruments that employ these to even experts in the field.

This sort of surveillance would not be welcome if you were a regular citizen, but I would submit, and we as a community submit that people who go into the field of synthetic biology or more importantly synthetic pathogens are not average citizens. No one is forcing them to go in that field, and they merit additional surveillance. This is very inexpensive surveillance, mostly computational. No red flags will be raised unless you try to order a select agent in DNA form without appropriate authorization.

So I think that is a straightforward thing, and the vote that may be going forward will be something to the effect that voluntarily as members of the synthetic biology community, we will not do business with companies that do not have a policy, verifiable, for checking such things.

I think that is an example, and there are many others I can go into if the discussion goes in that direction. But the point is that there are not just problems, but there are some grass roots solutions. The hope is that as the companies and community starts doing these things voluntarily, governments around the world will be able to point to these, and rather than governments having to create these things from scratch, which I think is very difficult, they will be able to point to a successful experiment and say, let's just make that law, rather than trying to think it up from scratch.

There is not quite enough technical expertise. I wish there was much more, but I think we need to have working experiments in the social fabric of the academic commercial interface so the governments can study those and decide which ones they like.

Thank you.

DR. JASANOFF: Thank you, George, and thank you also for introducing the role of companies into the discussion that I am sure we will have after the presentations.

The next speaker in the order you have in the panel is Sue Eckert, who is a Senior Fellow at the Watson Institute for International Affairs at Brown University.

DR. ECKERT: Thank you. I am very pleased to be here today. I have had many interactions with the National Academies over the years, I hesitate to say how many years, but I would say that the Academy has made very significant contributions to these issues at the intersection of science and security over the years. In fact, we just need to go back to look at some of the previous reports to understand the nature of this problem that we are facing today.

I am also in a rather unique standard here today as well, because I both was on the Hill for a number of years, and requested Academy panels to look at some of these very vexing issues, and I was in the executive branch responsible for implementing the policies, particularly the dubious distinction of dealing with export controls.

I spent most of the last six or seven years trying to forget what I knew about export controls, and went on to much easier issues like financing of terrorism. But somehow, the long arm of export controls always reaches back and brings you back into some of these issues.

I have to say that when I started looking at this again, having conveniently forgotten most of it before, I was really shocked in terms of how much there is a sense of deja vu all over again on this issue. It has been 25 years, and while the nature of the threat clearly has changed, and the targets have changed, it is no longer the USSR, it is uncanny in terms of how much some of the past bears on the concerns today.

Let me just read to you. The panel recommends that no restrictions of any kind limiting access or communication should be applied to any area of university research, be it basic or applied, unless it involves a technology meeting all the following criteria: The technology is developing rapidly and the time from basic science to application is short; technology has identifiable direct military applications or is dual use and involves process or production related techniques; the

transfer of the technology would give the, fill in the box, it used to be USSR, a significant near term military benefit, and the U.S. is the only source of information about the technology or other friendly nations that could also be the source have control systems as secure as ours.

Then it goes on to talk about the gray areas. The panel recommends in a limited number of instances in which all those four criteria are met that classification is unwarranted. The value of open science can be preserved and the needs of government can be met by written agreements no more restrictive than the following: Prohibition of direct participation in government supported research projects by nationals of designated foreign countries with no attempt made to limit physical access to university space or facilities, or enrollment in any classroom course of study.

This was written almost 25 years ago. This is the 1982 Corson Committee report, which Dick will remember, having been one of the people who served on it. It is really a sense of deja vu all over again, but unfortunately it is not unusual.

In the history of the academic community's

interactions with the security community, there have been these situations where the issues are never fully resolved, and the ambiguity creeps up from time to time and different interpretations flare up, depending on the circumstances at the time. While circumstances have clearly changed, we no longer have the USSR as the threat, we shouldn't be surprised in a post 9/11 world that we are facing some of these issues again, and that universities and research institutions have become the focal point.

What others have talked about in terms of the life sciences and biological agents and sensitive but unclassified information, all of these issues have been dealt with to some extent before, but are relevant today as we face these new threats.

A lot has been said with regard to the export control requirements. I think it bears reminding people, or explaining exactly what is meant by this, because I think that there is a lot of misunderstanding or at least characterization of some of these issues.

Let me just say that you will never find the word deemed export either in the Export Administration Act or in the Export Administration regulations. That is because it

is a policy interpretation which is based on, very loosely based on statutory interpretation, but regulatory intent with regard to technology.

It has to do with the transfer of goods or technology to a foreign national within the United States if it is deemed to be an export to the home country of that foreign national. Hence, we get the deemed export.

The release of information and technology is controlled if it is related to controlled goods, the actual equipment itself. So you have for example a tour of laboratories, foreign nationals involved in research, either students or academic professionals, professors, hosting foreign scientists, et cetera, are all situations which potentially raise the issue of deemed exports and being subject to U.S. export control regulations.

Now, one thing to be clear about here too is, there has been a fear that this applies to beyond foreign nationals. It does not apply to foreign nationals who have been granted permanent residents, greed card holders. That is important to know. I think some feel that with the slippery slope, people may want to go there, but it does not apply. I think that the executive branch has been

quite clear in indicating that it does not apply. It is only when we are talking about foreign nationals here without a green card.

The other thing to keep in mind too is, there are exemptions. There are exemptions in the regulations which have been around for quite some time. It is publicly available. It is not subject to export control requirements. Educational information and course catalogs that are taught as part of the routine courses is not controlled. Then of course, we have the fundamental research exemption. That is, if applied research were resulting in information that is ordinarily published and shared broadly with the scientific community, it is not subject to these regulations. However, the way the executive branch interprets that is not that there is a broad unlimited blanket exception.

I think some intervention think that the deemed export rule is new, that it somehow or other occurred with the publication of the investigations by the Inspector General, which frankly in the National Defense Authorization Act was an annual fishing expedition for inspector generals to find problems with agencies and

export controls. It is not new. Even the change that occurred in 1994, it does not mean that there were not deemed export requirements before that.

What happened in 1994 is, the industry was concerned, because at that particular time, and primarily companies were concerned about this, it was a question of when you knew that that foreign national had the intent to take the information or the technology out of the country. People were concerned that there wasn't a bright line.

Industry asked for a bright line and they got one. They weren't very pleased with the response, but you have a bright line from the perspective of the regulatory community. So one lesson some people may draw from this is, be careful what you ask for. But the intent was to clarify, in terms of the '94 language.

Deemed exports licenses. There are approximately a thousand every year. Ninety-nine percent are either approved or returned without action. Only one percent of them are denied. In terms of the volume, they are primarily for countries such as China, which now represents almost two-thirds of the licensing volume, India, Iran, Russia, a couple of other places.

The IG's recommendations. I'm not even going to deal with the country of birth, because I think that issue has been clearly laid to rest, but the definition of use. It used to be the Bureau of Export Administration, it is now the Bureau of Industry and Security, how they define use is that the technology for operation, installation, maintenance, repair, overhaul and refurbishing is how they define use.

In that interpretation, the Inspector General some of you know, has recommended that “the” be changed to “or”. One little word change, and it means that instead of all six of those being a requirement, only one of them triggers export control regulations. So that is one recommendation and one area which is not resolved.

The other is the interpretation of the fundamental research exemption. I know that the university-based regulation community has said that it is inconsistent with NSD 189, but there are different interpretations of what the language of NSD 189 says. So I think it is important to keep some of these points in mind.

The good news is that -- I didn't see the press report, but I knew that what the Administration was

considering is to announce that there would be a new FACA, Federal Advisory Committee Act, committee formed to look at these issues. I think that is a positive thing.

I should say too that the response of the community to the proposed changes in the regulations that were published by the Bureau of Industry and Security was overwhelming. I think it was a record. There were 309 comments made. I think that speaks very highly to the community's interest and involvement in this issue. Largely as a result of the outpouring of concern, the good news is that this issue is not going to be decided, there is no imminent regulation which says it is going to implement the IG recommendations. So there is not an adverse decision. That is the good news.

The bad news is that in a typical Washington response, we formed a committee to look at it and to kick the issue down the road. This issue is by no means resolved. I think that it would be a very wrong interpretation.

The Financial Times on Saturday had an article which previewed this. It said something about victory, or something along those lines. I think it would be very ill

served to think of this as a victory. I think what you should understand is that this issue is going to be a longer term issue that you are going to have to engage in.

But I think in the interim, one very important point is that what happens during this interim, what happens now, when you have a situation in which you have different interpretations out there, and you know you are looking at the policy to be revised, what are the implications for the community.

I would argue that they may not want to do it in a public fashion, but some understanding needs to be reached with the regulatory agency with regard to enforcement of these provisions, because otherwise universities are vulnerable at this point. If Stewart Baker's people show up at your door, the enforcement arm of the Department of Commerce, they can make a case that the academic community is too broadly interpreting. So there is a vulnerability that you need to address.

As we go forward, just three points I would like to make. That is, the dialogue has been very important and has been very good. I commend AAU and COGR for the kind of representation that they have made in the Washington

community, and the presidents, the leaders in the university community. They have been around talking to people and explaining the nature of the concern.

That is positive, but this is just the beginning of the process. I say this for several reasons. It is very clear in talking to people about this that the two communities are still talking past each other, that there is really not a fundamental understanding in the executive branch of how deeply the academic and the research communities depend upon foreign students, or the depth in which these affects the community.

By the same token, there is a perception in government that the university community has been somewhat loose in export controls in the past. I think there has been an enormous amount done on compliance in the last couple of years, but there are those that would argue that those requirements pre-existed, and there are all sorts of reasons. I'm not saying that the community has been, but I am saying you have a perception issue by some in the executive branch that there has been this broad interpretation of fundamental research in the past, and therefore there is an issue that needs to be addressed.

The third is, the different views with regard to fundamental research and use, they are going to continue. I think the IG pointed out a particular area, and they made a very good case. In asking individual people within the executive branch, they have interpreted both ways. You have individual licensing people who have been asked questions who have interpreted both ways, so you have a legitimate difference of view.

A second point I wanted to make is, not many people have focused on this, but the subtext of all of this is really a debate over China. I think you don't hear it and nobody talks about it in those terms, but this is not just a recent phenomenon with deemed export or the IG. This has been an issue which has been brewing in the bureaucracy and bubbling up in the security community since the end of the Cold War. There are people in the bureaucracy who have been talking about China as the threat. Take out USSR and put in China. There are those who have been working on policies to that effect for quite some time. There are even indications that the IG was first directed to some of these issues as part of a concern over Chinese scientists in Canada and the inability for us

to reach them, because they were considered Canadians.

I'm not a believer in the great conspiracy theory, because government is so inefficient that it could never really pull off the things that people would attribute to it. But I think you have to understand this issue for what it is, and it is a China debate now.

The third thing and last thing I will say is that there are several ways to approach this issue. As someone who used to be involved in the day to day things, I used to say I was about 5'11" when I started, and have been worn down. You can't see because we are sitting down, but I am nowhere close to that.

There are two ways to approach this. You can argue the technical issues, and you can engage the bureaucrats and the regulators in trying to find a fix that will work. Or, and it is not necessarily mutually exclusive, but you can take a step back, which I hope this panel will do, and engage in what I would argue is a fundamental rethinking of export controls in a post 9/11 world, a system which to this day, the way the law reads, you still talk about controlled countries, you use the terminology of the Cold War. Both the law and the

regulations are based on a different time, more than 50 years ago. There is I think a need for a fundamental rethinking of what constitutes security in this new age, and what is the true threat, and the role that export controls can play in this.

This is not an easy task, but I want to conclude with one final point. That is, in every time in which export control policies for the past 25 years has gone through a correction or a rebalancing, it has been based upon and preceded by a National Academy of Sciences report. That is because the recommendations made by the Academy carry the weight of the security community as well as the most distinguished expertise that we can find in the United States. Those recommendations have been decisive in the past.

While I said it is not an easy task, these are not easy issues, and the politics of this particularly as they relate to China are not easy, some of the people were talking about the politics on the Hill, I think that the timing is propitious. I don't know whether this panel has within its mandate the ability to do that or a follow-on panel to look specifically at some of these questions, but

I would argue that for us to secure, not just U.S. security but the international security, we really have to have that fundamental rethinking.

We have done it through a patchwork quilt approach for 50 years, and now it is time for a fundamental re-approach on this issue. I think the timing with regard to election, it is a new Administration, and that is usually the opportunity for fresh starts. I think that in the past, the Academy's work has been decisive in making sure that the policy community is held accountable and has the ideas and the arguments to move forward on sound policy.

Thank you.

DR. JASANOFF: Thanks, Sue, for the invitation to look backward and forward. Our next speaker is Suzanne Berger, who is the Raphael Dorman and Helen Starbuck Professor of Political Science at MIT, and also Director of the International Science and Technology initiatives here.

DR. BERGER: Thank you very much. I have learned a lot from this morning's panels.

What I am going to present comes at these issues from a somewhat different perspective. I would like at the

end of my talk to be focusing on what I see as a changing set of needs at universities, universities like MIT, for a very changing set of ideas about what our relationship to the international economy ought to be, and the pressures for change in our relationship to international institutions of research to foreign students to the opportunities for our own students to go abroad grow out of a rapidly changing set of ideas about how changes in the global economy are affecting what we ought to be doing in universities for our students and our own research.

The debate at MIT to some extent has been nourished by a research project that has taken place at MIT over the years 1999 to 2004. This is one that I participated in along with six other faculty colleagues and seven graduate students. The colleagues were social scientists and engineers.

What we tried to do is understand the impact of globalization on employment and innovation in the United States and other societies. We did this by carrying out a set of interviews in companies in North America, Europe and Asia. We looked at a variety of sectors. We tried to focus on a continuum that went from what I would call slow

tech sectors like textiles, retail and apparel, in which underlying technologies change very slowly if at all -- in apparel people are still using sewing machines around the world, even in the most advanced countries, that are not very different from the sewing machines of 50 years ago -- to the other end of the continuum, electronics and software, where the technologies of course change radically and discontinuously in very short order. Then we looked at a set of sectors that could be characterized as mid-speed technology based. That would be publishing and automobiles and auto parts.

In all, we went to 500 companies and did 700 interviews over this five-year period. Of course, what we observed was that between the 1980s, when MIT had carried out a project somewhat similar to this that gave rise to a book called Made in America, from the end of the 1980s to today, there have been enormous changes in the organization of the international economy and in the strategies of companies that are operating successfully in it.

If I had to stress one single, perhaps the most important of changes, it is that the companies that looked like the best companies at the end of the 1980s were

vertically integrated companies that succeeded exactly because they were able to carry out all the principal functions -- research, design, development, manufacturing, distribution. They had all these functions located within their four walls or within single corporate control, and they were able to carry out these activities in close proximity to their most important customers and their most important suppliers.

In some sense, the icon of the most successful company in the 1980s was something like Toyota, in contrast to General Motors. What we thought was deficient about the U.S. corporate performance at the end of the 1980s when we were all worrying about the Japanese eating our lunch was that too often in American companies, functions were not well coordinated. People were throwing designs over the transom, research and design and development people, expecting that somehow, manufacturing would be able to manufacture something that the designers had dreamed up, without any thought or manufacturing difficulties.

So the mantra of the end of the 1980s was one that focused heavily on integration. I think that if we look at the world today, we are looking at a world that has

radically changed, exactly because we have a complete fragmentation, or in many of the industries that we studied and many that we did not study, we could see a massive fragmentation not only of production systems, but of the systems of research, development, design and distribution. It is precisely those companies that have best mastered operating in this fragmented world that seem to be best succeeding today.

So if I gave you an example of what I see as an icon of the most successful sort of company today, it would be something like Apple, with the Apple iPod. When you look at what the genius of Apple was, it was that its designers were able to look out at the world and see that the Japanese companies were producing a set of electronic components that could be combined into a different sort of product. So Apple didn't invent or produce or conceive the components that today are the guts of an iPod; they simply identified the existence of these components that very successful high-tech Japanese electronic producers were making. The Apple designers were able to imagine, conceptualize, a product that would use these components and then have the product assembled in Chinese plants and

redistributed through Apple distribution channels.

So this is a product that is truly made all over, that is made not within the vertically integrated operation, but is made and has been enormously successful exactly because Apple was able to conceive a design, development, production and distribution in a world of fragmented activities.

What has made possible this enormous shift from the world of Toyotas to the world of Apple iPods are a set of factors driving globalization. Here I think there is very little that is new if we look at the set of drivers, but I think in our research we focused particularly on one of the enablers that I do think has had a dramatic effect over the last ten years. Those are new technologies, in particular codifiable specifications and industry standards that are what makes it possible to fragment production and separate it from research, development and design.

So if in the 1970s, in making a mask in semiconductor manufacturing we still needed to have the engineer who drew the circuits standing next to the technician, who more or less used a razor to cut out of the mask, a mask I think of as something like a stencil, these

two people had to be located within the same four walls. They had to be directly communicating with each other if you wanted to have a high quality for the mask. The more experience they had in doing this together, the better the quality of the mask and the result.

Today, the engineer draws the circuits on his computer somewhere, and the cutting machine can be located anywhere in the world. In industry after industry, we have had a shift like this that reflects the possibilities of using new technology, a digitization basically, that allow us to fragment production and design.

This results in a shift that I see as something like a shift in the world of making a model airplane to the world of making an airplane out of Legos. If you have ever made a model airplane with a child from a kit, you know that there are instructions on the box, and you can make one and exactly only one, if you are lucky one, airplane out of those pieces in the box. If you don't glue them together exactly right, you just have a failure. Once you put them all together in one way, there is absolutely no way of reusing those pieces to make another sort of thing. Nobody can come in and add anything to your model airplane.

So all of the pieces have to be customized for that one model airplane.

Today, the iPod is the exemplar of the Lego product. It is a product that is made with components that can be put together in multiple ways to make multiple products. It means that the most important companies and research activities today in the world are ones that are striving to produce Lego parts and not model airplanes. I think this has very important implications, first of all for the organization of production.

If you look here at the electronics value chain, what we are looking at are a set of functions that in the past used to be integrated within single companies like Motorola or Texas Instruments. Today, at each one of these arrows it is possible to break apart the functions and to locate them in different parts of the world, putting semiconductor manufacturing in Taiwan, product definition in California, design possibly in California or in Taiwan. Some of the manufacturing now is likely to be taking place in China.

In our research, what we tried to find out in the companies was what peoples' ideas were about where these

activities ought to be located, first of all, which activities should remain within the four walls of the company, and which might be outsourced. Of course, most outsourcing is domestic, so the outsourcing, the reorganization question in response to these new opportunities for relocating functions, that in the first instance is probably going to be a domestic decision. But once you can break apart these production, development and design systems, there is also the possibility of locating some of these activities outside the country, locating some of these activities offshore.

I think that it is out of these possibilities that our basic dilemmas or the pressure for change within the university has begun to manifest itself. I just want to show you rapidly, although this is not what we are focusing on here this morning, some of the conclusions of our general globalization study, just to suggest that some of our largest conclusions had to do with the possibilities for maintaining diversity in these decisions about organization and offshoring and onshoring.

Even for an industry like the electronics industry, if we look at any single product, what we find is

an enormous diversity of successful strategies. So on one hand, you will find a company like Dell that makes none of its components, and where manufacturing at Dell means exactly four and a half minutes in which components that are entirely made by others are snapped together, bolted together or welded together and software put in, that is exactly what manufacturing in the United States means for Dell, with the foreign suppliers' trucks lined up outside and Dell pulling in the parts exactly as they need them. Dell remains the owner of all these parts for about three hours, and after that they belong to the customer.

So on one hand, we have a Dell, where something like 85 percent of the value of a Dell PC is made outside the United States and is in the components made outside the United States, but in contrast, you can look at companies like Sony or Samsung that are making the same PCs and doing it largely within their own countries using components that are largely made by their own home enterprise. So a Samsung computer, if you break it apart, most of the components are Samsung parts. The microprocessor is going to be an Intel microprocessor, but the screen and all the rest are likely to be Samsung products. Both of these

companies, the Dell and the Samsung, are enormously profitable.

So what we have found through this study is in industry after industry, whether you look at fast tech sectors like electronics or slow tech sectors like garments, and compare a company like Zara to Gap, we found that there is a lot of diversity, and that this raises the opportunities for choice.

But I think from the perspective of universities, and these are the two points on which I would like to close, from the perspective of universities, looking at the world in which our graduates are going to be operating, I think the fragmentation of production and the possibilities for relocating research, design, development and distribution around the world puts us as universities in a very different situation than the one of 20 years ago.

Twenty years ago, at the end of the 1980s, our graduates largely went out to work in American companies that were vertically integrated companies, where our students succeeded to the extent that they were able to coordinate activities within their own companies. To the extent that they were able, as we learned in the Made in

America project, to bring research, design, development, manufacturing and distribution together, to integrate, to bring together in teams people who would be working together on solving these problems. The people who were being brought to work together were largely people working under the same corporate roof, people working in the same location.

The fact is, today our students who graduate now are going out to work in companies where the heart of their activity is going to be trying to access knowledge that exists outside the four walls of their own laboratory or outside the walls of their own company. They are going to have to access knowledge and capabilities outside their own organization's boundaries, and they are going to have to coordinate and bring together knowledge and capabilities that are outside their own organization's borders and outside their own country's borders.

At this point, our students are extremely poorly prepared to do this. There is nothing in the education or little in the education that we are providing students that help them learn how to solve the set of challenges which, whether they are scientists or engineers or managers, are

going to be their principal challenges in the world of work. There is little that we are doing to help them learn how to solve this kind of problem.

Though the dominant metaphor for this world of fragmentation is a metaphor of value chains, in which you might imagine that each link in the chain is somehow equal, I have to tell you, after doing 500 interviews, that each link in this global value chain is not equal. As some of the Taiwanese expressed it to us, this is really not a chain of equal links. Think of it more like a bullwhip, in which some people get to hold the end of the whip and the rest of us get jerked around on the end of the whip. I think as educators, we have a legitimate desire to have our students be in positions of greater control, positions of greater capability, and not the one that is being jerked around on the end of the bullwhip.

So as we try to think what kind of changes are we going to have to imagine in education and research in order to prepare people for a different kind of world than the ones in which they were moving to in the 1980s, I think the first big change that we have to imagine is, how do we educate our scientists, our engineers, our managers so that

we build in a capability to access knowledge outside of the United States. How do we teach people for example to understand vast new consumer markets that are emerging in India, in China? In the 1980s the U.S. domestic market was largely it for most organizations. U.S. laboratories were the best in the world, so people didn't have to worry so much about their ability to access knowledge outside.

So as we try to think about what we need to do with respect to international hands-on experience for our students and our scientists, as we think about the role of foreign students on our own campus, it used to be we were glad to have them come. We didn't think too much about them, they weren't really essential in some vital way to educating the students who were on campus already. We were glad that many of them were going to stay. That was important to us. But I think foreign students have taken on a different importance now, because these are not going to be simply our trade rivals; these are going to be people who we are going to be partnering with and working with for all our professional lives.

So I think many of the pieces remain the same pieces today, but they have acquired quite a different

significance for universities because of the changes in the international economy.

Thank you very much.

DR. JASANOFF: Suzanne, thank you for that very dramatic presentation, which reminds me of the fact that back in the early 1940s, the American sociologist of science Robert Merton talked about how universalism was one of the core values of science. I think what you are showing is that technology today is no different from science, and universalism has become a core value of technology. That I think raises some questions that I hope we will come back to at the end of the panel presentations.

Our last speaker for the panel is Deborah Stewart, who is President of the Council of Graduate Schools.

DR. STEWART: I must say, Suzanne, that I have just recently read this very light book, but conceptually good, by Daniel Pink. I don't know if you have seen this piece, but he basically makes the argument without data that you have made in a much more fundamental way. The fact that we are moving from a knowledge economy to a conceptual economy, where integration, synthesis, the

capacity to think broadly across cultures and fields, is going to be the currency that allows one to be effective going forward is of profound importance for graduate schools. I am delighted that you have done the work that you are doing.

I am going to take a few minutes just as a wrap-up here to speak about the perspective that senior administrators responsible for graduate education on campus have on the set of issues that we have been talking about over the past couple of days, that is, the variety of ways in which government is now feeling the need to provide more oversight and become engaged more in the way in which we do our work in our research laboratories.

A moment about the Council of Graduate Schools, just to establish what the perspective is here. The Council of Graduate Schools is the only organization nationally that represents all of the universities that are significantly engaged in graduate education. That would include eery major research university in the country, plus about 100 or so institutions that you may not have heard of that are doing important work at the masters level in particular, many regional universities and some smaller

privates.

The principal representatives of the Council of Graduate Schools are the deans of graduate schools, many of whom also hold the title of vice president for research. They have a particularly strong interest in the ebb and flow of international students. We routinely -- I say routinely; I have been in Washington for six years, and for six years we have been surveying our graduate deans in January of every year, asking them to tell us what are the top three issues on your desks as you sit here this morning.

For five of the six years, managing international student issues has been in the top five. In fact, for the last five years, the top issue, number one, alternates between the international student issue and financing graduate education. In fact, those two issues come together very closely in the discussion of deemed exports.

In March of this last year we released a report indicating that international student applications were up 11 percent for fall of '06 in comparison with fall of '05, up across all fields of study, up in science and engineering, up from all major sectors of the world,

particularly India and China, which are huge providers of graduate students to the U.S. graduate schools. And interestingly, up in all kinds of institutions, large research universities, smaller regional institutions, publics and privates.

But even with those gains that we reported just about a month ago now, the fact is that in terms of international applications to U.S. graduate schools, we still remain down 23 percent compared to fall of '03. We had a precipitous decline as you know between '03 and '04, continued decline in '04 and '05, and a pretty strong return this year.

I would like to spend a few minutes saying a word or two about first, why that rebound is happening, second, whether or not it signals a return to business as usual, and third, what the message in all of this might be for the committee.

Why did the rebound happen? There are two sets of actors who had important roles to play in the rebound story. We had presentations yesterday from a couple of them. Clearly Homeland Security and the Department of State intervened in ways to ameliorate the more negative

effects of their earlier actions, and happily have brought us back to the situation where we were roughly in the pre-9/11 admissions year with respect to international applications.

Now, I will not tell you that was an ideal situation. We were handling many, many complaints from deans from across the country in the pre-9/11 period about the difficulties with processing visas, but it clearly became much, much worse, and now it is much, much better again. Both Homeland Security and State, particularly Consulate Affairs in State, did a terrific job in responding to the concerns.

Also, I actually believe that there is some significant value in the PR campaign. I actually believe when Secretary Rice goes to China, speaks at Shingwa very passionately about her belief in and the country's belief in the value of international students. I was a real cynic when I first learned of the campaign the Department of State was about to undertake, but I have been in China and talked to people in Shingwa, and that actually makes a difference. That is very reassuring.

But the second set of actors were U.S.

universities. U.S. universities in important ways that might relate very much to the deemed export issue took the decline that they were experiencing in international applications and acceptances and actual enrollments in the fall of 2004 to heart. A whole variety of things were put in place.

The University of Illinois for example dramatically overhauled its electronic application system, so that it is much more user friendly now from the point of view of international students. Many campuses instituted call centers on campuses, so that there would be someone there on the other end of the line for the international student to call when he or she got caught up in the visa process, which inevitably does happen for some number of students. Many institutions' graduate schools dedicated new staff members whose job it was to deal exclusively with the interface of their office and other offices on campus that touched international student applications.

Actually, the most dramatic thing that I have seen that is different is that U.S. graduate schools are taking a much more focused, active and ultimately effective approach to recruiting international students. The old

process in my many years as the dean of a graduate school was to open the mail, or as we got electronic applications, to click open the electronic application. Those days are gone. Starting this fall we will for the second time have a group of 20 major U.S. universities meeting this fall in Shanghai, last fall in Beijing, with 38 of the 38 designated major research universities in China bringing together administrators, faculty and students from those major institutions to meet staff from U.S. graduate schools.

So with all of this, I think we could get back to a situation where the application flow will ultimately look like it did in the pre-9/11 period. But the fact of the matter is, over a ten-year period the United States has been losing market share for international students. We will continue to lose market share, because the American approach to graduate education has succeeded. In fact, graduate schools are developing all over the world, and undergraduate education is expanding all over the world, so two things are happening. The number of students who potentially go to graduate school somewhere is increasing, so our absolute numbers are unlikely to decline, but the

capacity for the whole higher education establish worldwide to absorb these students is also expanding.

So do these upturn signals ever return to business as usual? The answer is probably no, because global competition is on the rise as I have indicated. Countries as diverse as Scotland and Austria, Singapore and the Czech Republic, China and Japan most recently with its establishment of these new graduate schools, are now initiating very conscious national policies to attract international students.

Europe is very much on the move. Graduate schools American style are being established all over Europe, with one of their major responsibilities to be an open face to the international student community. U.K. has recently adopted a very explicit immigration policy designed to attract both high-skilled workers and students.

So it is from this perspective that I think about the impact of any fundamental change on the way in which research is conducted and students are trained in U.S. graduate schools.

We have heard from a number of experts on national security and the research enterprise over the last

24 hours or so. The issue has been how do we strike the right balance between openness on the one hand and security on the other.

I would just argue that as we try to strike that right balance, we need to insure that we no longer take for granted that it will be easy for us to attract the most talented students from around the world. The next frontier for U.S. graduate education is attracting the highest quality student. We will get the numbers because the pool is increasing, but to continue to attract the highest quality student, we need to try to understand what international students value.

I want to mention three specific concerns particularly with the deemed export proposals, but also with any of these suggestions for placing serious constraints on the openness of our laboratories.

One of the attractive features of doctoral training in the United States for international students is the opportunity to work in open laboratories. I want to just tell a very quick story that tells this better than anything else. I was recently in Beijing meeting with a woman who is -- I don't want to identify her personally,

but on the faculty of physicists at Shingwa. We were talking about international student flows. She attended graduate school in the United States, got her Ph.D at LSU. I said to her, would you recommend a student come to graduate school in the United States, given the growth of your own programs and the huge problems that at that time students were still facing in gaining visas. She said, I'll tell you, I would. I said, why? She said, my three years at LSU were the hardest three years of my life, but they were also the best three years of my life. I said, I understand why they were the hardest three years. Why were they the best three years? One of the things that she started talking about was the open character of the intellectual exchange, and very much a different total life experience. She was integrated into the research laboratory with people from the Middle East and Japan. She was describing, Suzanne, exactly the kind of impact that the American research laboratories have on expanding peoples' capacity to learn and grow and connect. This is an asset.

We typically think about what foreign students are going to -- the worry is what do we not want them to

export that somehow will damage us from the economic point of view. Our most valuable thing actually, which we cannot clamp down on without hurting ourselves, is the capacity to train people to learn and grow and think in an open and free society, and one that is as highly charged as the American research laboratory is.

There are also practical concerns. I am over my time, so let me just say quickly, there are also practical concerns with the proposals that graduate deans have, mostly having to do with how you could ever manage a system in which students were either badged or otherwise designated for participation, only allowed to be funded on some research grants, not on others. The typical graduate student is funded by multiple sources of support over time, some RAs, multiple TA streams, and it would be simply unmanageable. At this current point, we are already in a situation where with the large public research universities, many of them are so stressed financially now that if this regulatory burden were put on them, it is likely that you would get a lot of administrators resigning at least.

Thank you very much.

DR. JASANOFF: I'd like to thank the panel for an extraordinarily interesting lineup of comments. Before opening it out to the audience, I would like to give the panelists a very brief charge to respond to each others' statements. But before doing that in turn, as an academic myself I can't help wanting to take a couple of minutes to highlight some of the things that I think I heard across the panel as a whole.

One short comment is that at least from this panel, it sounds as though the title of this committee ought to have a tacit industry built into the partnership and a tacit technology built into the science and security. So whether or not the things are there in print, we seem to be talking about government-university-industry partnerships in science, technology and security. Sitting here at MIT it would be a deep mistake to leave the technology out, anyway. I think Suzanne's presentation made that abundantly clear, if nothing else.

Secondly, conceptually and intellectually what strikes me is that all of you are speaking of a time in which borders are vanishing on the one hand -- and I am reminded that Doctors Without Borders is a Nobel Peace

Prize winner, and NGOs have figured out something about how borders don't matter if you want to achieve certain kinds of things, and at the same time, security is a concept that depends on there being clear and definable borders.

So it is not that American national interest demands borders and universities are bucking it. It is that the American national interest demands a world without borders and yet a world with borders, putting both of those things on the side of national interest rather than universities wanting one kind of thing and the nation wanting another for security purposes. It might help us build towards that convergent idea of partnership. It is as much in the U.S. interest to have areas where borders are dissolved, and I think all of you have spoken about that in various ways.

I have thought for a long time how ironic the whole deemed export idea really is. In effect it takes what we previously used to think is a territorial boundary thing and brings it into universities, that have tried to create territorial boundaries inside the open space of universities.

I think it is worth highlighting maybe the

problems that all of you collectively have raised about why that is difficult to do, and maybe you want to say a word or two about that. Creating boundaries as we know from eons of social science work isn't an easy business.

We create strong boundaries where everybody is culturally trained to understand boundaries in the same way. For instance, I am a lawyer by training, and I know just how much training it takes to understand the distinction between fact of law, which lawyers will talk about at the rhetorical level all the time but other people don't see as clearly. So we are trying to in the security arena create boundaries against a flux in these communities that don't understand terminology in the same way.

So you have talked about dialogue and community building as one solution to how we get to have clear boundaries. You have talked about enforcement and clarification as another mechanism by which we can arrive at clear boundaries. You have talked about training and education as another method for getting people to recognize right from wrong in certain ways.

There are at least two other ways that come to my mind that I'm not sure you have explicitly touched on, and

I wonder whether those would matter to you in thinking about how we have this world with borders and without borders at the same time. One is professionalization, that is, can the professionalization of people in certain fields like your genetics students, George, that you mentioned achieve something, and a last one is ethics, which is a word that nobody has brought up, but talking about a world in which people learn to have different antennas for right and wrong in a sense, when they are behaving right and when they are behaving wrong. I wonder whether any of you see a place for ethics training as an alternative to command and control regulation or to enforcement carried out by people who don't understand the limits of their powers and don't understand the meanings of the terms that they are trying to implement and apply.

You don't have to respond specifically to my questions, but those are some questions that did come to my mind. Let me give each of you two minutes to respond to each others' comments or reflections if you have them. You can pass if you don't want to.

DR. CHURCH: I would just quickly respond to your questions, since those are fresh in my mind.

I think in terms of boundaries, there is in my field at least a great deal of effort going on into breaking down boundaries of various sorts between academia and industry and between nations. In a microcosm way there are international genetically engineered machines which Tom Nyden and others have pioneered which now has expanded from one month exercise of a few students to 40 universities worldwide this summer, and it is on another exponential curve. That is going to stress biology quite quickly and hopefully ethically, in the sense that both the synthetic biology meeting and the IGEM stresses the positive constructive aspect of things and diminishes the motivations to do otherwise, and increases mentoring and surveillance on a person to person basis. So I think those are grass roots things that can be done.

DR. REPPY: I had a question for George, but I wanted to say something about boundaries, too. My feeling is that a large part of the problem we have in the export control regime is that the kinds of boundaries that underpin creating this regime, the U.S. versus the Soviet Union, these things have disappeared. Yet the culture of that community is still very much to think that there are

these bright lines.

So I don't want to lay all the blame on the security community, but they really do have to get with the program if we are going to make any progress. That would be my response.

My question to you, George, is about this bicoastal synthetic biology committee meeting. In the Fink Committee we discussed the Silimar experience a lot as a possible model. It was thought that although that had been reasonably effective in the longer term although contentious in the beginning in setting up a self regulatory system for genetic engineering, but the problem now was that the community was too large, that you couldn't have this kind of meeting where everybody could get in a room together.

For molecular biology as a whole I think that is true. What I hear you saying is, here we are the small group of people who do synthetic biology, and we can repeat that experience. Is that the way you are thinking of it?

DR. CHURCH: I don't mean to be speaking for the whole community, but I think the opportunity is there for the small -- it is a thousand people that will be meeting

in Berkeley. Bicoastal just referred to town meetings that had preceded it, but it is an international group most definitely.

They will meet on May 22, and the intention is not for them to speak for everybody, either, or me to speak for them, but to pass whatever resolutions seem reasonable at the time, and continue a discussion on a larger scale. It is not intended to be a Silimar 2 or 3 or whatever it is at this point, but to make some practical suggestions and see how that particular community feels about them.

DR. ECKERT: I also wanted to pick up on a point that George made. I hope that the panel will take him up on his offer. There are solutions, practical ways in which some of these concerns can be addressed. In particularly sensitive areas I think it is particularly important to have practical solutions of what can be done.

So I think Sheila really hit upon a key point here. We hold onto boundaries because that is what we know from the past. The world is scary without boundaries. It is a question of control. We want to try to maintain the fiction that we control.

I think that what we need is a fundamental

education of people with regard to the new world. We all read about it, we all think about it, but I don't think that people really understand it. That is where the work of the panel can come in to explaining the world, both in terms of the threats, but the reality of the technology, and to try to convince people to understand that our strength and our security is best served through openness, not through trying to close down. It is not practical to begin with, first of all.

Second of all, many of the policies we have been talking about today are unilateral, they are by definition doomed to failure. That is one thing we haven't even talked about, is the fact that none of our other allies, let alone people who aren't close allies, share the kind of views and restrictions that we are talking about today.

But I think that there is a need for education about the realities. I think it involves some give and take on both sides. That is why I was particularly interested in what George was talking about. Some of it is moving to new models of cooperation, which are self regulatory, or which are restraints which in the past the academic community has been unwilling to take on, or there

is a wall built around it, fundamental research should be exempt from any kind of restrictions.

That is where I think professionalization and ethics come into this, but there is a role for new models for the type of responsibility that the research community can develop. It is not going to come from the government. It is going to have to come from the academic and the research community as to what some of those new norms, in what areas of particular sensitivity can be established.

DR. BERGER: I would like to pick up the point that Sue Eckert made in her original presentation about the substitution of the word China for the words Soviet Union as a way of thinking about some of these security issues.

Here, I think that the academic community has a certain share of responsibility in the way this has happened. Just as we tried to exploit the existence of the growing capabilities of the Soviet Union in making our arguments for having more resources directed to our own educational and research activities, there has been a strong desire to hype the China threat as a way also of making a case for a greater flow of resources in our own direction.

I think that there is an enormous danger in pushing this idea that the world is flat, the number of Chinese engineers, the growing capabilities of the Indians. Over and over again, we have seen that when you actually look more closely at some of these claims, exactly how exaggerated they are. Professor Gary Gereffi at Duke went out to see -- I think some of you may have seen the studies -- exactly what is meant by the word engineer in China. It turns out that anybody who has something like a vocational education degree gets called engineer. If we called all those people engineers in the United States, the figures would be quite comparable. The hyping of the outsourcing to India; how many of you have read articles that say, not only is it back office low-end jobs, but even radiology jobs are being exported. A professor here at MIT has gone out and had a team of students looking at India. He found exactly three Indian radiologists who were reading screens.

So over time many things will happen. Of course there is a tremendous source of dynamism, but I think we ourselves are creating a kind of threat that then will come back to us in ways that I think the members of the panel have laid out this morning.

So I would like to say first that we need ourselves on the education front to examine far more carefully the kinds of challenges that China, that India, that developing countries are presenting on the front of research and education. Secondly, with respect to -- and here I am coming to Sheila Jasanoff's point, to emphasize again how much it is in America's interest to maintain the openness of this society. In exactly a world of fragmentation of production, research and development, we have unique capabilities to recompose rapidly the character of our own activities that virtually no other society on earth has the same culture of openness and willingness to break apart old activities and reuse pieces, to let digital equipment go bust and then to see the top engineering talent go found companies like Sun Microsystems and Cisco. Protectionism and trying to put walls around this, we would be the most hurt by this in the near as well as the long term.

DR. STEWART: I just want to build on that point. I spent a lot of time looking at what our competition is doing around the world. The smart competition around the world is copying us, at least copying the way we are now,

not the way we could be if we decide to defend ourselves by some of these strategies.

The best example is this construction of graduate schools. The traditional way in which students were educated in Europe at the doctoral level was that they worked with a professor who had almost total control over that individual's life, and when he or she concluded that the student was finished, the student was finished.

The main driver of the establishment of graduate schools, the Free University of Berlin and across Germany where this was stronger than anywhere else, at places like Imperial College in London, is to insure that the norms of openness, of community, of interdisciplinarity, of engagement, the things that we do better than anywhere else in the world, are in place in all doctoral programs. They are even requiring in many countries courses so that students have exposure to information about the culture of science.

So it would just be the ultimate irony if at this moment, when the rest of the world has decided to replicate exactly what we are doing, that we decide it is just the moment to somehow close down.

DR. JASANOFF: Thank you very much for these further thoughts. Let's now open it up to the audience, if you would please identify yourself. Keep your questions as brief as possible and maybe the panelists keep answers brief, too, so we can get as many comments as possible.

MR. HART: I think we are deeply grateful for all your presentations. You have made a great contribution.

DR. JASANOFF: Could you identify yourself?

MR. HART: Gary Hart. I am a member of the panel. Let me just say, presume that our mandate says fundamental rethinking, or we start from there. The question is, what does a new regime look like? We are anxious to have people not just describe the present situation, but make specific recommendations to us as to how to change things, so that can go forward beyond today.

DR. ECKERT: Are you looking for an answer specifically to that? I think it is a process. Frankly there are things that can be done.

I warn you, there have been attempts in the past to fundamentally rethink some of these things, but I don't think that they have comprehensively defined security and what it represents today. I think that is the opportunity.

But it is a process, and the process takes time, because the process is educational as well. It is bringing in the people not only of the academic community and industry, but the security community.

I think there are some of those on the panel here. There are others to reach out to. In the past where these panels have been most effective is where you have people who have unimpeachable credentials in security, who spent their life worrying about security, saying we have got it wrong. We have to change the way we are doing this.

I think there have been a number of people who have been making those noises. In the post 9/11 world, people have made some of those things at risk because of the political cost that they have incurred by saying we are not doing it right.

But the movement has changed, and now is the right opportunity to be asking those questions. I think it is a process which is going to take some time, because it is not only investigating, as you were talking about what is going on in India and China and other places, or what our relationship should be. These are major questions in terms of looking to the future, and it is going to take

some time.

Hopefully, in the context of what the panel can do here, if you have a time-limited mandate you may not be able to do the whole thing, but taking on a piece of it and defining a mandate for what can be done specifically in some of these areas.

I agree, you don't want to repeat the problems of the past, but unfortunately we need to relearn some of these things, and more than relearning them, we need to adapt to current realities, which people don't want to face.

DR. JASANOFF: Thanks, Sue. It is of course a well-known lawyer's trick, when you can't give a substantive answer you go to process. But sometimes that is the only thing that is available, and it is a useful reminder.

DR. GUILLEMIN: I have a question about the emphasis on regulation. This is something I mentioned yesterday concerning the U.S. biodefense program, which has talked about $70 billion as an investment this year. Where is oversight? I am not hearing anything in terms of practical issues of oversight of our own rather broad and

in some ways rather dangerous high-risk venture into the realm of what we call biodefense. That is, BSL-4 laboratories being built.

Also, I think we have to go here to Department of Defense programs that are contracted out to commercial entities. We know there are CIA black programs, we know there are all sorts of activities including within Homeland Security, but I haven't heard anything about oversight mechanisms. The emphasis seems to be on, let's regulate university laboratories, which seems to me the very first reaction that we had after the anthrax letters. That is one thing.

Then the other thing I haven't heard here is the issue of shared risk. My area is biological weapons issues, but also epidemic diseases. I haven't heard anything about shared risk, which brings us for example to China, which had a tremendous wakeup call in 2003 with the SARS epidemic. In my visit to China, I found people in government and public health very concerned that they not be identified again with keeping an epidemic disease secret, because they don't want the negative trade repercussions, an interesting argument.

But anyway, those two ideas. One, where is oversight and transparency beyond the issue of regulation, and the other one is, what is shared risk in the biological sciences, which from my point of view we are supposed to be dedicated to the relief of human suffering and to prevent death. It makes them very different from the physical and chemical sciences that otherwise we discuss in national security forums.

Thank you.

DR. REPPY: Let me say something about the biodefense oversight question. I share some of your concerns. One of the problems has been in the beginning at least the recommendations of the Fink Committee, which have been carried out, focused very much on open university-based research, not on company research. Part of the reason for that was that we couldn't get the companies to participate.

But another I think is a practical concern. If what you are worried about is access to the biopathogens on the select list or any list you want to make, one thing that industry does pretty well is maintain security. They have intellectual property reasons for doing that. So the

question of an open university is not at issue there, it is whether or not you've got the guards and the gates, and they have got them.

So I think it was a copout because we didn't have the capacity to deal with that problem, but we could also say to ourselves, for that set of issues it is not the big problem that the very open university system is. The problem of course is that the biggest risk for bioterrorism, at least I would argue, is always going to be an insider. So the more laboratories you build, the more facilities you have, you are creating the capacity which also creates a lot of potential for disgruntled employees.

So I think what we have to hope is that Congress at some point is going exercise oversight over that part of the budget. But I think you are right, there is not much now, and it hasn't even been the focus of attention.

I'm not sure what you mean by shared risk, but it seems to me that one of the benefits of the programs that have been put in place has been the strong public health component of some of them. So if you are asking, can we think about how we protect ourselves against emerging diseases, a lot of this stuff that we are doing to protect

ourselves in order to identify some kind of biological event should be equally useful for emerging diseases. So there is a synergy there. But it is not clear that is what you meant. I really didn't understand that part of it.

DR. CHURCH: Just a quick word. I think both oversight and shared risk can be addressed by surveillance. That is partially a technological issue. We are getting better at inexpensive surveillance methods of biologicals, but it also requires some will to monitor people that are moving back and forth in BLS-4 facilities and going in and out of government agencies from academia.

DR. ECKERT: Sheila, could I just say one thing? I think that perhaps rather than characterizing it as shared risk, perhaps we ought to characterize it as shared interest. I think again, part of the problem here is, we are looking at this as U.S. security, when it is really, countries have the same interest to address these questions in terms of pathogens and weapons of mass destruction.

DR. GUILLEMIN: Let me be a little more clear about that. I meant the emerging diseases issue, avian flu issues, international cooperation. The SARS epidemic reference I used as a code. It did get to Toronto, it

actually did have repercussions around the world, though not as many as it could have had.

That is the shared risk issue among people in public health. It is a question of pandemics, but also, if you have millions of people dying for example in Africa, that is a risk that everyone eventually shares. We just don't want to look at it that way. But it is a public health reference.

DR. JASANOFF: Thank you for the clarification. We are almost into the coffee break time, but I see four people, and since this is a public information meeting, I think it would be important to get your ideas and questions on the record. So with the panel's permission, I am going to ask each of you to limit yourself to no more than a minute, and say very briefly what your questions are, and then come back to the panel if there is a last round of responses, and then break for coffee.

DR. GAST: We heard yesterday and today that export controls are probably not the most appropriate tool for today. I appreciate Sue's remarks. I find those in some sense perhaps to be an admission yesterday by some of the government officials, and that in itself is progress.

But we haven't heard what would replace them. Sue referred to our correction. I'm not sure whether it will be a correction or we could go beyond that.

I wanted to touch upon Suzanne's discussion of the fragmented world that industry works in, and think about whether the thesis that this interdependence helps stabilize the world. if component parts come from all these parts of the world, it is in their best interest to cooperate rather than to be confrontational, and to work together to be able to supply goods to these companies like Dell putting together the laptop.

So my question then is, would something that would be much more internationally focused, along the lines of a cooperation, be able to help rise above this idea that every transaction and movement between countries should be somehow export controlled?

DR. JASANOFF: Thank you. I will just ask the panel to hold your comments there.

DR. PEARSON: I'll try to make three very quick points and recommendations to the committee, and panelists can respond if they want.

First, I think we heard a lot from this panel and

yesterday that one thing it would be very good for this committee to do if we are looking at a fundamental rethinking of the structures, is to do a fundamental look at what the threat is that we are trying to address. That is what the Corson Committee tried to do when it did its work, and I think that is what this committee needs to do.

Especially in the biological area, we hear all kinds of different things about the threat. There are disagreements between the way the U.S. view threats, the way many other nations in the world view threats. Even within the U.S., three years ago the Director of Central Intelligence, to take a very narrow example, talked about bin Laden having a sophisticated BW activity. A few days ago the Director of National Intelligence talked about biological agents on a small scale being within the reach of some non-state actors, and by biological agents he meant crude methods for producing or disseminating toxins, specifically ricin. So that is a bit of a discord even within the context of three years in this country. So I encourage the committee to take a rigorous look at the threat.

The second point is, I would make the suggestion

that the committee may, in dealing with the issue of sensitive but unclassified information and so on, make the recommendation that we try to define in the biological sciences a very narrow range of information that simply should be classified, and that is the approach that we should take.

That actually has the benefit of again focusing a rigorous analysis on just what is the information that truly shouldn't be out there in the public eye, and in that way has a way of generating more openness, in the sense that it prevents the creeping encompassing of information that can otherwise occur. So I would suggest that as a recommendation that the committee might be able to make.

Finally, one thing that hasn't come up here is the distinction between the life sciences and all of the other sciences that impact on national security, physics, cryptology and so on. All those other fields have accepted military applications. In the life sciences there is no acceptance of military applications. That is a profound distinction that I think should somehow be inserted into the deliberations of the committee, and what that means for the types of information control mechanisms that get

established, and how other nations will interact with those information control mechanisms, and look at what happens in this country, just as we look at what happens in those countries, in the light of a technology that has absolutely no acceptance for military applications.

DR. IMPERIALE: I have a specific question for Dr. Church. It partly responds to Alan's third point. The committee has been thinking a lot about the fundamental differences between life science research and the other sciences. In that respect, when you talk about trying to have some sort of surveillance program or regulation of equipment or crude chemicals for doing synthesis, that sort of thing, the question is to what extent is the cat already out of the bag, and is it feasible to go in that direction.

DR. KELLMAN: I am hearing a lot of discussion about the tradeoffs between open flow of information and closing off the flow of information in the name of security.

I can't help but think -- and we did this, Judith, on the Fink Committee -- that this is really a bogeyman issue, that this is something that we can all stand up and proudly offer the virtues of openness. I

really don't think it is the relevant issue.

I stood up when I thought that Senator Hart's question was not answered very well. The question here is not, do we favor openness or do we favor closedness. The question is, can we develop systems so that information can get to the security structure without causing it to be closed off; can we protect confidential business information and confidential scientific information in a way that still allows those people who are engaged in the security process and have those responsibilities to have some idea of knowing what is going on.

I work in biological weapons issues. The issue is not what is going on on that pathogen in that lab, it is to have a general sense of what are laboratories doing. I don't need to get into this now, but the point is, we have to think about what are the kinds of reporting systems that are going to enable the security structure to be able to do what it needs to do without interfering, but taking advantage of the information.

How are those information systems going to operate at an international level? Again on a national level we are doing it not at all. So how are they going to

operate on an international level? What are going to be the measures and the processes for thinking about compliance? How will we have some way of knowing who is doing what they are supposed to be doing and who is not?

That leads to the most important point, which is, what we are fundamentally concerned about is not what these people do, these people writ by 100,000. We are really not interested in terms of security in what legitimate scientists, bio or otherwise, are doing. We are interested in the one in a billion who is a bad guy.

The question then is, what kinds of systems are we going to develop not to control the 99.99 et cetera percent that would never think about doing something that is harmful to humanity, but how are we going to have the systems that will enable us to quickly detect and hopefully interdict the one in some very low percentage who has a different bent.

Those are the questions I am just not hearing answers to. I think a lot of it technological. Some of it is policy, but I think that is the question that the committee has to deal with.

DR. JASANOFF: Thanks very much. That is a huge

challenge. I'm not sure that the panel will agree that it is a challenge for it, but I'll let them answer. But the, I'm not hearing any answers seems to go to the panel's activities of the morning.

DR. STEWART: Well, I certainly don't have an answer to this last question, but let me simply say that certainly I and perhaps other panelists were responding more to proposals that actually have been made, for example, the Commerce Department and the Department of Defense's proposals with respect to deemed exports.

The specific proposals that were made were proposals that would have changed if implemented in a straightforward way the quality and the character of graduate education and the research activity in the United States. That would have happened. That would not have been a good thing.

So perhaps in defense of all of us, I think what may be important going forward is to try to think more proactively about ways of articulating the core that needs to be defended than we have done in the past, and think more proactively about ways of facilitating the kind of communication that would lead to a more profound

understanding of that core.

So again, this is a process response, but I actually believe in process. I think process is how you get to content, and having the right process might allow you to achieve some kind of ultimate consensus.

DR. BERGER: I guess I would like to respond to the person who raised the last question. That person, I'm sorry, I didn't catch your name, but you said our problem is detecting the one bad apple in the billion.

From the point of view of being a faculty member at a university, it seems to me that at this point, looking at the government and looking at the fact that so many Chinese scholars that I know have not been able to come, listening to the difficulties of our graduate students, as I sit on this end it seems to me that the activities of the government have been focused not on detecting the one bad apple in the billion, but on the objective of reducing the numbers of people even across social sciences, even across fields which are extremely removed from any activity that in and of itself could seen to have --

So I think this question of what the threat is or what the effort of our own government has been with respect

to the flow of foreign scientists and students into American laboratories, maybe we don't exactly agree on what the process has been and what the objective has been, and what the problem to solve is.

Sitting where I sit, it seems to me that the effort over the last few years has been with respect to those coming from China to simply reduce the numbers across every category of scientist and researcher coming from that society into our university.

DR. ECKERT: I agree with everything that has been said. The export controls is not the answer to these problems. What you have to do is come up with what are other modes of cooperation, first after identifying what the true security threat is.

I agree, I think that in the life sciences you have a real core group of issues here that can be dealt with. If you can define that -- the issue of encryption, we went through this on encryption as well. We were so concerned about encryption, and we have largely dealt with it, and export controls are not the answer, again.

So I was particularly interested in what George said, because I think that -- I know people don't like the

term surveillance, but talk about voluntary codes of conduct, talk about putting in place procedures with regard to research. Those kind of systems can advance it. But in the absence of some of those specific models of cooperation, the private sector and the government and the research community's cooperation, where they are going to hold on to regulations. So what we have to do is articulate what those alternative modes are after defining what we want to protect, articulate what in some areas can be done.

Unfortunately, the answer may be in a lot of areas, nothing can be done. The fact is, the cat is out of the bag. Then are we really that concerned about those specific technologies we cannot control? It is a question of how we have our limited resources, and it is the cooperation with the community that needs to take place.

The ideas are going to come from groups like this and from the research community itself. The government is not good at coming up with ideas. It is good at defending what the current system is, regardless of how ineffective it is.

DR. CHURCH: I will try to answer the last two

questions with one answer. The question is, is the cat out of the bag in terms of surveillance that Mike asked, and what do we do about openness and the one in a million actors.

I think that the answer to both is openness. If we have ten million people teaming up against the ten bad actors, we have got a chance of combining intelligence. However, if we hide that information where only the ten can get at it, then we don't have ten million opposed to them, and we have a very serious problem.

I think our only chance is to follow this exponential curve that is going. We can't stop the exponential curve. That would be harder than many of the things we talked about today. But we can monitor it in an open way. The cat is not fully out of the bag. If we put cost effective monitoring of all the things that I mentioned, chemicals, oligonucleotide genes, equipment and expertise, if we just monitor them, don't stop them, just watch them, that means that somebody that goes and manufactures their own chemicals and genes, et cetera, is drawing attention to themselves by that activity. Even if we don't know what they are doing or why they are doing it,

maybe they are making yeast in their garage for baking, it nevertheless is alarming that they are doing it by an expensive and accurate and time-consuming manner, and we should watch them more carefully than the average baker.

DR. JASANOFF: Thank you very much. I'm sure there is plenty to talk about over coffee, so let's give our panel a hand of applause.

DR. GANSLER: Can you try to get back at ten after, so we can get back close to schedule? Thanks.

(Brief recess.)

Agenda Item: Creating A New Partnership

DR. GAST: I'd like to welcome you back to take your seats. It is a great pleasure to have the opportunity to introduce Mr. Timothy Bereznay from the FBI. The FBI has been very interested and active in these issues in the past year. They have been cosponsoring a committee of university presidents and government officials to discuss many of the same issues that our committee is facing with the new government-university partnership. So we particularly wanted to have a representative from the FBI here to tell us about some of those activities.

Mr. Bereznay is the Assistant Director for the

Counterintelligence Division of the Federal Bureau of Investigation. I encourage you to read his biography. I find it fascinating. Maybe I have read too many academic biographies and seen too many movies, but his last activity as a section chief on the Russian bug in the State Department is probably worthy of a side story conversation. It is a great honor and privilege to have him here today to speak to us.

MR. BEREZNAY: I would like to first of all thank MIT for hosting this event. I would also like to thank Dr. Gast, the committee, Dr. Gansler for the opportunity to speak here today.

I would also like to take a real quick moment to introduce some other individuals who are here today from the FBI. The first individual I would like to acknowledge is Tom Molleck in the front row here. Tom is going to join me for the question and answer session. Tom is a member of the Naval Criminal Investigative Service. He has been assigned to FBI headquarters for approximately one year now. The purpose of his assignment is to help the FBI understand the military acquisition aspect, and he has been very, very helpful in helping us understand that issue. We

will be talking about that shortly.

I would also like to acknowledge some attendees who are here from the local FBI Boston field office. I'd like to recognize Assistant Special Agent in Charge Kevin Kline and Supervisory Special Agent Lucille Broh, both here in attendance today.

Very quickly, what I would like to do is go back in time just a little bit. I'm not going to go back to the cotton gin or some of the other inventions that have been discussed, critical inventions, because they do shed the light on what the issues are here today, but I need to go back to discuss where we were in the counterintelligence program in the FBI, where we are and how we got to where we are today, and then some ideas about where we go from here.

I'll start in the end of the Cold War 1990 time frame. The walls are down in Berlin. The FBI had been funded very heavily for counterintelligence purposes to fight the Cold War. Over the next decade, Congress, the Department of Justice and the FBI demanded and took a peace dividend from those resources that had been devoted strictly to combat counterintelligence.

That peace dividend resulted in a shift of

resources away from counterintelligence. Instead, those resources went to address other pressing issues of the time, whether it was the war on drugs or the epidemic of violent crime that was impacting our country. The shift of resources was steady, and it continued through that decade. By the year 2000, the resources that had been devoted to counterintelligence were reduced by approximately 50 percent within the FBI. I would venture to say that there were similar reductions throughout the intelligence community.

In an arena with reduced resources, the FBI realized a series of counterintelligence failures in very rapid succession. In 1999, the FBI suffered through the Wan Ho Lee investigation, the investigation targeting a Department of Energy employee. This was followed in 2000 by the episode in which Russian intelligence successfully placed a listening device inside of our State Department. It was followed in the spring of 2001 by the arrest of Robert Hanson, who had betrayed the internal FBI operations to Soviet and Russian intelligence for over 20 years. Then September 11 occurred, and the criticisms of the intelligence community and the FBI for the failure to

connect the dots. The focus of all of these failures occurring in rapid succession in the FBI caused a lot of folks inside the organization to question what is going on, how do we stop the decline and how do we reverse this trend in order to truly protect national security.

While all of this is going on inside the FBI and inside the intelligence community, we have this whole horizontal transfer of information and information technology that is taking place simultaneously, if not preceding it, and we were oblivious to this transformation. What we did come to realize is that the FBI had been stuck, and it has been said over and over during the past two days, we were stuck in the Cold War model. Being in the Cold War model combined with the reduction of resources, the FBI found itself with its counterintelligence resources clustered around cities in the United States that hosted diplomatic presence, whether it was an embassy to the United States, mission to the United Nations, whether it was a consulate, but our resources were clustered around those buildings.

We came to realize that the threat was no longer a symmetric threat. It was no longer force against force,

Russians, Soviets, U.S. The very change that had evolved was more of an asymmetric threat than the symmetric threat of the Cold War. That asymmetric threat means that it was coming at us by different countries that we weren't focused on, and that the collection platforms being used by foreign governments to collect information in the United States, that those platforms were beyond just diplomats. Those platforms could be businesses, it could be academia, it could be advanced students, it could be researchers, it could be a wide variety of platforms that were available to use to collect intelligence.

It is in this background that Director Mueller one week before September 11 becomes Director of the FBI, not a good time to become Director. In the spring of 2002, he changed the priorities of the FBI. He tried to change the organization from the law enforcement focused organization, and he is forcing the change onto the organization that has as its top priority preventing counter terrorist, and he elevates to the second priority in the FBI counterintelligence. These are dramatic changes for an organization that had spent a good portion of its time based in a law enforcement mission.

He changed the priorities. We in counterintelligence have to now change our focus and change what we are doing. So in the summer of 2002, we rolled out to our 56 field offices a new strategy, a strategy that we wanted them to use as they address counterintelligence issues.

This is a logic model of that strategy. It is approximately a 30-page document boiled down here into a one-page chart. At the top, we want to protect U.S. against foreign intelligence collection and espionage, we still have to work espionage. The strategic goals that we wanted to address through that impact are to prevent proliferation of weapons of mass destructions. We want to prevent the penetration of the intelligence community, the U.S. government and/or its contractors. One of the hardest things that we have had to try to do is to try to protect critical national assets.

As we shift this mission, we have also got to shift away from that clustered environment we were in. So also in 2002 we began to shift our resources away from those buildings and establishments, and spread those resources throughout all 56 field offices in the United

States. We eventually got the point where every field office now has a component that is dedicated to counterintelligence, and it is to address the counterintelligence threat that is present in their territory.

How do we want them to go about addressing that threat? We gave them -- and it is shown down in the second box up from the bottom, those are the strategies that we put in place in our field offices. As we have gone through this, we have come to realize that if you were to put these in the correct order, engage in strategic partnerships is the most important piece in that box.

As we engage in strategic partnerships with a variety of entities, we then position the FBI to know your domain. So we are asking our field offices, know your domain. What does that mean? That means understand what is inside your field office's territory that is going to be of interest to foreign intelligence collectors or foreign governmental collectors inside your field division, understand what is there that is a target for collection activity.

We also want you to understand the threat,

understand who is coming into your territory, who is it that is interested in collecting that information which resides in your domain. The key to being successful in both of those endeavors is engaging in strategic partnerships.

As we worked our way through this, the field offices would come back to headquarters and they would say, who do you want me to have these strategic partnerships with? Who is it important that I deal with to understand the threat so that I can protect the counterintelligence equities present in the domain.

It was pretty easy to come up with the first group of folks we wanted them to engage with. That was other individuals, other governmental entities. We have to understand for the government what are the issues, counterintelligence issues that are of concern to us. So that was the first issue we tackled.

That was followed shortly by us dealing with private industry. Lots of things of interest to foreign collectors reside in industry. A shift in where those things resided; it used to be in the Cold War era, those things were owned, developed, by the government. A shift

has occurred, and as we heard the previous panel discuss, those things are dispersed now and many of those reside in private industry. So for us to know our domain and understand the threat, we had to engage with private industry.

The last one that we came to realize was important to us was to engage with academia and to have a discussion and open a dialogue with academia about what is it that we want to protect. Again, this whole shift is away from being a reactive program where we are waiting until Robert Hanson is identified to arrest him. We are not going to wait until the Russians have put a bug inside the State Department before we try to protect that equity, but it is truly a shift from reactive to proactive, and a shift to prevention, prevent the loss of critical national assets.

I would like to address those three different groups. We have used a similar approach in those three groups, and I will talk real briefly about each of those groups.

In dealing with U.S. governmental entities, there is at least 15 governmental agencies that make up the

intelligence community, and when you add on corollary agencies that have other responsibilities that impact counterintelligence, we are probably dealing in the neighborhood of between 23 and 25 different federal agencies that impact the FBI's counterintelligence program.

So we formed a national counterintelligence working group at FBI headquarters. We brought in representatives from all of those 25 agencies and we sat down and said, here is where we are going in counterintelligence, what is it you can do to help us, and equally as important, understanding what is critical to protect. If we have limited resources inside the FBI to address counterintelligence, we have to insure that those resources are going to the highest priority issues, and that we are putting counterintelligence protection around the most important information assets or intellectual property.

From the national working group we also came to realize that we have two big field offices in the FBI. One is located in Manhattan, New York City. We have another large field office located right across the river in Newark, New Jersey. Previously we dealt with the

counterintelligence program in those two offices as separate issues. So we had New York doing its own thing, Newark doing its own thing, and we won't let those two mix. It is based on the old judicial boundaries that we used in prosecuting our law enforcement cases. So we were set up based on judicial boundaries.

Bad guys, collectors, don't pay attention to those boundaries. They don't understand the boundaries and they are not worried about them. They are collecting across boundaries. So we had to get our organization dealing across boundaries, and we had to get them talking to each other, and understanding that the threat of a collector assigned to the mission in the United Nations or New York City could just as easily be targeted technology, targeting information, in New Jersey. So we had to get our organization talking to each other.

So that led us to regional working groups. From the national working group we dug down to a regional working group. In fact, we even asked them on a field office by field office basis that they engage in a counterintelligence working group within that field office.

The purpose of these regional working groups, the

national working group, is a sharing of information. It is a sharing of information from the FBI as to what we see is the threat environment at the present time, what is it that we see foreign collectors doing right now and how is that impacting the various entities within your domain. So it was the sharing of information that is the key. It is through the sharing of information that we are then looking for feedback from these working groups to tell us we have something that we think affects the whole effort that you have ongoing.

So we are sharing threat information, we are seeking their help in helping us to understand the threat, and understand who is being active in their domain. We also want their help to identify what is important to protect. We can't figure that out. It is a very hard thing for the FBI as an organization to say this is critically important to protect. You have got to help me figure that out, because I can't do it.

The other thing, we wanted to educate, and we started with U.S. governmental entities, we needed them to understand the threat from the insider. The insider threat piece was critical. We learned tremendous lessons as the

FBI from the failures of Robert Hanson, and there were at least two other penetrations of the FBI prior to Robert Hanson. In studying those cases, we came to understand that the insider threat piece was important to the government. As we matured, we realized that insider threat is just not a threat to the governmental entities, that insider threat is just as equal in private industry, and that insider threat is just as important in academia. The insider threat is the trusted individual who is inside the four corners of those walls, the insider threat.

We learned a valuable lesson as we moved into the next sector, moving out in our new strategy, and I'll get back to that in a moment.

Private industry was the second area I mentioned we wanted to get into. We began discussions, we began engaging with some of the largest defense contractors in the United States. We selected three of the prime defense contractors and we entered into a dialogue with them. We wanted to understand how they did their business. We wanted to understand how it is that they protect themselves.

In our discussions with them, we came to realize

that they had very good security. People understand security. That is gates, guards, guns, access, that is security. Security is very good, but it does not take into account counterintelligence.

We came to realize that there is a third piece that you have to roll into that, and that third piece is the cyber piece. That cyber piece as to what is on your systems, how are those systems protected, and who is taking advantage of your systems, and is that system being taken advantage of by foreign collectors.

So in coming to that understanding, we then come back and take a step back and say, the insider threat piece. To be effective in addressing the insider threat piece you need three s separate components working together. Those three components are your security component, it is your cyber component, and it is a counterintelligence component. It is only by combining those three elements that you are going to come up with an effective program to deal with the insider threat, whether that threat is in the government, private sector or academia.

We continued discussion with private industry.

We said, if this is what they think they need to have good counterintelligence, we need to help them. What we did is, we started working with Tom, Molly, working with Defense and said, help me understand how these defense contractors do business, how does this stuff work.

What Tom was able to bring to the FBI and to help us understand was, this is a graphic, a similar chart that came out in the last discussion, where it showed how you go from something that is an idea, you go into research and development, you then go into production, and then eventually in the military they worry about having foreign military sales.

In this graphic, as you move along this line, eventually that information may move into the classified arena, or it may move into the dual use technology arena. It may stay up top there, it may not dip down at all. It may just go from an idea to a laboratory for development to industry for production and eventually for sales, so it could be any technology this model will apply, but this just happens to be the military model.

So as we in the FBI came to understand how this worked, we also came to realize that for years, we had

focused the majority of our effort down at the very bottom of this model here. We were down in the classified world. We were staying and playing in the classified world, doing our business in the classified world.

What Tom and the military, DoD helped the FBI to understand is that a lot of that stuff worth protecting is being done in the research area, it is being done in development, it is being done in laboratories. The bad guys -- bad guys is an old term; foreign governments have figured this model out, and foreign governments have figured out that they can target the technology, the research and development, before it is protected, and that by doing that they can save themselves tremendous costs in research and development.

So coming to this understanding is what led us to the next step in our evolution here. That is, reaching out to academia. Academia is involved in this cycle. They are involved in the research. They are involved in classified research. So the labs that develop it are in academia.

Private industry I have addressed earlier. We are talking with them and trying to understand that, but as we have come to understand the cycle we then go back to

industry and we say, we think we have figured it out now.

So what we did is continuing to work with industry. I think we are not quite there yet with academia, but I think we can get there. We developed a tool, it is a counterintelligence vulnerability tool. It is a tool that, based on the best knowledge of the FBI, members of the intelligence community, members from that national working group, we have put together this tool that we share with private industry.

We will give them this tool. It is a tool that they can look at to evaluate how are they positioned to address the insider threat, how is their security dealing with their cyber piece, how is all that dealing with the counterintelligence piece, and how well do you understand how you are being targeted by foreign collectors.

We have rolled that tool out to private industry within the past six months. We are starting to get the feedback from private industry. As we get that feedback, we will continue to tweak that tool and continue to make it relevant for use by private industry.

The second piece that helped us identify dealing with academia, once we realized how this worked, was a

study that was done by the RAND Corporation. It was done in 2002. I believe it is referred to as Radius. It basically was a report that tracked federal funding for research and development in U.S. colleges and universities. It was getting this information and studying this information that helped the FBI make the next step in our development of dealing with academia and why it was critically important.

At the time, it was $80 billion a year of federal funding going into research. I believe that although there has not been an update to this study, the information I am getting is that it is around $120 billion, and I'm sure the folks in academia here can probably give me the dollars and the cents by federal agency. I just don't know that off the top of my head.

But understanding how this model worked led us to saying we need to engage with academia in discussion. That is what led us to the next step, which is an academic alliance, research alliance. Again, the focus is an awareness on the part of academia, awareness on the part of the federal government as to what is going on here, and eventually to the formation of the National Higher

Education Advisory Board.

That board was formed in September of '05. There was a press release, and I'd like to read just two snippets from that press release. It was announced by Director Robert Mueller that he has formed this advisory board in order to foster outreach and to promote understanding between higher education and the FBI. Please read that to mean really the U.S. government, because through that national working group we are bringing all of the federal inputs into this and engaging in this dialogue with higher education. Graham Spanier, the President of Penn State University, was the chair for this board, and has been very instrumental in helping the FBI get this board up and running.

To further describe the FBI vision of how this board would work, I will also quote from the press release from Director Mueller. As we do our work, we wish to be sensitive to university concerns about international students, visas, technology export policy and the special culture of colleges and universities. We also want to foster exchanges between academia and the FBI in order to develop curricula which will aid in attracting the best and

brightest students to careers in law enforcement and the intelligence community.

In September '05 is when this board was formed. Those are the members who participate in the board. It has had two meetings. The third meeting is scheduled the first week of June. The first meeting was pretty much introductory. The second meeting is when things got down to issues. At the request of Dr. Spanier, Assistant Secretary for Commerce McCormick was present and a very lively discussion ensued on the deemed export issue. Not much else was accomplished at that meeting, but it did serve as a forum for an exchange between academia and the FBI and the government, a very healthy dialogue.

I'm not going to take credit for today's announcement. I don't think we had anything to do with it, but Assistant Secretary McCormick did leave that meeting with a very clear understanding of the concerns for academia, so it was I believe very successful. There will be followup on that issue at the June meeting.

I do want to mention one other issue that has been a significant change in the counterintelligence program in the FBI. That change occurred in December of

'04, 2004. As we understood that model and that we were trying to protect technology, trying to protect critical national assets, protect what is important to the United States, we realized that we weren't positioned to do that.

So we petitioned to the Department of Justice, and were successful in getting concurrent jurisdiction with Commerce and EIS into export control violations. However, the Department of Justice limited our jurisdiction and those violations where we could show that there was a foreign government sponsored effort in that collection activity. So we are not worried about all export control violations. We are not worried about all munitions control violations. The FBI was focusing its efforts on those instances where the activity was being sponsored by foreign governments.

As a result of that jurisdiction, we have shifted the focus. This is a shift that is critical. I think it points out a significant change in counterintelligence of the U.S. government.

In the past not quite two years, since we have got that jurisdiction, we are seeing a change in the prosecutions being used by the Department of Justice. That

shift is away from enforcement of the espionage statutes and more towards the protection of dual use technology.

There is a growth in prosecutions on the technology side and the espionage side is still important, we are still going to aggressively pursue espionage investigation, but I think we are seeing the beginnings of a shift away from the old Cold War espionage, protect classified information. I think the violations in the future are going to be more in line with intellectual property and dual use technology.

I would also like to comment on one other pattern that we are seeing. I am asked constantly about foreign students and what is the FBI doing about foreign students, why are you investigating foreign students.

What we are seeing, and the trend is -- and this is in the public domain, there are a number of these arrests that have made their way through the prosecution process, and what we are seeing is a trend. The trend is, there are students from China who come to the United States to get their degrees. They come to get an advanced degree, they come to get a doctorate degree. Once they get their degree, they then leave the world of academia and they go

into the world of business in United States. They will go to work for a defense contractor, and they will be on the unclassified portion of that project. They become PRA, permanent resident aliens, and eventually qualify for U.S. citizenship. Once they have citizenship, they then move from the unclassified arena in U.S. industry into the classified arena, where they develop the contacts, develop the understanding of that technology. Eventually they move away from the U.S. private industry piece of this and they start their own front companies, they start their own technology broker companies. They have the contacts in industry, they understand what pieces are important.

The trend that we are seeing is that there have been a series of approximately 25 arrests over the last two years of U.S. citizens of Chinese ancestry who are involved in the collection of dual use technology for the benefit of China. So that is the trend that we are seeing develop.

Are we focusing on these students when they are here as a J1 student? No, but that trend does exist. Is that going to be the future? I don't know.

In summary, what I would like to say is that we started this transformation of the counterintelligence

policy inside the FBI with the recognition that we needed to be engaged in strategic partnerships, and that strategic partnership eventually moved us from dealing with governmental entities to the private sector, and now we are trying to engage with academia in this discussion. Again, the objectives are, we want to engage in those strategic partnerships to help us understand our domain and understand who are the intelligence collectors who are targeting that domain.

Thank you very much.

DR. GAST: I imagine there might be some discussion. Senator Hart has departed, so someone could ask on his behalf.

DR. ECKERT: Just picking up on a point made yesterday, I comment the FBI in moving forward and trying to think about these issues in a different way, but one of the questions was, what is the true nature of the threat and what kind of information can be shared. I think that until some of the information gets out there -- it was news to me that you had 25 cases of Chinese-American citizens.

I think to the greatest extent possible, it would be very helpful to the community to try to understand what

you are seeing in terms of trends and the information that you have. Even in some of the previous NAS meetings, they are alluded to studies and things underway, but from what I have heard from people who have heard the classified version, let alone the unclassified version, the information that was given was really not very persuasive at all.

I think from your standpoint you have an education problem, if there is a problem, but you have to define what the problem is for the community in order to understand what kind of actions they need to take.

MR. BEREZNAY: In dealing with the defense contractor industry, it has been a little bit easier for us moving forward, because the vast majority of the businesses that we are dealing with do possess clearances. So we can share the classified information with them.

In dealing in the unclassified, we have to wait for the prosecution of these cases to conclude, at which point in time we then need to be aggressively engaged in educating not just academia, but the U.S. public about what this means. I don't want to draw any conclusions about what it means, because we are way too early in this process

to be making any conclusionary statements about what is China doing.

We are very concerned about it. We are looking at it. There are two cases right now that are in the prosecutive process that will have direct impact on academia. As those cases move forward it will be incumbent upon the FBI to share that information and to be engaged in all 56 field offices, the three sectors, in sharing that information.

That is the relevance that we bring to this, that this is the threat as we see it right now, and this is how we believe they are trying to disadvantage our national security.

DR. GAST: I think you could share with the academic community some dope, because quite a few of us have clearances.

MR. BEREZNAY: They do. In fact, everyone on that education board does have a clearance. Those that did not have it, we got them clearances. In fact, we had to shift the composition of that group, because there was one individual who was from Canada who the Canadians did not want us to give him a U.S. clearance. So we had to juggle

that a little bit, but we do.

DR. GAST: I would urge you even with this panel to share the information, because it is hard to draw conclusions unless you know the information, and a number of the people have clearances and can receive that information.

MR. BEREZNAY: Very good. We will work with them to do that.

DR. BIENENSTOCK: It was striking, the numbers that you gave in the scenario that you just described. I think we have hundreds of thousands of Chinese students passing through American universities getting doctorates. You are talking about 25 cases after people have had access to classified information. It would seem then that academia is too early in the chain to be looking for them. You would have to apply such a blunt instrument at that level that it wouldn't be very helpful.

So I am uncertain what you are going after with academia. I would be the person at Stanford who would have to deal with it. I am uncertain as to how you deal with these very large number of students. Well, I made my point.

MR. BEREZNAY: I don't disagree with your point. I think it is a very valid point. I think as we look at this issue, when we come to understand it, as we engage in the dialogue with universities to come to truly understand what are the issues, what is it that is taking place on your campuses.

If that discussion educates and enlightens the FBI that you are wasting your efforts in this endeavor and you may be best focusing elsewhere, if that in the end is the outcome, then we accept that outcome. But I think we are in the process of trying to understand that threat right now, and as we continue to evolve and the information continues, I think there is a bigger issue there, a fundamental issue of, is protection warranted in this environment. I think that is the question that this committee is struggling with.

DR. GAST: I'm afraid we are running short on time, so we can have maybe one more question.

DR. RUDCZYNSKI: Andrew Rudczynski from the University of Pennsylvania. From your presentation I think you described an approach about -- you have bilateral threats that are present, and you are trying to address two

separate issues, and I am wondering about your approach to these.

First of all, the first approach you talked about was the protection of U.S. assets from foreign governments. But I think you also have this much more diffuse threat from unaffiliated actors. It seems to me that you are applying the same techniques to both of these issues, when they may actually demand different kinds of solutions and approaches. I was wondering how you would go about differentiating these two major loci of interest.

MR. BEREZNAY: One of the cases that I am citing that is in the process right now is one of those diffuse collectors that you are talking about. It is a case that is currently pending in Hawaii. The subject of that case is an individual named Noshir Goadia. He is an example of the second class that you have mentioned. Because it is a pending prosecution, I am reluctant to comment further on it today.

I think the key is educating the target, who is being targeted by these individuals, whether they are doing this as a state sponsor, whether they are doing it as a private businessman, doing it for profit, or whether you

are doing it as a surrogate for some affiliation of individuals that may or may not be nation states. So it is really an education part. I would like to discuss more with you the other case, but I can't do so at this time.

DR. GAST: Thank you very much.

MR. BEREZNAY: Thank you.

Agenda Item: The Role of the Research University in U.S. Security and the Need for Rational Government Policies

DR. SKOLNIKOFF: Given the time, and leaving the best for last, Chuck, it will just be a very brief introduction. You have the description of Chuck Vest's background and some of his many activities. The little biography doesn't begin to cover them all.

I just want to say it is a special pleasure for me to introduce Chuck. I was part of the search committee originally back in 1990 that recommended Chuck Vest to be president. Our faith in him and what he could do was amply justified by 14 years of superb leadership of this institution. Chuck has been not only a leader of MIT, but he has been a national leader for science policy and for

science and technology in the research universities generally. He is a member of the President's Advisory Committee on Science and Technology, was once president or chair, whatever the title is, of the AAU. He was on the Augustine Committee, you have the report that was handed out. In any case, a whole series of very important national activities which I don't think even come close to the role that he has played not quite such a public role, but in Washington generally and with the Congress and with the Administration.

He is one of the rare people that has very strong views about what is important, and is able somehow to work with people from very widely varying political orientations, not only to deal with the issues but to be constructive and not to get people angry at him. I don't know how many people have gotten angry at you, but I don't think very many. He has made a huge difference for us all. I don't even know what party he votes for, so that seems to me a great recommendation.

Chuck, please.

DR. VEST: Thank you very much, Steve. I have to say that I have got a great fondness for the Boston FBI

office, because I had the incredible privilege of serving on the Rob Silverman Commission for over a year on intelligence and weapons of mass destruction. I spent many long winter hours in a skiff over in the Boston FBI headquarters, editing the two final drafts of that report.

I also want to say that I thought Mr. Bereznay's presentation was extremely important. It left an image in my mind that I would commend to this committee. The curve you used, starting with fundamental research, working through the universities out to the end of the acquisition cycle is very telling, but it should be three dimensions. The whole point of this conference is, there is another curve that starts at the same point, then comes down and moves up the scale of commerce and building our economy and health and quality of life and so forth. It is trying to figure out how to put these two things together in the right way in those early cycles that we are all talking about.

I also have to say that based on the experience of the Rob Silverman Commission, it was very painful to put a signature on a report that was a very strong indictment of information failures, because despite that, I came to

understand that there are some incredibly good and dedicated people in the intelligence and counterintelligence communities, to whom we all need to be very grateful. So anything I say that is critical is still in that context.

First of all, as I know has been said many ways during this meeting, we have to work together. Partnership is essential for a number of reasons. First, maintaining U.S. leadership in science, technology and health. Second, to combat terrorism and other security threats to R&D and through our education, and third, to understand the risks and benefits -- and I am going to try to emphasize that a little bit in my remarks -- understand the risks and benefits associated with potential restrictions on the way we do things in universities.

Having just heard from the counterintelligence context, let me look a little bit at the context for universities, research and education. I think there are four key issues that we have to wrestle with. First is enabling national, and as someone commented yesterday, also global economic vitality, health, security and quality of life, contributing through our universities and our work

directly to our national security, third, handling scientific information and materials, which is what has in essence brought us together, and fourth, figuring out how in all of this to maintain the openness and the global flow of people and ideas that is inevitable and important going forward.

So I am going to make just a couple of very brief comments -- I know there will be some redundancy -- on each of those four things. First of all, America's comparative advantage in 2006 in this world is a strong science and technology base, coupled with a free economy. I would add to that, built on a base of democracy.

We all know that we have something very informal, very loosely coupled, that we call an innovation system, that creates new knowledge and technology through research, that educates young women and men to not only create more new knowledge, but also to understand what is being generated and to ultimately move it into the marketplace in the form of new products, processes or services.

This has been an enormous success. You all know these numbers. At least half of the growth of the economy since World War II in the U.S. has been due to

technological innovation. Much of that has come out of universities.

I like to show this list that I put together six months or so, because sometimes we know that we are not as appreciated as we might be for some of the really major things that have come out of universities.

Here are a few innovations, these don't happen every day by definition, in which universities played either the sole or at least the dominant role, computing, laser, the Internet, the fundamentals behind the GPS system, numerically controlled manufacturing, the organization of the World Wide Web, financial engineering, the genetic revolution, modern medicine, et cetera. This is not to use the phrase used yesterday small potatoes.

What about contributing directly to national security? I'm not going to emphasize this today, but I think we all are very much aware that there are things we can do, and more things to be done. But in saying that, I want to make a couple of points here. One is that counterterrorism is not all about high technology. Second, I don't believe that a Manhattan Project style activity which many have suggested fits the role of terrorism. It

is too unfocused, it is too complicated, too diffuse, has too much non-technological component, and so forth. But I do believe that we can and are in this and many other universities contributing to this national issue through specific projects, and also through participation as partners with government and industry.

I also want to make the point, and I know it is redundant with previous speakers, but life science and biotechnology I believe do pose particular opportunities and challenges that are actually quite different than those that we are used to dealing with. Just as the counterintelligence world has to make a shift from the Cold War era, we have to understand that some of the challenges based on modern life science are quite different than things we have dealt with in the past.

Just a reminder that terrorism to date has been pretty much a low tech undertaking. Mechanisms, knowledge bases, truck bombs, commandeering commercial aircraft, credit card fraud, materials, nothing particularly sophisticated, fertilizer and diesel fuel, off the shelf chemicals.

The second-largest attack in this country by

terrorists was of course in Oklahoma City. The terrorist was a white American citizen and veteran, and he used a rental truck and fertilizer. I think it is very important particularly in the university world that we keep these things in mind.

But of course, our worst nightmare is about terrorism are those with a much higher technology content. The idea of nuclear weapons and missiles being used against us, either by state actors or worse yet, in the hands of terrorists in some way, the information to do these things has been accumulated over many years, and the materials involved must be maximally secured and are. But as we know, unfortunately there has been huge leakage around the world, materials out of the former Soviet Union, knowledge and technology through the AQCON network, and so forth.

Cyber terrorism, mentioned in the previous speech. Again, the information that is needed is quite sophisticated, but it is absolutely readily available. What about the materials to be used? Well, computers and high-speed network connection, it is everywhere. Bioterrorism, much of the information that is needed is readily available. The facilities needs are quite modest.

Materials we have to be careful with, among other things, by securing them and minimizing them.

So how do we in universities handle these things, the materials and scientific technology information that could be useful for terrorism? These are very simplistic comments, but I wanted to try to keep it at a fairly high level here.

I think we have to think about the seriousness of strength of risks. The most serious kind of things even today in this post Cold War era are knowhow relevant to sophisticated military scale weapons systems. We must continue to take these things extremely seriously.

The vast majority of academic science and engineering research, while I am not naive enough to say poses no risk, in general is modest at best. As was pointed out previously, generally they are things that take many years before they might come back to haunt us. One can dream up counter examples to that, but I think in general modest at best.

In truly fundamental research and education, I think the risks are minor to nonexistent. I'll come back to that point in a moment.

So I think for these serious things we must continue to apply traditional classification mechanisms that are well understood, well in place, we know how to deal with them, as we do at MIT in our Lincoln Laboratory, in industry, and so forth.

For those that are modest at best, and those are frankly what we are here to talk about, I would say that there are not many obvious actions that we need to take, and those that are minor to nonexistent, truly fundamental research and education, I hope that we do nothing.

Now, think a little bit about this. Some of the things that are in the academic domain in terms of materials will include in a small number of university laboratories around the country certain pathogens which are absolutely deadly dangerous materials. We have a responsibility, and I believe we are, and I believe the government guidelines are in pretty good shape, we have to be extremely serious about restricting amounts and use and access to those pathogens.

There are a number of dangerous chemicals around that are pretty modest in their danger, but it is not zero. Then I think there is access to explosive chemicals, and so

forth and so on.

So the first, as I say, reduce access, restrict amounts, track carefully. These today follow the select substances regulations, and I think those are generally good things as long as the lists remain appropriately moderate in length.

Dangerous chemicals we should be careful with. I think the main thing to do is use the smallest amounts possible, and inventory and track carefully, and for other things that have modest dangers, just keep your inventory small.

A few other thoughts on risk reduction, about knowledge, information, education that has at least potential damaging uses against us. As I said, we have to maintain in this country a sound classification system. I will comment in a little bit, I think we classify too much, but that is classified, we have to protect appropriately.

I think we have a responsibility in our universities to educate our student researchers about security. I think this should be wrapped together with the other things we have a responsibility to embed in the thinking and actions of our students, that is, issues

around health, around safety, around environment and so forth. I think these should all be put together so it becomes a natural consideration that is in the water and the air, so to speak.

I think that as simple a thing as strengthening laboratory groups and their communication and their sense of community is one of the most important things we can do. If people are working together all the time, quite frankly the opportunity to engage in dangerous activities goes down relative to a system in which kids spend long hours in the laboratories by themselves.

I think we have to emphasize care and rapid processing and granting of visas, something I am not even going to take time to talk about here, we all know these issues, while we remain open and welcoming. We do have a responsibility to maintain at a certain level tracking systems for students and visitors, but the information tracked should be very, very highly limited. In scientific materials, I have said what has to be said about that.

Let me turn directly to the issues of openness. I believe that fundamentally, walls just won't work, especially in 2006 and beyond. First of all, and this is

our side of the Cold War mentality, we know now that people everywhere in this earth are smart and capable. We can no longer pretend that the U.S. is the fount of all important knowledge, and it is just a matter of protecting other people from knowing the things that we know. People everywhere are smart and capable.

Science and technology, regardless of steps we take or don't take here, are going to continue to advance relentlessly. I have a little map I sometimes use in presentations about innovation that shows that by sector, North America, Europe, Asia, we are spending in each of those areas almost the same amount on R&D today. We are about 40 percent higher in North America, but in general everyone is increasing spending in these areas.

Globalization is a dominating reality. No use to talk about it in the abstract anymore. It is here. It is here especially for industry. We have to recognize that. We also have to recognize how fundamentally we have been transformed by the Internet and the World Wide Web, which despite the vulnerabilities that they bring to bear are in my view the most important democratizing forces out there today.

So we in universities are being pushed and pulled. I think we are being pulled outward by the web and by globalization, and we to some extent being pushed inward by concerns about dangers of all too real terrorism and by export and immigration controls and so forth.

I put this simple diagram for the purpose of stating that the web and globalization are huge forces, and they are going to be present, and if we are not the ones to respond and recognize the opportunities, it will simply be universities in Asia or Europe or elsewhere.

Terrorist dangers today exist everywhere in the world, and hopefully the more awareness we have, the more we can protect ourselves a little bit. These are all giant forces. The forces of export and immigration controls on the other hand are policies set by our government, relatively finite in scale, and things that we can talk about how to do better than we are currently.

Two quick lessons, or at least we might consider them lessons. One is to step away from the military and terrorist based threats and think a little bit about economic security. I start with what I am going to call the theory.

Back in the 1980s universities were considered to be huge sources of technology which was going to flow. The term used was normally our crown jewels, was going to flow out of universities in general, MIT specifically, over to Japan where people were going to take it, commercialize it, come back and eat our lunch economically.

The reality is, after all this sturm and drang was over, I would propose that we probably learned more from the Japanese about manufacturing and management than they learned from us technologically, despite the fact that I wouldn't begin to kid you that the wanted a level playing field. I think throughout this period, standing up for openness ultimately served us well, even though as I say that openness was pretty asymmetric between Japan and the U.S. at that time.

What about the Cold War? I think there is a very important thing about the Cold War, because we won. Our technology superiority was absolutely essential in that victory. It was driven by our research universities and our national laboratories by and large, and was developed as we all know in large measure by immigrant scientists.

Again, I think our open society and institutions

were superior. Many people in this room know very well that the Soviet Union was full of brilliant scientists and engineers, but that constrained inward-looking system did not stand up to our openness. Global communication, keeping the lines of communication particularly in the scientific community between the East and West at that time was very important.

So I think these lessons, while they don't map exactly onto the problems today, still are things that we need to keep in mind.

Let me close by doing something really gutsy. I attempted to answer the eight questions that your committee posed, or at least give a little guidance to them. So don't take all these too seriously. That is why I say these answers may be a little easy, but there are a couple of serious points certainly within them. I tried to paraphrase your rather lengthy questions.

Number one. Today what is the appropriate conceptual framework for national security, science and technology research, given speed, competition and terrorism? I do not mean this to be flippant. I am absolutely serious. I think the primary framework is what

I have stated here, that it is more important to keep filling our bucket with new knowledge and technology than it is to obsessively plug all the little leaks.

I think it is finding that balance that we have to deal with. Plugin links is great if it is going to be effective, but the problem is, if all your energy goes into that and you slow down the filling of the bucket for all the right reasons, you will be in trouble. It is a little bit like the famous quote from Through The Looking Glass. We are in a situation where we have to run twice as fast just to keep in the same place. So we can't slow the system down unnecessarily.

Secondly, what threats do we face, and how do sensitive but unclassified designation and deemed export controls mitigate them appropriately, given the character of 21st century scientific discovery? I believe, maybe a little naively, but I believe that clear bright boundaries tempered by sound informed judgment are what make good policy. Not so much in the context of what has been said here today, but some of the other things that I am a little bit cognizant of.

I think one thing we do is, we classify far too

much stuff in this country right now, thereby overwhelming our security apparatus unnecessarily. More relevant to the work of this committee, I believe that the designation sensitive but unclassified should be somewhere between rare to nonexistent. In other words, we should figure out what the really critical areas are and we should build high fences around them, everything else should be secondary.

Third, can we afford security policy that does not address economic issues? And how do we integrate security with international commerce and interactions, controls and openness? Again, a little bit simple but I mean this quite sincerely. First of all, if we lose our economic security and our personal liberty, the enemy will have won.

Secondly and a little more complicated perhaps, but I think if we fail to bring more and more of the world into better economic, educational and human health, the enemy again will have won. These to me are the primary arguments for coming down on the side of openness in the vast majority of decisions that have to be made.

Fourth, what risk-benefit analysis is needed for the security and for research academic communities to

promote mutual understanding and good policy? We should probably spend more time on this than most of the things that I have mentioned. I think it is just common sense and experience that common cause is forged when people work together on substantive issues. Trust and effectiveness for both of us, both the counterintelligence and security communities and the academic scientific communities, will be the byproducts of this.

I think that risks can be categorized. It is always a bit of an art rather than a science, thinking about things as Ropick and Gray's book points out on two metrics: What is the likelihood of this threat occurring, and what are the consequences. It is weighing those two things together that begins to help us do a risk-benefit analysis.

I think, and this is a very specific suggestion, I think it would be a very productive joint endeavor for the science and security and intelligence communities to work together on doing a lot of risk analysis. This helped us get started, by the way, several years ago in thinking about environmental issues. Working together, much of this could be done, I'm quite certain, in the unclassified

domain, just thinking through threats, thinking about consequences with good strong -- this would be a great way for people to work together, do something worthwhile, get to know each other, and hopefully form this better sense of common cause, trust and effectiveness. I'll come back to that in just a moment.

Number five, do biology and biotechnology raise new kinds of security concerns? What paradigm is needed? The answer in my view as a non-life scientist seems to be, yes, absolutely, these are somewhat different entities than we are used to dealing with. Again, thinking about risk assessments would be a good way to get started in thinking about this.

Once biology and synthetic biology and so forth begin to enter the scene, this is certainly not yesterday's war, and it is not going to be won with Maginot Lines, or even the nuclear weapons style controls. Open cooperation of some form between the intelligence, security and science communities is absolutely essential.

Maybe the most important message I would like to leave with you is, you have got to engage young scientists. It can't just be all of us folks that have been around a

long time that worry about these things. You have got to get the new people who have the vision of what the future is going to be, who understand its pace and so forth, we somehow have to get them engaged. As several speakers have said over the last two days, this is going to have to be done in some kind of a new open format. There are some starts on this.

What is the role of social science in the security discussion? I think it is huge. I think that social science and also scholarship about culture and history are absolutely essential as we heard the other day from Professor LaFree to understanding the causes and nature of terrorists and terrorism, to contributing in very important ways to risk analysis, and frankly, to balance the somewhat technology-centric view of threats and countermeasures.

I don't want to trample on anybody's toes, but I keep thinking back to the days immediately after 9/11. As you can imagine, my e-mail was full from within the MIT community and from other colleagues in engineering schools and so forth around the country, of ideas of what we should do. The most popular idea was, we needed immediately to

put a crash program together to figure out how to take over remotely the control of aircraft when they were commandeered, and land them. I think it was a much better idea to harden the cockpit so people couldn't get in. So we can't let ourselves get too carried away with the technology-centric view of either threats or countermeasures. As I pointed out, to this point in time, while it may not be true forever, it has been a pretty low-tech business.

The lack of perspective and strategic analysis from the social sciences and so forth were absolutely at the core of some of our worst intelligence failures, especially that in Iraq. This isn't the time or place to draw that out, but trust me, it is a true statement.

Finally, social science is essential to the privacy and security debate that is going to be heating up even further in this country, in which the Academies are again going to play a role in trying to think through.

Number seven, what are the effects of restrictive policies on research and education collaboration in universities, national labs and abroad? Just very simply, if they continue to grow rather than attenuate over time,

they will isolate us from each other, and do it at a time when collaboration, interdisciplinary work, globalization and to use the increasingly popular industry phrase, open innovation, are cornerstones of progress.

Finally, number eight. What mechanisms for government-university-industry dialogue and radar will work best? Should these discussions be international? Here I am going to go out on a limb and make a few specific, sometimes Don Quixote-type recommendations.

First of all, I think we should begin by strengthening the role of scientific and technology advice in our government, beginning with the age-old quest to strengthen further the role of the President's Science Advisor and the office that supports him or her. I think that every Cabinet Secretary virtually should have a serious science and technology advisory mechanism. The Defense Science Board is a great model and has been very effective over the years. That provides the kind of continuity that we need. I think the new intelligence community university board will have that same kind of role of continuity, high level policy.

But I think we also need what I have always

called in the university world hit and run committees, things that get thrown together in a very agile and timely way when issues come up to provide sound analysis and policy advice regarding security threats. This could go back to the risk-benefit, it could be other things. It should involve young people.

The reason I like this kind of pull a group together, get a job done, let them disband is, they don't get sucked into it. Whatever you do, if you do it long enough, you begin to form hardened opinions and views. You need these fresh insights and continuity.

I think there probably will be instances in which some level of international participation is known. I haven't thought that through in great depth.

Just a few further recommendations. I hope the first one doesn't seem too self serving, but we should implement the pace in ACT legislation, that is, to implement and fund the recommendations of the Augustine Committee outlined in the executive summary of the Rising Above the Gathering Storm report you have. This will bring more Americans into science and technology. It will simultaneously help us to maintain our openness to the best

and brightest around the world, and keep that S&T base on which many important things are ultimately based strong.

I think as you heard many people say during this day and a half, we have to reinvigorate the American can-do spirit and get rid of this total dependence on oil. That is the most important thing, as many others have articulated more knowledgeably than I, perhaps the most important thing we could do.

Here again, being a little bit of a Don Quixote, I think the President of the United States should reissue and order a strict interpretation of NSDD-189. That may sound pretty esoteric, but those of you in this room know that that is the basis of much of what the university community has been worried about. It remains the policy of this Administration and our government, but it has lost its teeth, and is being interpreted far too loosely by people who are understandably risk averse many layers down. I think the way to attempt to break that is to get it reissued by the President.

I think we need to make another quantum leap, I don't know what it is, in the processing of visa clearances, especially for scientific visitors. Here I

want to say that everybody literally from the President on down has worked hard and effectively at improving the issues around visas especially for our students and long term visitors, but there is still more work to be done.

As has already been announced by Under Secretary Dave McCormick, we will conduct a high level government-university-industry review of deemed exports. It is a good start, but I think that once we get that done, and that is the most important immediate issue, we really need some serious rethinking of the entire export control regime.

Running through all of this conference has been a view that the world is changing fast and industry is operating in totally new ways, and somehow this too needs a real fundamental rethinking.

Finally, I would call on the Academies to jointly establish a panel with the intelligence community to rethink intelligence gathering, specifically regarding bioterrorism capabilities. There are some things underway, but this is the really new, different, nebulous thing that I think still requires a lot of work.

I know that Senator Hart has left, but I want to end with the famous quote from the Hart-Rudman report,

written months before September 11. Second only to a weapon of mass destruction detonating on an American city, we can think of nothing more dangerous than a failure to manage properly science, technology and education for the common good over the next quarter century.

Thank you very much.

DR. SKOLNIKOFF: I told you we saved the last for the best. That was wonderful, Chuck, thank you. We have a little time. Any questions? It is a good thing you didn't talk yesterday, Chuck, because there would have been no point in having a meeting.

If we have no further questions, I will take the opportunity to call the conference to a close. I think Alice has a couple of remarks of logistic type.

DR. GAST: Chuck, I would like to thank you very much. We do need a copy of your slides so we can write our report.

I would just like to thank everybody for their participation. I think it has been a very fruitful discussion, and we benefitted quite a bit from input from everybody. I would like to remind you, for those of you who are roadies and want to follow us around, our next

regional meeting will be at Georgia Tech on June 5-6, and then a third one at Stanford University on September 27-28.

So thank you very much. You know where to reach us if you have additional thoughts after this and would like to give us input or ideas or suggestions. We are very grateful for all your input. Thank you.

(Whereupon, the meeting was adjourned at 12:40 p.m.)