

Note: This is an unedited verbatim transcript of the Deemed Export Policy Workshop, held on May 6, 2005 and prepared by CASET Associates and is not an official report of The National Academies or The Policy and Global Affairs Division. Opinions and statements included in the transcript are solely those of the individual persons or participants at the conference, and are not necessarily adopted or endorsed or verified as accurate by The National Academies.

THE NATIONAL ACADEMIES

NATIONAL RESEARCH COUNCIL

**THE ROUNDTABLE ON SCIENTIFIC
COMMUNICATION AND NATIONAL SECURITY
THE PROGRAM ON SCIENCE, TECHNOLOGY, AND LAW
THE GOVERNMENT-UNIVERSITY-INDUSTRY
RESEARCH ROUNDTABLE**

**DEEMED EXPORT POLICY:
A WORKSHOP ON THE INSPECTOR
GENERAL'S REPORT TO THE
DEPARTMENT OF COMMERCE**

Friday, May 6, 2005

**The National Academies
Lecture Room
500 Fifth Street NW
Washington, DC**

Transcripts By:

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

TABLE OF CONTENTS

	<u>Page</u>
Opening Introduction - Dr. Colglazier, NRC	1
Presentation of the IG Report:	
Moderator: Mr. Murphy, CSIS	3
Mr. Lichtenbaum, Dept. of Commerce	5
Discussant Panel:	
Moderator: Dr. Hamre, CSIS	49
Ms. Johnson, Texas Instruments	52
Dr. Mote, University of Maryland	61
Mr. Rice, Coalition for Employment Through Exports	67
Dr. Short, DoD	72
Mr. Fisher, DoD	79
Questions and Answers	86

Agenda Item: Opening Introduction - E. William Colglazier, Executive Officer and Chief Operating Officer, National Research Council

DR. COLGLAZIER: My name is William Colglazier. I'm the Executive Officer for the National Academy of Sciences and the National Research Council. I want to welcome you on behalf of the National Academies as a whole which in addition to the National Academy of Sciences and the National Research Council includes the National Academy of Engineering and the Institute of Medicine.

I think the size of the audience this morning demonstrates the intense interest in the issue of deemed export policy. And there are many stakeholders -- academia, industry, government agencies. In addition to the people in the audience this is also being Webcast, going out to a number of people who are also listening on the outside.

First, I would like to thank and express our gratitude to the Bureau of Industry and Security at the Department of Commerce for all their efforts in supporting this workshop. And I particularly want to thank Peter Lichtenbaum. He has been tireless in meeting with members of the scientific community on this issue over the last several months. And we are all very grateful to all the

discussants who have agreed on very short notice to give talks here today.

Deemed export policy, as I think all of you know, constitutes a very complicated set of issues. Everyone I'm sure agrees with the goal of preventing the export of technologies and information about things to our adversaries that threaten our national security. However, it's also clear that differences exist over the best means for achieving this goal, especially with regard to foreign nationals in the United States, and also what constitutes the most appropriate criteria for making judgments about what to protect, and how best to do so.

I think the goal this morning is to better understand differences in the details of these issues. And our goal is really to leave everyone better informed.

I would like to make one administrative note. The audio tape of today's discussions are going to be posted on the Academy's Web site under the Roundtable on Scientific Communication on National Security, and it should be up by Monday. And a transcript will also be posted later next week for any of you that are interested. For additional information please contact any of us on the staff.

Now, I would like to turn it over to our moderator this morning, Terence Murphy. There is a

detailed biography of him in the proceedings. He's eminently knowledgeable on all of these issues. One interesting fact that I learned from reading the Web site was the role he played as a junior officer at the time of the Cuban missile crisis. So, he has experience that extends over many decades.

So, I would like to turn it over to him to introduce our speaker this morning.

Agenda Item: Presentation of the IG Report -

**Moderator: Terence Murphy, Managing Editor/General Counsel
- MK Technology, Senior Associate, CSIS**

MR. MURPHY: Thank you very much, Mr. Chairman. I will make one addition to my own biography, and that is that thanks to the wonders of Patricia Wrightson, she lifted my entire biography from CSIS, with which I'm also involved, but you don't know that from that, because the CSIS headline isn't there. So, that's the job I have where I don't get paid, but it's a fairly intensive one in this issue, among others.

I'm not going to introduce Peter in any meaningful way, because you will have everything that you need really for him in your materials. And if you don't know who Peter Lichtenbaum is, you are probably in the wrong meeting. I will, however, say one thing, and that is just like I truly am with CSIS, he truly is not only the

Assistant Secretary of Commerce for Industry and Security. He is the Acting Undersecretary of Commerce for Industry and Security, and with that, he has gotten himself into a huge pickle here, because he's got this project.

I would like to make one introductory comment. I'm going to be just simply the moderator, the traffic cop here. But I do have one statement I would like to make, and it's much more persuasive coming from Harvard than it is from Terry Murphy. I'm going to quote five sentences from an article last year by the dean of the Harvard School of Public Health, Barry Bloom, in an article called, "Bioterrorism and the University." It's worth your full attention, and I'm quoting it without any change.

"There can be few higher privileges for the scientific community [this is the lead sentences] than to contribute to the security, freedom and well being of our nation, and of the people around the world. It is precisely that freedom and security that make possible the pursuit and transmission of knowledge, the fundamental mission of the university in society. Yet, we live in a world in which much of the science that can contribute to improving life for millions on the planet can also be misused by terrorists to destroy millions of lives. This paradox creates the fundamental tension under which universities and the scientific community now live. The

challenge is to insure to the extent possible, both the security of our nation, and the openness that is critical to the vitality and progress of science."

And to that I would also simply add the business would share those sentiments without any question or any qualification.

So, with that, and having got his proper title right, I'm going to turn it over to Peter Lichtenbaum and hide until the question period.

Peter.

Agenda Item: Presentation of the IG Report - Peter Lichtenbaum, Assistant Secretary of Commerce for Export Administration, US Department of Commerce

MR. LICHTENBAUM: Thank you, Terry.

It's a pleasure to be here with you today. I must say I had not been aware of your past in the Cuban missile crisis. I'm sure that everybody here would find it much more interesting to have a discussion of the Cuban missile crisis than deemed export. So, I was wondering if perhaps we could shift topics?

MR. MURPHY: I graduated from Harvard with a non-honors degree in English. And I graduated from the Navy Nuclear Weapons School at 24. Go figure.

MR. LICHTENBAUM: I saw recently, Prime Minister Blair's appearance before a rather hostile public forum.

You may have seen it. This is the one in which Blair ends up by the end of the session literally dripping in sweat, because of the various accusations that are thrown at him. And I thought to myself, gee, I have a forum coming up too, and I hope I don't end up the same way.

But I was very happy this morning to see that the prime minister had won a reelection and a Parliamentary majority. So, in any event, that story has a happy tale, and I'm sure this one will too.

Let me get down to business. This is just an overview of my remarks here today. And I do want to have as much time as possible for questions and answers. Some of this stuff that I intend to go through will be well known to some of you here in the community. I see a number of you who I know could give this talk yourselves. But I do want to make sure, given that there are some who may not have the same familiarity, that we are all on the same page, so that the focus of the discussion is really on the issues that matter, rather than perhaps on distractions or misunderstandings.

So, the first part of this will be a discussion of how our deemed export program works as briefly as possible; key issues for the research community and industry resulting from the IG's recommendations; and then what the Commerce Department has done in response to the

IG's report that was issued last spring.

The deemed export program is one part of what we do at the Commerce BIS, and that is controlling exports and re-exports of sensitive technology to countries of concern. It's a critical national security and law enforcement mission, particularly after 9/11. And we have the deemed export rule in place since 1994. So, this is an important point. It's not something that is newly being imposed.

Rather, it dates back to early in the Clinton administration, and reflects a concern that absent any kind of restriction on release of technology to foreign nationals in the United States, it would be all too possible and likely for foreign nationals from countries of concern or terrorist groups to be able to circumvent our controls on the export of technology by coming to the United States and obtaining that very same technology.

So, given the information that we have that foreign countries seek to acquire illegally controlled US technology that could be diverted to weapons programs, we have an obligation to have the deemed export program or something very similar to it in order to prevent that kind of circumvention.

At the same time, and picking up on the point from Harvard that Terry referenced, there is no question that foreign nationals play a vital role in US industry and

academia. They contribute in many ways and significantly to restraint of our industrial base, our high technology advantage, and thereby our national security.

So, it is simply not the case that national security is on one side the ledger and industrial interests and restraint of our academic sector on the other side. We are engaged in a discussion about how best to protect our national security, and we will damage our national security if we unduly shut off the participation of foreign nations in industry and in academia.

So, trying to achieve this challenging goal of protecting our national security without unduly burdening the regulated community, we have developed against since 1994, an export control program in the deemed export area. We license about 1,000 foreign nationals each year, and conduct significant outreach, and outreach that has expanded greatly in the last couple of years to the affected communities.

It is important to understand that industry, academia and the federal laboratories are required to comply with the existing rules which have been in place for a decade. In other words, the IG recommendations are not to impose a deemed export rule. We have a deemed export rule. Industry certainly has been complying with the deemed export rule for some time, and as shown by our

licensing program many universities have been as well. So, we have a program in place today, and everyone has an obligation to comply. We have an obligation to enforce the existing rules.

What are deemed exports? Our regulations define a deemed export as the release of technology or source codes subject to the EAR to a foreign national. Now, such a release is deemed to be an export to the home country of the foreign national. And situations that can involve release involve such things as tours of laboratories; foreign national employees involved in research and development; foreign students or scholars conducting research; hosting of foreign scientists.

We can't try to encompass everything that might involve the release of technology on this slide, but the ultimate question is are you releasing controlled US technology to a foreign national from a country to which that technology requires a license? Now, there are exceptions from the rules, and we'll get into those in a couple of minutes.

Here is a sequence of deemed export analysis which may be useful to proceed through. And this will be the sequence of the next few slides. We have exceptions from our rules for foreign nationals who have become US citizens, green card holders, protected immigrants. We

have other license exceptions. If those don't apply, then you classify your technology and determine whether it requires a license, and then lastly seek that license. So, let's go through those in a little more detail.

Persons exempted from the rule. So, people may be born in Iran, let's say. They may even retain citizenship in a foreign country, but they are exempt from the rules if they have attained US citizenship, or if they have even attained permanent residence in the United States; green card holders. They are also exempt -- this is also a smaller category -- if they have political refugee status, political asylum holders. But the deemed export rule does not apply to people who have obtained US citizenship or permanent residency in the United States.

Other licensing exceptions, and this quite important in assessing the burden of the current rule and any changes contemplated in response to the IG report. Publicly available information is not subject to the deemed export rule. So, if it's on the Internet, obviously it's not subject to the deemed export rule; available in libraries, et cetera.

Manuals that you can purchase at cost from the company, manuals that come with things that you can purchase from the company. So, as long as they are not proprietary, they are publicly available, and they are not

subject to our rules.

Educational information, and this is particularly important in the context of the university community. When information is released by instruction in catalogue courses, that is not subject to our rules, and there is a specific regulation that says that. Patent information and fundamental research; I will take a little more time on a couple of these.

Information resulting from fundamental research. Fundamental research is defined as basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community. Now, obviously there can be some room for interpretation there, but I think there is a fairly good general understanding of what is meant by fundamental research and research that is intended for publication.

The fundamental research exception applies by regulations to information that arises during, or results from the research. And that is in our current regulations, so we follow it, and the regulated community has to follow it when applying the scope of the fundamental research exception.

As a result, you have to be able to make the determination if you seek to rely on the fundamental

research exception, that this is indeed information that arises during or results from the research. So, there is not a blanket exception as long as you are engaged in fundamental research that any information that needs to be transferred doesn't require a license. You actually have to read the words of the regulation to be sure that you come within the exception.

Now, coming back to the pyramid here, if you have a person that is not a US citizen or permanent resident, green card holder, and none of these license exceptions apply in terms of publicly available information or fundamental research, educational instruction, then you actually have to classify your technology.

And here I would emphasize the point that most technology is not controlled, what we refer to as EAR 99 technology. That's just a term we use for basket, leftover technology that is not controlled. It may be subject to our regulations, but it is not controlled unless you are dealing with very, very small sets of foreign nationals, basically terrorist country nationals who would like to be a very small segment of students or researchers or employees.

Sensitive technologies are controlled based on specific parameters of export control classification number, ECCNs, on the Commerce controlled list. And that

Commerce controlled list is in our regulations 15 CFR Part 774. And that's important, because technology for the use of many types of controlled equipment is not controlled at all.

Some people have said, gosh, we see the definition of use technology. That's a broad definition. So, anything that meets that definition is going to be controlled. No. You have to go to the actual EECN involved and say, is there even a control on use technology? And if there is, what are the parameters of that use technology control? In other words, the use technology definition sets the outer limits of what may be controlled, but does not actually say what is controlled.

And then if you have a controlled technology, that may require licensing, depending on the foreign national's country of origin. Most deemed export licenses are for Chinese nationals, and there are really two or three countries that represent the vast majority of our deemed export license applications. I believe that China is in fact more than half of our volume, and my staff is nodding. So, this isn't really an issue as it relates to the 200 countries in the world. This is really an issue as to a very small set of foreign nationals.

And now licensing. If the transaction makes it to the bottom of that pyramid that I mentioned earlier, and

an export license is required, the good news is that the vast majority of deemed export license applications are granted. In the last fiscal year we approved 85 percent. We returned without action about 14 percent. That means that perhaps no license was required for those, so we didn't issue a license. We simply said you don't need a license. And we denied about 1 percent of the total of again, about 1,000 deemed export applications.

Most of these are processed in 45 days under an executive order, and from a practical perspective what that means to me is if you do identify a need for an export license, as long as you build that into the system for a foreign national who is coming over, whether it's as an employee or as a post-doc researcher, it is very likely licenses will be granted, and it is very likely that you will be able to get that license in time to have that foreign national start work or start research without delay.

The key point though is from a compliance standpoint, to build that into the process so that when you are seeking the visa you have this in mind, that you may also need a deemed export license.

With that whirlwind tour of deemed export controls under our belt, let's talk about the inspector general's report. Now, a very important note here, the IG

is an independent organization within the Commerce Department. It is not directly affiliated with BIS. It does not speak for BIS. We do not, have not endorsed the IG's recommendations. The suggestions made by the IG are not our proposals as they are sometimes described in the press. So, we have to be very, very careful in distinguishing between what the IG has said, and the BIS response thereto.

Now, the IG had a number of issues that they raised, but I think of principal interest to this community are a suggested clarification of controlled use technology of the country of origin; how you determine the country of origin of a foreign national. So, let's get into that.

Background regarding use technology. This is a point that is frequently misunderstood, and I don't say that to be critical, but it is perhaps not an intuitive point, and one that is easy to miss, and I have seen it repeatedly, including as recently as an article that appeared yesterday in Nature. The use of controlled equipment is not a deemed export. Deemed exports occur only if controlled use technology transfer to a foreign national.

So, it is of course quite possible that you might need to transfer a controlled technology to a foreign national in order for them to know how to use the

equipment. But the actual activity of using the equipment is not what triggers the license requirement.

The term "technology" as used in the EAR refers to specific information necessary for the development, production or use of a specific product, e.g., a computer, fermenter, a machine tool, oscilloscope, the list goes on. So, that is how we get to use technology, because if you have technology control, it may include a use technology control, depending again on the specific EECN.

Now, the current regulatory definition of use is technology for the operation, installation, maintenance, repair, overhaul and refurbishing of equipment. So, again, I've said this a couple of times, but whether the use technology is controlled in a particular situation depends on the specific technology involved as detailed by the specific EECN.

So, just because you are teaching somebody how to operate a machine tool, and that machine tool is controlled for export, doesn't mean that the technology that you are teaching that person is controlled for export. You have to look at the technology control relating to that machine tool, and determine whether there is a use technology control for machine tools, and what the scope of that use technology control is.

Now, to the IG recommendation, they recommended

that we revise the definition by replacing the word "and" with the word "or," so let's scroll back to the definition for a second. Right now, our definition says operation, installation, maintenance, repair, overhaul and refurbishing. So, some may have read this to mean that unless your use technology relates to all six of those activities, no license is required.

The IG suggested that that doesn't make a great deal of sense, because if we have a concern that operation, installation, maintenance, repair and overhaul is sensitive, a license ought to be required whether or not the person learns how to refurbish, whatever that means separately from repair of the equipment.

And so, it is in the IG's view anyway, it would essentially read use technology controls out of our regulations if you interpret "and" to mean that all six of the activities have to be met, because it is so rare that you would be transferring technology to teach all six of those activities to a foreign national, that you could essentially interpret this control away.

To deal with that, the IG suggested changing "and" to "or," so that if technology relating to any one of those activities is transferred, that at least in concept is use technology. And then you get into the question of whether in the specific technology there is a control or

not. So, we have said that we would examine that issue. We did not take a position as to whether that was correct or not.

Country of origin. The IG recommended modifying the current policy of recognizing the foreign national's most recent country of permanent residency for non-US permanent residency and citizenship, again for non-US citizens for purposes of determining deemed export licensing requirements.

The IG recommended that BIS determine country of origin based on a foreign national's place of birth. So, this revision would not apply to naturalized US citizens or foreign nationals that have achieved permanent resident status. These persons are exempt today, and would remain exempt even if we adopted the IG's recommendation.

And indeed, I think there is a quote in the IG's report that makes clear what they are talking about they talk about foreign nationals, is in fact people who are considered under the current system, as foreign nationals, rather than US citizens or green card holders. And I would be happy to get into that more in the questions and answers. I know it's an area of interest. We said we would examine that issue, taking into account whether there are any legal impediments or inappropriate policy outcomes.

So, what have done in response to the report?

Well, they urged us, and I haven't focused so far on it, to increase outreach to make sure that the existing controls are well understood. We completely agree with that, and we have increased outreach with the government laboratories and research universities where the IG particularly focused.

We will do about 100 deemed export activities during this fiscal year. Bernie Kritzer and Todd Willis, sitting in the front row there, are doing many of them. Alex Lopes as well, you may run into. And since the fall, we have done about 30 outreach activities to the academic community and government laboratories.

Very recently, last week I think, our folks went out to Stanford University, for example. We spent a couple of days out there with them. I think it was a very successful visit, and it confirmed the experience that we have had that there is a concern. And I can understand the concern that the impact of compliance with deemed export controls will be devastating for the universities.

But in fact, if you take the time to go through the sequence that I described, the impact on universities is much, much less in terms of licensing than universities fear when they are first looking at this issue. And I think I can say that was the result at Stanford. It's been the result at other universities.

Now, that does not mean that there is no cost of compliance. Clearly, there will be. But I think the cost is one of figuring out that small universe of items that requires a license, rather than a flood of licenses that will be required. So, I think universities will be able to comply if they treat this like any regulatory program. And universities, I need not tell you, are subject to a host of regulatory mandates.

We have partnered with the American Association of Universities to create a task force to address specific issues raised by the academic community. I think that has been working very well. And it's indeed under the AAU gambit if you will, that we went out to Stanford, because we agreed with the task force, that it would be very useful to do a pilot run so to speak, to get a sense of the scale of what we are talking about here, and whether the concerns are as great as they had feared.

We are also participating in a number of task forces. There is an ad hoc interagency group, which is a US government group organized by the Office of Science and Technology Policy. And that has helped us reaching out to labs. We also have the Government-University-Industry Research Roundtable or GUIRR that is organized by the folks at the National Academies here, and that also has been very helpful to us in increasing the understanding of our

controls, and hearing more about what the potential impact would be of the IG recommendations.

Finally, and in the context of this meeting, especially timely we published an advanced notice of proposed rulemaking in The Federal Register on March 28. That was basically to seek public comment on three key recommendations in the IG report: the definition of use technology, and the licensing policy for third country nationals. Those are two things we mentioned earlier. And then somewhat less significant, but still we thought we would get comment, revisions to certain questions and answers that exist in our regulations on fundamental research and government research.

So, the public comment period will last until May 27, which is 60 days from date of publication of the notice. We are seeking comments that are specific, and as much as possible are based on factual information. It is much more useful to us to have facts, than to have rhetoric or assertions, and we urge you to take the time to give us that data.

How would specifically a change in the current definition of use technology from "and" to an "or" affect the burden and quantitative estimates of licensing and compliance impacts, whether it's the number of licenses you expect would be required, the number of people you would

expect to have to hire, et cetera. It would all be very useful.

On the issue of country of origin, here are some things that we think would be useful, although we don't mean to constrain you from saying whatever you want to say. What would be the licensing impact of changing from our current approach to foreign nationals based on country of permanent residency to the foreign national's country of birth?

Would the change raise regulatory issues for the overseas operations of US industry? And how do the requirements to obtain permanent residency in other countries compare to US requirements? And to me, personally, this is an area of significant interest, because there is not a discussion of this point in the IG recommendations.

And it seems to me, a critical data point for us to have in evaluating whether we are doing the right thing in our current regulations by deferring to other countries' determinations of permanent residency. Is it meaningful when an Iranian national goes to Canada and becomes a landed immigrant in Canada, such that we should now treat that person as Canadian?

It's an important question to ask for our national security standpoint, whether there is a meaningful

review of that foreign national by the Canadians that justifies us deferring to a Canadian determination that this person is now while not a citizen, has strong ties to Canada, and is entitled to be considered as a permanent resident. So, industry and academia may have some perspectives on that. We are also trying to independently develop our own perspectives on it as well.

There is more I could say, but I think I will stop there to have to have time for questions, and here some contact points that you may wish to follow-up with in the future.

Thank you.

[Applause.]

MR. MURPHY: Thank you very much, Peter.

As the acting undersecretary, you can't leave the room until we have finished with you. I would say one other small point, and that is in addition all his many other distinctions, he's a super lawyer. And I have known Peter in that capacity since long before he was an assistant, not to say even an acting undersecretary of Commerce. So, I greatly admire him, and indeed his entire family.

I have one question, and it is not an accidental or absent-minded question. The nice thing about this business is that you do an awful lot of work for which you

are paid almost nothing. If I got a charge for every tiny bit of work that we do for CSIS and this and that and the other thing, and Ed Rice's working groups of everybody in industry, I think we would probably be paid about somewhat less than the average taxi driver on a per hour basis for the kind of work that goes into this effort.

So, the question I'm putting to you now, Peter, is not an absent-minded question. And it reflects the involvement of your own colleagues, because I know for a fact that there is a huge amount of concern about the definition of foreign nationals in the business community. I can't speak for universities, but I certainly know the business community is very, very concerned about that.

And with that in mind, I'm going to ask you a question, and I think I know what the answer will be. But I would like it to come out, and I know that you would like it to come out. Here is the question. In The Federal Register notice of proposed rulemaking on March 28, the BIS has requested public comment on the inspector general's recommendation for covering foreign nationals under the deemed export controls. You have asked for as much specific detail as possible.

But to respond to the BIS request, industry and academia need to know what is within the scope of the term "foreign national." Some interpret The Federal Register

notice as suggesting that the IG is concerned with deemed exports to naturalized US citizens and permanent residents of the United States, i.e., green card holders and some others, as well as permanent residents and citizens of foreign countries. Is that correct?

Specifically, should industry and academia assume that "foreign national" would include green card holders for purposes of the BIS notice? What other categories would included in that term? We finished this at ten o'clock last night.

MR. LICHTENBAUM: Well, thank you for the question, Terry. I apologize if this has the flavor of staged colloquy.

MR. MURPHY: It certainly does.

MR. LICHTENBAUM: But you are correct, that The Federal Register is concerned with permanent residents and citizens of third countries, e.g., an Iranian national who established permanent residency or citizenship in Canada. A naturalized US citizen, somebody born aboard for example, who has become a US citizen or a permanent resident, i.e., green card holder or a protected individual would not be a foreign national for purposes of The Federal Register notice.

And further, I believe that is consistent with the IG's recommendations and their understanding of what

they are recommending that we do. If I may read from the IG report, they state that in its written response to our draft report, NIST -- which is of course part of the Commerce Department -- took issue with our recommendation for BIS to amend its policy to require US entities to apply for a deemed export license for foreign national employees or visitors with access to dual use technology if they were born in a country where the technology transfer in question is EAR controlled.

Specifically, it stated that our recommendation could be interpreted to include naturalized citizens of the US, particularly those who were born in a sensitive country. However, if a foreign national becomes a naturalized citizen of the United States, they are no longer considered a foreign national, but rather a US citizen, and the EAR controls involving the transfer of technology to such an individual no longer apply.

So, I think the IG is fairly clear in its rejection of the NIST concern. And I have had my own conversations with the IG that this recommendation does not relate to people who have become US citizen or green card holders. Rather, the question is assuming that somebody is not considered as a US person, what is the correct foreign country of origin of that foreign national?

So, I hope that is responsive.

MR. MURPHY: It's certainly a great reassurance to me as the faithful, dutiful son-in-law of Doreen Tooley Sherman, who after a mere 57 years on these shores from Australia, became a United States citizen two years ago. And she is living in an assisted living environment, but she can now not worry about the long arm of the law reaching out to her.

I think we should open to the floor. This chair will exercise one prerogative, and that is to prefer -- we have half an hour, so I think there is time for a lot of people -- but we are going to prefer questions from the universities and academic communities. We have undoubtedly lots of time for the business community. The business community is here. It's very active, and it will have lots of access to this issue.

But that doesn't mean nobody can speak. I just want to say what we will do. Now, if people will raise their hands or come to the mike, and do whatever you want to do, please state who you are, otherwise the chair can't do what I just said I wanted to do.

Yes?

DR. ALBERTS: I'm Bruce Alberts, the president of the Academy, but I count myself as a university person. I'm going back in two months. So, I get to ask a question, I guess.

I'm not clear what rights you have. You have rights with regard to the law to add the "and" I'm sure, remove the "or." You have the right also to remove the word "operation," because that would solve, it seems to me, a lot of the problem. In other words, if you add the "and" and you take out "operation."

MR. LICHTENBAUM: We do have the legal right to modify our regulations, as long as we act consistently with the statute. I don't want to sit here and give myself legal advice, but since I am no longer active as a lawyer, I don't think that could create a statutory issue for us, which would be the constraint on us modifying our regulations.

Of course, our regulations do receive interagency clearance, and so, any regulatory change would go through the normal OMB process. But we do have the right, if we can get a regulation cleared, to modify the regulation as you suggest, by removing the word "operation."

MR. MURPHY: This is Bill Root. I'll introduce him myself. He is an esteemed colleague on the Commerce Department's Advisory Committee on Regulatory Issues. I happen to be on it, as does Cynthia Johnson, who is going to be heard from later. We're among the people who don't get paid much for this kind of work. But Bill Root knows a huge amount, ladies and gentlemen, about this subject,

going back to his State Department days.

So, whatever flag you want to fly, Bill, go ahead.

MR. ROOT: I can shed a little light on excluding "operate." Most technology, as you pointed out, is not a controlled option. Use technology in particular is not included in the controlled as seven of the nine categories for the items, which is most of the list. The eighth one, which is telecommunications operations, are explicitly excluded.

But even where use technology is controlled, there is one factor which you omitted from your Power Point slide, which I think is terribly relevant, and that is it's controlled only in accordance with a general technology known. And the principal factor in that know is the word "required," which doesn't mean anything until it is defined.

But is defined, and it is defined in a very specific sense. It must be materially responsible for achieving or exceeding the embargo specifications, and operation technology of course will not do that.

Refurbishing might, which is why of the six categories one or two might be applicable of use category. But certainly operating, I cannot conceive of a situation where operating technology could be construed as "required."

MR. LICHTENBAUM: Well, I'm not sure if there was a question there, but I do appreciate Mr. Root sharing the benefits of his long and outstanding experience in this field.

MR. MURPHY: Have we taken all the fun out of this by the colloquy? Okay, Toby Smith of AAU.

MR. T. SMITH: Toby Smith with the American Association of Universities.

First, I want to BIS. We have been working with you all in trying to come to some reasonable interpretation of the regulations, so we appreciate that. After having heard these presentations several times, I have come to a conclusion though. I think it's probably in my mind -- this is maybe not my role as AAU, but as a citizen, what concerns me.

The ambiguities, to understand this, and I'm starting to understand it finally in the sense of what we mean by use technology, but we'll get some clarification. But the ambiguities and imprecision in the regulations themselves, my concern is that they in and of themselves, because we are not being as precise in our language as we really need to be, cause us a national security risk.

And what do I mean? I think a lot of universities want to -- as universities, we want to understand the importance of national security. But if we

cannot understand the regulations, then we are not going to solve the problem we are trying to solve. In the end, it's going to be the faculty who are on the front line, who are trying to deal with this.

And if it takes 10 meetings for me to start to understand what we are really talking about, the average faculty member, even despite that we are putting in place education programs trying to get them up to speed on what their responsibilities are with regard to export controls, will never understand this, and therefore it will be from the point of really trying to improve national security, not positive.

So, there are a few things, and we are starting to work on our comments. I guess I have a whole host of questions, but one is I understand that -- and you said it, Peter, that if publicly available, if it's not proprietary, does that mean it's publicly available? In other words, is the opposite of publicly available in the regulations proprietary?

That would make a huge difference, but it's got to be spelled out in the regulations. I have read the questions and answers. It implies that proprietary information is that which is not publicly available. So, I guess that would be the first question. Is that an accurate interpretation? Is there somewhere in the

regulations themselves that say what we really mean by publicly available is that information which is not proprietary?

MR. LICHTENBAUM: Well, let me take the question and comment in reverse order. On the question you just asked, Toby, I think it is true to say that if it proprietary, then it is not publicly available. I think I could imagine a situation when something was not proprietary, but was not publicly available, because it was not readily available to people to obtain.

In other words, other people have to be able to see it too. And even if it's not subject to some type of legal restriction, of it's not as a practical matter, available to the public, then --

MR. T. SMITH: I guess what concerns me is give me a specific example of such a situation. Because that ambiguity is exactly what I'm concerned about. That's where it gets really hard for us to make the decisions. And if it's left to us to decide, and there is not precision on the government from your side in terms of what it really is, then I get worried.

MR. LICHTENBAUM: I do have to I guess disagree there that there is a definition of publicly available in our regulations. It is quite specific as to the activities that create public availability. There are questions and

answers in our regulations. So, I think we have explained in fairly good detail actually what it means, and how you get something to be publicly available.

In addition, people are of course free to submit advisory opinion requests if they have a particular situation that they are concerned about. And I would urge you, if you think that there is a question and answer that would be helpful, then pose that question and your proposed answer in your comments to the IG report, because we would be more than happy to add additional questions and answers if there is a particular area that isn't sufficiently clear.

MR. T. SMITH: Just a comment on that. My only concern is ultimately you are responsible for complying with the regulations, not the questions and answers. So, I don't think it's enough to answer these questions in questions and answered. They need to be defined in regulatory language. And I am concerned that the definition of public available, at least from our vantage point, is not very clear.

And while we are told what we really care about is proprietary information, the regulations don't support us. If we were to base our decisions on that, I think we would be really on shaky ground based upon the definitions in the regulations. And again, it makes it very hard to

insure absolute compliance, which forces us into a position where we will have to go the extra nth to insure compliance will be conservative, which will cause some of the problems and the fears that I think all of us are worried about.

So, I would just urge that it not be questions and answers. That questions and answers are not enough. We have just gone through this with the questions and answers that says if I have a foreign national working on certain research, do I have to apply for a license? And that question and answer never said anything about equipment, yet all the sudden we are told no, we have always meant equipment. Equipment has always been a concern, it's just not in the questions and answers. So, I just say let's really work on the precision of the regulations.

I don't want to consume all the time. Probably other people have questions. But the other thing I want to talk about is the regulatory burden. I do think based upon our discussions, there is probably a very limited set of licenses that are required. However, the big concern is for the volume of equipment that we have on campuses, which is a huge amount, we now have to make sure we now the EECN numbers of every piece of equipment.

We need to make sure that we know -- and the bottom line is, and if you know and understand what

happened at Stanford, the T6 countries, the embargoed countries are still a question. In a lot of instances you will be required to have licenses for those students. And we do have Iranian students. We do have Iraqi students on our campuses working in some of these labs.

You still have to go through that burdensome process to get there. For people in the academic community, EECN numbers don't -- controlled technologies don't come with EECN numbers attached. You have to go and classify every one of these pieces of equipment, and that is a huge burden.

I think the administrative burden is a real problem even if at the end of the day there are very few licenses. And in terms of costs and regulatory issues on campus, it will be a tremendous burden to get there, and the question is, is the real security threat that we are trying to solve worth that cost in the end of the day? And I think we are all willing to comply. We'll do it, but it raises a real question.

MR. LICHTENBAUM: Toby, you raise important issues for us. Let me respond briefly to that, and then we can go to other questions. On the question of costs and benefits here, and what is the national security case for these, let me just say that we are asking those questions as well. We are of course not an agency that can solely

make that judgment. We do so in coordination with other agencies.

But we are actively seeking and expect to have in the very near future, and before any actions are taken, an up-to-date assessment of what the national security concerns are related to foreign nationals seeking information in the United States, and with particular relevance to the university community. And that is, I think, a very important thing for us to do, so that we don't take action in a void.

Again, I think this is something that was not actually done by the inspector general. The inspector general presumed that a problem exists, but did not go out and talk to the intelligence community or the national security community. I have confirmed that with the inspector general. So, we need to do that work in order to assess the current nature of this problem.

I would say that I would love to be able to simplify the regulatory structure as much as possible to your earlier point, Toby. But the problem is that it is a complex area. And simplification might mean that we either fail to protect our national security, or impose excessive burden on our industry and academic community.

And so, ultimately the controls are as they relate to specific technologies. And if we try to

oversimplify perhaps, I am concerned, though I would welcome suggestions of how to do this in the comments, that we run the risk of jeopardizing our national security, or imposing too great a burden on the regulated community.

So, with that, let me call for other questions.

MR. MURPHY: If the chair can just help a little tiny bit. And that is back to the publicly available. I quoted Harvard. I'll quote myself from memory. Once upon a time I wrote an opinion as to what not public availability was, and it included among other things scientific meeting, engineering meetings where you have to come in and pay money, and basically be accepted in to the society of engineers or whoever is discussing whatever the subject is. That subject, though it may be freely shared within the group, is not publicly available under at least Murphy's opinion some years ago. That doesn't make it true, but that might be helpful.

On questions and answers, I would say again from experience that the questions and answers in the -- any boycott regulations of the Commerce Department on what is controlled in fact for a corporation are extremely helpful, and they are used widely across the government and the business community having nothing to do with any boycott if people are trying to figure out if a corporation is controlled or isn't controlled.

So, some of those questions and answers can be helpful. I'm not commenting on this one, but the technique is actually potentially useful. And OFAC, the Office of Foreign Assets Control, is using questions and answers. The legal profession is critiquing questions and answers, as you know very well from our own previous work together. So, questions and answers can be improved, and always should be improved, but they are not necessarily wrong.

So, having said I wouldn't be involved, I just got involved. But I think we have intimidated the business community. But since they are all here, here is Eric Hirschhorn. He has been very polite, and he is an extraordinarily knowledgeable lawyer, and a highly respected member of all kinds of different communities.

So, Eric.

MR. HIRSCHHORN: Thank you, Terry. You don't have to pay back that loan.

MR. MURPHY: He and I once argued a case to the Supreme Court together and we won it, or at least we prepared it. So, he's a good guy.

MR. HIRSCHHORN: Thanks.

I think when we look just at the March 28th notice, and one can compare it to someone saying I'm just going to make a little cut here on your hands. And it will bleed a little bit, but you will be able clean it up, and

it will heal fine, and you won't even remember it.

I think the broader concern, and one that so far has not been addressed here, and perhaps it's a little unfair to ask you as one individual in the government to address it is the death of a thousand cuts. Is the tightened visa policies that have lead to a drastic reduction in the number of foreign engineers coming here to study and ultimately to work. Bill Gates can't even find engineers, and that's a pretty attractive place to work I think.

It's also the widespread rumors that there is a lot more going on under the surface here than what's in the March 28th notice, coming from usually reliable government sources, that there is really much more of an effort going on at various levels in other agencies and in the White House to reach into the green card area.

I have always thought that the strength of this country can from encouraging smart people to come here, and not trying to convince them that they ought to go elsewhere if they want to work freely. And that our strength has come from keeping our research and development here, and not convincing multi-national companies to do it offshore instead, which is what we are definitely beginning to see as a result of these policies.

And I concede that it's broader than the subject

matter of this session, but you are certainly someone who is very thoughtful and very knowledgeable, and I would be very interested in your reflections on this.

MR. LICHTENBAUM: Well, Eric, you don't have to pay back your loan to me.

But certainly from the standpoint of the regulated community, which has to cope not just with our regulations, but also with visa issues and other issues, I understand the death of a thousand cuts metaphor. We, I think though, have to deal with the issues that we have, while also looking at them in the broader context, and not shy away from doing the right thing in a particular area because of impacts that are happening in other areas.

Now, that is not to say we shouldn't take those into account, but ultimately if there is a correct policy in this area, I think we ought to try to find it, and not say well, we're going to offset here, taken as a hypothetical that visa policy is too restrictive, a subject on which I'm not qualified to comment. And say well, because visa policy is too restrictive, we are going to have a more lenient deemed export policy than we would otherwise have.

I think the remedy if indeed the visa policy is too restrictive, is to fix the visa policy. But we ought to play deemed export policy to try to achieve the right

solution for our national security. Whether we are doing that, as the discussion makes clear, there can be a variety of views on how best to do that, but I am certainly trying to do that.

As to rumors that I know are current in the community -- it's the Washington community, for those of you who are not from here, thrives on such rumors -- I can't really comment. We do not have any good information regarding any initiatives of the kind that you described. Initiatives to strengthen deemed exports controls would ultimately come to my desk, as they are my rules. So, if there are any such initiatives, they are certainly a fair ways down the pipeline.

MS. BODEN: My name is Ann Boden. I'm from the University of Maryland.

As a follow-up to what Toby Smith had said, I don't think the universities have an issue with licensing so much as making all of the efforts to find out whether the equipment we have is controlled. At Maryland we have done a very rough estimate of the cost to classify all the equipment in our labs based on the number of labs we have, and a rough estimate of the number of pieces of equipment in all of those labs.

We have extrapolated that, asked for bids from companies, estimates from companies. A conservative

estimate to categorize all of the equipment going through the ECCNs, determining whether there is control on use technology for each of those is \$1.5 million. Now, that's a commercial cost.

Certainly, it would be much cheaper for university employees to do that, but it would take an entirely new department of many, many people to accomplish what outside companies already do as a matter of business.

MR. LICHTENBAUM: Well, that's certainly the type of information that we are seeking in The Federal Register notice, is an assessment of the burden. It would be interesting to me to understand as well, to what extent that estimate reflects the marginal cost, if you will, of complying with the rules as the IG has recommended they be changed versus the cost of complying with the existing rules which are in effect today.

But certainly, we would be very interested in any information of that kind. We would be more than happy as well to visit with you to see if perhaps there are ways in which that compliance burden can be mitigated. But we are certainly very interested in receiving that information.

MR. BONHURST(?): Hi, I'm Mark Bonhurst from the University of Minnesota.

I think I'm going to repeat a theme you have been hearing, but it is very difficult for us to figure out how

to go forward when we do not know what the rules are in terms of what equipment might or might not require licenses. At this point our understanding is that people who sell us or loan us equipment for our research labs know that they are sending that equipment into an open research environment.

Our purchasing department doesn't know of any equipment we have received that has any restrictions about manuals or blueprints or use information. I don't know of any restricted equipment that we have in our campus.

The IG's report called out fermenter technology. So, the first thing I did was talk to our fermenter folks, and fold the editor and chief of the five volume encyclopedia of fermenter technology, which is updated on the Web. He said there is no way there is anything about fermenter technology that we are teaching, or that other universities are teaching that is not already widely known.

So, the only way that I can see to manage this is to say if we are getting -- the regulations already say if you are doing fundamental research, you are getting confidential information from the sponsor, obviously that information is not in the public domain and is subject to export controls.

Well, if we have got a vendor or somebody who is loaning us equipment, and they tell us that there are

restrictions about use of the equipment, then okay, that's a nice way for us to know that that equipment is subject to export controls. But otherwise, I think it's a very reasonable presumption that the equipment we have is not subject to controls.

That the people who run those labs could take all the information they know about how to use the equipment, put it on the Web, put it in the university library. There is no restriction on their ability to do that from the vendors anyway.

So, why should we go to the expense of spending millions of dollars trying to classify thousands and thousands of pieces of equipment, when we have no reason to believe that any of that equipment is restricted. And indeed, no reason to believe that Iranians shouldn't be able to use it?

MR. LICHTENBAUM: I think all those are excellent points, Mark. As a former counsel to companies, you've got to focus on what the highest risks are. And if you think that there are whole areas of your technology that are very unlikely to be subject to control, I question whether it makes sense to invest resources in classifying every single piece of equipment that's in a lab in order to determine whether technology related to equipment -- you have the ability to self-classify.

Part of that ability to self-classify is the ability to say it's extraordinarily unlikely that equipment in this lab is going to be controlled. And I'm not going to categorize all that equipment, because it's so unlikely. I know the types of things they have there. It's fermenters. It's whatever, and I am confident that the type of equipment based on talking to the guy who runs that lab, that technology is publicly available on the Web.

There is no need to go through a bureaucratic process of saying that we have to have a chart that says every single piece of equipment that we own, here is the technology, and here is where it's classified. I would really try to focus, to triage on what is the most sensitive technology that you have in your community, and let's classify that.

Even the best companies in America, with the strongest commitments to export compliance, and we have some of them there, Intel let's say, they make judgments about how to spend their compliance resources, and they focus on what matters. They don't try to have a 100 percent thing that would cost them \$1 million a year or whatever it is to be classifying each piece of technology that they have anywhere in the company.

MR. MURPHY: We are near the witching hour. I have to say that with long experience chairing conferences

in Europe particularly, the chair is usually graded on two things, one, general contribution, which is usually minimal, and time keeping, where the grading is merciless. And so, we have to watch our time.

MR. R. JOHNSON: Peter, a quick question. There is the IG report for Commerce. But obviously there is the interagency report, which also touches on Commerce programs, and in some respects has some recommendations and concerns that go beyond the specific ones in the IG report for Commerce. I just want to ask about the process. Is there an obligation for Commerce to be responding on the interagency concerns, or is it going to be limited to the Commerce IG report?

MR. LICHTENBAUM: Well, I think that the interagency report largely as to Commerce, reflects the conclusions of the Commerce IG report. But we will certainly respond to the interagency report as well. And so, if there is anything in there that you believe is important to comment on, that is not contained in the Commerce Department report, we would certainly like to get your thoughts on that as well.

MR. MURPHY: Is there anybody else? We are going to break into the coffee break, which is probably vastly more important than any subject we discussed this morning. But one last, yes?

MS. MILLER: I'm Judy Miller at Williams & Connolly. I'm also a trustee of a college, so I sort of am a Washington lawyer, but I'm also someone who cares about the academic part.

As I watched your presentation, Peter, the sort of pyramid of going from EAR 99, which although not controlled, is in fact subject to, so it means practically the technology out there really is subject to your regulations. And to get down to 900 licenses, applications seems extraordinary to me in terms of the amount of burden that I think people have already commented on for the academic community, and even for the industrial community.

I wonder whether there -- this is probably too way out there to suggest -- I wonder if there is any possibility of thinking about re-organizing how the fundamental analysis of the EAR regulations are applied, starting always with EAR 99 subject to and marching through, down to whether or not you've got an alien who is a problem.

As opposed to perhaps starting with do we have the foreign nationals here who are actually at issue, and then working back that way. Would that make any difference do you think in the compliance burden you are putting on all of these universities?

MR. LICHTENBAUM: Well, it's not for me to write

the universities' expert compliance programs. It is certainly an alternative way that a university could proceed to say, look, the vast majority of potential deemed export licenses as the Commerce Department has told us, relate to Chinese nationals and a few other countries. I think I would put Russia, India and the T7, which is now probably a little smaller than T7. It's certainly less than 10 countries that you are talking about as the likely areas of deemed export licensing.

And a reasonable approach might be to start from where do I have those individuals in my research community, and what do they have access to? That's another way to go about this, rather than again classifying everything that is on campus, or large parts of the things that are on campus, given that such people may not have access to that technology in the first place.

So, everybody has to access which way is easier for them. The end goal is to focus on what's most important in terms of nationals from countries of concern having access to technology that is of significant concern. And how you get there really depends on your own individual circumstances.

MS. MILLER: I'm just making a suggestion that the risk balance that Commerce has drawn for a long time might in fact be looked at differently for an overall

reappraisal of your regulations. That could work too, that's all I'm suggesting.

MR. LICHTENBAUM: Thank you.

MR. MURPHY: If the chair, under the ferocious guidance of the clock can now bring this to a conclusion. I would tell you one thing. Some of us have been members of large law firms which almost defines ungovernability. But universities must be that cubed.

But having said that, one particular university that I happen to know pretty well has the best analytical talent for this issue that I have seen anywhere. I won't mention it. It would be indiscrete. I also am conscious of the camera pointing at us, and my colleagues at that university are watching and listening.

But the individual in question has done the best piece of written analysis of an export control that I have seen in my professional career. So, I don't think it's beyond the intellectual powers of our colleagues in universities to do these issues.

I think with that, unless you want to refute everything that has been said, Peter --

MR. LICHTENBAUM: I can agree with that.

MR. MURPHY: Peter will be back on the next panel. I will not, because I have tried genuinely to be neutral, and I hope everyone has now been heard, and feels

that we have had a good exchange. I certainly welcome the chance to have been with you this morning.

We are adjourned for the coffee hour.

[Applause.]

[Brief recess.]

Agenda Item: Discussant Panel - Moderator: John Hamre, President, Center for Strategic and International Studies

DR. HAMRE: My name is John Hamre. I'm the President, CEO over at CSIS, the Center for Strategic and International Studies. I was asked to come over to moderate this session, because I have been working in and out, and on and off on issues of exports controls, both when I was at DoD, I was the deputy secretary of defense at DoD, and since I have gone to CSIS. And then we have been partnering with the National Academy on a series of issues like this, so, they roped me in.

So, my goal here is to move an impossible panel through the morning, because we've got very, very fine presenters, all of whom have a lot to say and we only have two hours to get this done. And I'll tell you right now, we are probably not going to do the break. We just aren't going to have time for it.

So, in order for you to hear what they have to say, each one is going to get 10 minutes, and I am going to

be the schedule Nazi to make sure we really will stay on the 10 minutes, because with five presenters, we are going to consume a lot of our time in this, and so we are going to have to move that along. And then we will open it up for discussion with all of you.

It seems to me that there are three questions we've got ask any time the government wants to impose itself on the private sector. The first question is what's the problem we are trying to fix? Second is does the fix they are offering solve the problem? And the third question is are the consequences of it less than the benefits you get from the fix, or is it the other way around? That's what all of government is about when you get right down to it.

But just to editorialize, what we have with deemed exports is a theoretical problem that is politically defined in particulars. And in a paranoid national security environment after 9/11, the particulars are all that matter to the government, because that is what you are going to get criticized for.

But we are proposing fairly sweeping regulations that set us on a path. And you have to ask yourself, is this a problem that you are really fixing with this? If the goal is to stop industrial espionage, is this a fix? And is that really the goal? What is the goal we are

really trying to fix?

And with all due respect, I apologize I wasn't here to hear you, Peter, to say that you have a regulation where 99.9 percent of the people pass it doesn't strike me as being a very effective policy tool. Either you have misdefined the problem, or we have completely made it an implausible solution to the problem. It's got to be one of the two if 99.9 percent of the people pass in 45 days.

So, we've got to think about these three questions. What's the problem that we are trying to fix? Does this solution really fix anything? And are the consequences in scale to the problem that we fixed?

Okay, so let's go. I'm not going to read the introductions. You've all got that in front of you. Take a look to see who these fine people are, because we just don't have the time.

Cynthia, I think we're going to start with you, because you've got a Power Point. The other colleagues are going to be doing it more verbally, and so, then we'll take the machine down. But I would like to start with you, and then we'll go back to the regular order as printed in the brochure.

**Agenda Item: Discussant Panel - Cynthia Johnson,
Director of Government Relations, Texas Instruments**

MS. JOHNSON: Thank you.

I just want to start by thanking the National Academies for having this workshop today, and for the SIA on whose behalf I am appearing, the Semiconductor Industry Association. I also want to thank and recognize the Bureau of Industry and Security representatives who are here today. We do work with these individuals sometimes on a daily basis. They are administering a very complex set of regulations, and we appreciate their hard work. So, nothing I have to say today is meant to disparage any way the fine work that is being done by the BIS on this topic.

And I also wanted to address something from the previous panel. My presentation does address the US permanent residents green card holders. The reason we did include it is because there are some ambiguous comments in the IG's report that we think could implicate green card holders. And there seems to be some direction to the BIS to work with Congress and some other agencies to take a look at that category of individuals. We have quite a few permanent residents working for my company, and in the semiconductor industry. And so, we feel that that's important to address.

And finally, before I get into the Power Point, I did also want to say that what we see when we face this issue is technology, and the technology that we are dealing with is global. It is not limited to the United States.

It is not made only in the USA. There are centers of excellence in many of our competitor countries, in Europe, even in China and other places, India certainly. So, we are not talking about technology that is resident within the United States, and the control of which can be accomplished by just keeping it in the United States.

Secondly, we are talking about a rule that is applicable only to US companies in its current form. Other countries do control technology, but as far as I'm aware -- I'm sure I might be corrected by many of the very distinguished people in this room -- but as far as I know, we are the only country that has such a rule, so it is a unilateral control that only US companies have to comply with, and to the university community, welcome to your new world.

And thirdly, for those of us who are compliant, and that includes many of the companies in this room, we are also aware, and I think the IG's report underscores that there are many, many companies in the United States that are not complying with the deemed export rule either because they are not aware, they don't have resources, they don't know how to classify their products or so on.

So, you are ratcheting down to a very small number of companies that are actually trying to wrestle with -- I shouldn't say a small number, but you are actually dealing

with a limited universe of companies that are trying to adhere to this.

Of the companies that are trying to adhere to this, you are filing license applications. And what happens to those license applications is addressed in the IG's report. Again, there are name checks that are done by the FBI, but in the IG's report it also indicates that the CIA is reluctant to do these name checks anymore, and they are providing information to BIS to do the name checks, but they themselves do not see a value in continuing with this practice. So, I think that kind of underscores the questions as to what kind of national security purposes we are achieving with this rule.

As has already been pointed out, we have an existing rule. We do try to comply with the existing rule. But the kinds of things that have been suggested in the IG's report in terms of extending the research of the deemed export rule seem very, very egregious indeed when you look at the fact that there are some fundamental questions with the way the rule is existing today.

So, with that, I'll try to get through these as quickly as possible. This is just an introductory slide on the semiconductor industry. There are over 101 members; 85 percent are in the United States. Our global revenue was \$213 billion. The majority of our research and development

and production does occur in the United States, but as I mentioned before, the industry as a whole is global and China is one of the biggest and fastest growing markets in the world today.

We exist, as I mentioned before, in a very competitive environment. SIA companies compete in global markets for market share certainly, but also for scientific and engineering talent, and I will get into this a little bit later in some of the other slides. Today, over 50 percent of graduate level engineering students are not US citizens.

And when you look at levels like PhD candidates, you are talking about I think it is percentages exceeding 60 percent are not US citizens. Now, not all of those people are going to be from prohibited countries, but you are talking about a very diverse population from which we have to draw for our human resources.

We learned from other debates in immigration, the H1B debate, the cutting off or curtailing our access to talent, drives people overseas to overseas competitors, and will blunt our competitive edge. As a company and across our industry, our people are our most important asset. And not only do we have to attract these people, but we have to retain them when we get them inside the door of our companies.

And that brings into question the kinds of work opportunities they have. And one thing that hasn't been addressed yet is that the conditions on the deemed export license can sometimes limit the opportunities of some of your best people when you are bringing them in. Even if they had skills in the university setting, when they come to your company they may be subject to conditions which would limit their ability to implement those skills when they come to your company, and that doesn't seem to make a lot of sense to us.

Finally, this rule conflicts with our efforts to create strong and diverse teams to solve all these difficult engineering challenges that we face.

This is just a slide of our sales, most of which are outside the United States, as you can see; 77 percent of our capacity is still in the United States, although there are a lot of pressures to go overseas. And 55 percent of our employment base is in North America.

These two slides are just to show the kind of competitive pressures that are under. I have already mentioned right now US companies are the leaders in the semiconductor industry with 47 percent. But our competitors, as I said, are found all over the world, and they are in some cases, gaining ground.

As I mentioned in my beginning comments, some of

these companies are not subject to the same restrictions we are. And the deemed export rule is just one example. There are others in which only US companies are subject to these kinds of controls.

When you look at the pool of talent that we have draw from when we are trying to staff our companies, you can see by this bar chart that numerically many of these promising, bright individuals are coming from restricted countries. They are coming from China. They are coming from India and from other places. So, the trend lines are that we are going to have to continue to look to some of these sources for our engineering talent. And that brings of course in direct conflict again with controls in this area.

This is another slide showing the percentage of engineering graduates. Most of the companies that I'm representing today of course do try to employ engineers.

So, a little bit of this has been covered by Peter, and I will not try and be too repetitive here, but the index rule does date back to 1994. Previous to that time, the rule was an export would be deemed to have occurred if there was a showing of knowledge or intent that the data was going to be shipped out of the country.

So, there was a rebuttal presumption prior to 1994, that the foreign national would export controlled

technology. However, you could overcome that presumption if companies took measures to protect against such illegal exports. And all the companies sitting in the room today, and many of our other colleagues were taking such measures.

However, in 1994 it was deemed necessary to have a clarification. And so there was a legal fiction created, which is the counterintuitive concept of deemed export, an export that can occur on US soil, even though it doesn't seem like that might be possible if you just approach it from a common sense point of view.

I've mentioned some of these things before but we feel that this rule has left us with an unlevel playing field, it does ignore other measures against unauthorized transfers. But I think the main factor for us is that for some of our brightest engineers this cuts against our hiring, our retention, and the teamwork that's required for our companies to excel. And I'll get to two, okay, the two recommendations, if I could just go over these briefly and I'll conclude after that.

On the country of birth recommendation, before I get into the points here, I did want to mention that, and again I ask to be corrected if I'm wrong on this but the way that the recommendation is couched or the way it's phrased in the IG's report would make this particular control for dual use items more restrictive than the ITAR

controls for military items. Because in ITAR it is required that you look at the most restrictive country of citizenship in the case of dual citizenship but it does not require that you go all the way back to country of birth. I'd ask for further discussion on this but I again ask does it make any sense to have a more restrictive rule for dual use items then it does for military items, and I assume it possibly does not.

We talked about compliance burden and many of the universities have spoken to this point very well so let me just go on to the next point.

We do include U.S. permanent residents and we hope to include this in our comments. The main point here and since I'm running short of time I'm just going to shorthand this, when I asked within my company about the possibility of this applying to U.S. permanent residents the main concern here is that many of these, we and many of our colleagues in industry try and retain these people so one of the things we do is help work through establishing permanent residence for these individuals. We do that because we want them to stay, we want them to be a contributing part of our team, and if they're not going to stay here and work for us they're going to work for our competitors.

If you applied this today to our workforce you

would end up submitting to license some of the technology drivers within our company and I think we are not unique in that respect. So we're talking long term committed individuals who are high, high contributors to our technology edge that would be subjected to licensing conditions which are somewhat unpredictable and would restrain their ability to continue to contribute to our workforce. So we see this as a very, very serious issue and we look forward to being able to comment on this more fully later.

Thank you.

DR. HAMRE: Cynthia Johnson, thank you very much, very good way to get us started. Let me turn now to President Dan Mote, University of Maryland, done a fabulous job with the university, we're delighted he can join us this morning.

Agenda Item: Discussant Panel - Dr. C.D. Mote, University of Maryland

DR. MOTE: Well, John, thank you very much and I will try to not be repetitive and stick to my time of course.

Deemed expert control regulations of course effects security, economic and scientific leaderships of our nation, it is really essential that we get the balance among them right. Just as an example, feeding off the

discussion this morning, on a federal funded research project we had recently meteorologists wanted to send 12 pieces of equipment overseas to measure the incoming ultraviolet radiation. And although it ultimately did not require getting a license for those equipment, in other words it fell into the 14 percent category that was mentioned this morning of equipment that did not require a license, it did take 90 hours of attorney and faculty clock time and six months to get the conclusion that a license was not required. This is an example of even if you don't have a license this is an expensive and time consuming process.

Over 50 percent of the university engineering faculty at Maryland, plus the dean, are foreign born. 52 percent of the engineering graduate students at Maryland are foreign born. 45 percent of the graduate students in science at Maryland are foreign born, plus the deans. So you begin to get a picture of what the impact of restriction on equipment is going to be at a university. And oh by the way, 57 percent of the nation's postdocs in science and technology are foreign born. So this is not a small issue and this is not an issue of add on technology strength to our economy and our security, this is a central issue, our nation depends on these people.

I find myself deeply concerned with this topic

and I have been working on this with Peter actually for over a year on this, and I really, I have three concerns and five recommendations that I'd like to buzz through in my ten minutes. We have a handout if anybody is interested in more information.

The first concern, what is the real problem and one of the real costs of this deemed export licensing. I do not have one example of a grad student in mind at the University of Maryland or anywhere else who has undermined national security through operation of a sensitive piece of equipment let alone the scale of violations that would raise the threat to such a level that we would risk suppressing our technology future to try to suppress it. And I was also interested to hear this morning that the Inspector Generals did not have one either.

Even though the IG report has proposed that operation of export controlled equipment will require a deemed export license for some foreign nationals it has been offered that not all operations of equipment may require license as we heard this morning. Some users may not require a license if information garnered by the user is already in the public domain, whatever that actually turns out to be. This would vary with each piece of equipment of course, each foreign user from a particular country, and it would likely vary from time to time as

well. How will institutions that want to avoid violations of deemed export regulations cope with the vagaries of this policy? Of course they won't very well.

If you're not confused by all of this you're just not thinking about it hard enough.

[Laughter.]

Subcontracts of course to universities from industry will also be very, very cautious as we are seeing already by the way, thereby limiting the use of export controlled equipment by foreign nationals. The mantra will be when in doubt apply for a license and of course that will be most of the time and if no one thinks that's not, if anybody thinks that's not going to be the structure they're also not thinking about it hard enough.

So what is the outcome of, my second concern is what are the outcome of compliances with deemed export licensing. Well, on the federal side of course they'll be a burden of licensing and updating lists of controlled equipment that reflect all the new technologies, not only those that we currently know about but all those that show up weekly in Science, Nature, and professional journals, I mean that's really the new stuff after all.

The federal laboratories of course have hundreds of foreign postdocs working with and around state of the art equipment, as do commercial enterprises and 3500 U.S.

universities and colleges and technical training facilities. It is really reasonable to question whether such a system could ever work well as a matter of fact, and that is well meaning, without either bringing the work to a halt or most likely suppressing international participation in the U.S. research enterprise.

The greatest problem for universities are one, the disruption of the research programs and two, the ultimate loss of access to the international scholar talent pool. Universities cannot run research programs where a two to three month delay is necessary because of certain requirements like to categorize each piece of equipment under EAR, to identify the nationality of each user of each piece of equipment based on the definition of nationality, to evaluate the extent of foreign national use of each piece of equipment. And is a license required, we heard that discussion this morning, it's not clear. To obtain a license for an individual, nationals, to make particular uses of individual pieces of equipment. This assessment could happen more than once during the course of one person's doctorate or postdoc because the dynamism of the list and of course the research, and the fact is that none of us in this room knows where these lists are going to go and what the requirements are going to be in the future. This is going to be a dynamic process. This type of

interruption really should be a problem for all the federal laboratories too.

My third concern is is it possible that the Inspector General's recommendation in the March '04 Report to Congress on Export Controls is based on the incorrect premise? We heard earlier that the Inspector Generals in fact had no examples of security risks. The risk to our national security from international students and postdocs who have been cleared through the visa and visa mantis procedures is not obvious at all. The cost to the U.S. research enterprise which is already under enormous pressure as we have heard, especially when denying a visa to an undesirable foreign national and/or classifying technology to maintain security seem live obvious, cost effective, and thoroughly tested solutions. This is especially true and many corporations do not advise customers of the export control classification of their products, do not inquire as to the nationality of purchasers or users of their equipment from the sources other than universities.

Five recommendations if I may, one, first recommendation, greatly narrow the list scope of controlled technologies requiring deemed export licenses and ensure the list remains narrow going forward.

Two, delete all controlled technology from the

list whose manuals are available in the public domain, in libraries, over the internet, or from the manufacturers. I think that may be in sync with what is currently planned.

Three, delete all equipment that is available for purchase on the open market overseas from foreign or U.S. companies.

Four, clear international students and postdocs for access to controlled equipment when their visas are issued or shortly thereafter so that their admission to a university academic program is coupled with their access to use of export controlled equipment.

And five, don't change the current system of license requirements for use of export controlled equipment in university basic research until the above four recommendations have been implemented.

Thank you very much.

[Applause.]

DR. HAMRE: Extra bonus points for ending early, Dan, thank you. Ed Rice, who is with the Coalition for Employment Through Exports, a long time expert in export issues, worked extensively up on Capitol Hill, we're glad you're here. Thank you.

**Agenda Item: Discussant Panel - Dr. Ed Rice,
Coalition for Employment Through Exports**

DR. RICE: Thanks a lot, John. Today's meeting I

think for all of us has been very helpful in defining the ambit of what the Inspector General recommendations are and I think it also reinforces the value that many of us have put on having BIS at the central leadership on this and Peter and his colleagues in particular in managing this and keeping these issues in the proper balance. But I'd like to use the few minutes I have to broaden the perspective a bit because I think it's important to understand the context into which this particular Inspector General recommendation fits and what's driving this within the U.S. government.

Along with several of my industry colleagues, some of whom are here today, we've been delving into this over the past four months fairly intensively. And what we've concluded is that there are fundamental shifts underway within the U.S. government on technology transfer policy more generally and on China specifically, and China has an awful lot to do with both the Inspector General recommendation as well as other initiatives.

What we found is that at the Defense Department, the State Department, the Office of Science and Technology Policy, and in certain elements of the intelligence community, there's a good deal of ferment on these two issues of tech transfer policy and China. We see two major trends that I think you ought to take away from this, not

specifically with regard to the Inspector General recommendation or the need for us to comment but as things to watch out for.

First of all there is an effort underway to redefine U.S. policy on the benefit/risk balance of technological openness in the United States, both in the academic setting and in the industrial setting. We see this in particular in the foreign, the annual Foreign Economic Espionage Reports, the most recent one of which was issue in the latter half of April, which raises significant concerns about the national security threats of technology access within the United States by foreign nationals, both legally and covertly.

You also see this coming up in recent speeches by the FBI's Director of Counterintelligence David Zadi(?) who spoke most recently in February here in Arlington, Virginia, and also by the National Counterintelligence Executive Michelle Van Cleve, who spoke most recently the first week of April down at Texas A&M, again on the national security threats of technology access by foreign nationals here in the United States. Again, both legally as well as covertly.

With regard to China all you have to do is keep track of the Defense Department's Annual Report to Congress on the Chinese Military, the most recent one of course is

about a year ago, the one covering last year is due out sometime this month, again as would the unclassified version of the Foreign Economic Espionage Report, there is an unclassified version of the Chinese mil report. I'd encourage you to look at it, last year's report as well as the one before that on Chinese mil makes a specific link between technology access by Chinese nationals in the United States as well as outside the United States to U.S. origin technology to the Chinese military modernization, which of course is now a big concern within the U.S. government.

I'd also commend to you Robert Kaplan's article in the June issue of the Atlantic which describes in some detail the planning that's not underway within the Pentagon for a military conflict with China, and again raises the issue of technology transfer. Michael O'Hanlon's recent op-ed, Michael O'Hanlon up at Brookings most recent op-ed in the Financial Times about a week or so ago, again echoes the same findings about what's going on within the defense establishment on Chinese access to military technology, to U.S. technology.

These public reports are echoed by private discussions that several of us have had with officials at DOD, State, and within the intelligence community, all reflecting the same reevaluation that's underway more

fundamentally. I think what we're faced with if I could suggest it, again beyond the specific Inspector General report and beyond the policy that BIS has so effectively maintained for all of us, is the risk of a more fundamental change in the center of gravity within the United States government on tech transfer issues. This is raising questions about the basic direction of post Cold War U.S. export control policy, i.e., the idea of greater openness, and the refining of export controls both geographically as well as substantively, specifically questioning U.S. technological interaction in integration with China, and I think we're going to see more of that. And it also raises warnings about other countries as well and again I would commend to you that Foreign Economic Espionage Report that's on the website of the National Counterintelligence Executive.

I think we need to pay attention to these trends, again reinforcing for all of us the value of having an agency such as BIS and the officials who lead it playing a central role in this but there are other actors at work here and I think that for those who are trying to understand where these kinds of Inspector General recommendations come from and what other things might happen in the future, you need to understand where this policy is heading.

Thank you.

[Applause.]

DR. HAMRE: Okay, Jim Short, Jim Short is with the Department of Defense, he does the lab management and we're delighted he's here today. Thanks Jim.

**Agenda Item: Discussant Panel - Dr. Jim Short,
Department of Defense**

DR. SHORT: This is the second time that I've spoken in front of a very distinguished audience here at the National Academy of Sciences, the last time I did it was almost exactly three years ago and it was actually Dr. Hamre's fault that I had to do it then. He had signed a series of memos, I think it was February of 2000, dealing with how we protect research and technology information in the Department of Defense. I came here on that day three years ago to what I thought was a very hostile audience and I left having made a great deal of new friends and I think the academic community was soothed and satisfied by the message I delivered then.

Now I'm in the part of the Department of Defense where I'm responsible for the operations of our laboratories and in the part of the department that is responsible for our fundamental research program. And the Department of Defense needs universities, we need students, and we need the best students that we can recruit to work

in our fine universities here in the country.

So I have experiences that I want to share with you because I have run afoul of the EAR, or the ITAR, three times in my career and on each time it was scary going in, I think I was scared not unlike you all are a little bit scared right now, but it turned okay in the end and I think Dr. Hamre's point about when you have rules and regulations that 99.9 percent of the time people pass they're not rules and regulations to be, they are to be taken seriously but they aren't something to be afraid of.

That in the Department of Defense we know how to protect information and we know how to determine what kinds of information need to be protected, whether it needs to be classified, whether it's simply controlled unclassified information, or if it's public releasable information and of course in our fundamental research programs it's very rare that the information that's generated in those programs is not public releasable, in my 27 years I don't have one example of where I've ever classified any research that's been going on in my programs that I sponsored. And my observation has been that in our defense laboratories our compliance with the deemed export rules is quite good, I'm not going to tell you it's perfect because we're a very, very large organization with hundreds of laboratories and mistakes are made.

Similarly when I visited university campuses where research has been ongoing under my sponsorship it's been my observation the compliance there has been very, very good. So I don't see that the particular changes that Mr. Lichtenbaum and the BIS are proposing are a specific issue, rather I think it's the issue that maybe you all are just coming to realize that there have been rules and regulations out there that maybe you weren't aware that you need to be following.

Those rules and regulations are out there and I'll tell you about the three times I ran afoul of these rules and regulations. For 20 years I was the chairman of an international symposium on explosives, it's something that obviously when it comes to military information research and technology information about explosives is sometimes controlled, sometimes classified information, and so having that kind of a meeting and international forum is something that we do very carefully and the meeting is a public released meeting.

It costs money to run these meetings and so one technique that I tried in order to get money to help defray the cost of the meetings was I invited commercial vendors to come in and display their materials. Well, I got in trouble because one of the commercial vendors came in, he was selling scientific cameras, and it turned out that at

that symposium he began the negotiation of a contract to sell an ACC(?) controlled camera to a foreign country that wasn't permitted to receive that camera. And so I wasn't directly involved in that but nonetheless I was responsible for creating the linkage between the camera vendor and the person receiving it.

And so it was a painful experience as I was, I don't know if the word investigated is the right thing but the situation was being investigated, but in the end it did work okay for me, the camera company got in trouble, you can go to the BIS website, you see the examples of awful things that people are being fined for selling things illegally, however I think the kinds of problems that those of us in the room here in the academic section at least are faced with are going to be nothing so horrendous as that.

I had another occasion where I had one of my symposiums in 1989 and early in 1990 there was a little paragraph that appeared in Newsweek Magazine that suggested that the participation of three Iraqi scientists at my symposium had enabled the Iraqi nuclear weapons capability. That caught me deep in the heart, I know nothing about nuclear weapons and so I have no idea if something I do is enabling the Iraqi nuclear weapons capability and what's more since everything that was discussed at that meeting was supposed to be publicly released information, in fact

it was publicly released information, that there should not be an issue.

However, there's always the things that go on during the coffee breaks, as we said coffee breaks are very important, I had the unpleasant experience of falling asleep in front of my television one evening and then waking up about 1:00 and there was the world's or the United State's preeminent investigator reporter Geraldo Rivera talking about my symposium with the illustrious Congressman Dingle. And this led to more serious consequences to me, that there was a closed session, a classified session held on Capitol Hill where my symposium was discussed. But once again, my experience, it was scary, it was frightening, but when it was all over said and done there was no problem, this was another one of the 99.9 percent of examples where everything was fine, it was just that people were frightened at what they were seeing.

The third example involves, lots of mention has been made today of China, and we have representatives here with us today from the Embassy of China, but there was a period in my career about 15 years ago where I actually lost my security clearance and the reason that I lost my security, suspended is the word. The reason I lost my clearance was that information in a paper that I had written was released for a symposium that was being held in

Beijing. And again, when this information was released, I recognized that it was released, I realized this didn't make sense, I called it to the attention of the appropriate security people, and an investigation was done and once again it was determined that everyone, while there was misunderstandings, that everything had been done according to Hoyle(?) and that there was no improprieties.

So you're going to run into these kinds of difficulties as you go out there and deal with these rules but these rules have been in place and I think they are, there is benefit for the country. That in the Department of Defense we have a very robust research program and what we try to do is we don't want to give our technologies, our military, our technologies that we're applying for military applications, make those easily available to our potential adversaries, because if the adversaries get the technology then we have to redouble our technology efforts to stay ahead of our adversaries. So there is definitely benefit in controlling information and it's definitely important that we know when we are releasing information to foreigners here on our domestic soils whether or not the release is an appropriate export or if it's a controlled export, and obviously we shouldn't be doing the controlled export.

But it is to the benefit of the Department of

Defense that in our fundamental research program I think seldom will we run into this problem, seldom will you run into those problems in the universities. However, in these economically difficult times for universities, my wife is a vice president at Georgetown University by the way, the universities are going more and more into areas that are not in our fundamental research program, they're going into what we call our advanced technology development programs and things of that sort. And I just have to caution you that you go there with risk and so the campuses, some campuses do an excellent job in what shall say putting up a firewall to keep separate their fundamental research programs from their advanced technology kinds of demonstration programs that they do for our department, other campuses are not so good and we in the basic laboratory segment of the Office of Director of Defense Research and Engineering work not only with our laboratories to help them do a better job there but we want to work with the universities to help them do the better job as well.

Thank you.

[Applause.]

DR. HAMRE: Thank you, Jim. Chuck Fisher, Chuck is with the DOD Counterintelligence, I don't know if you're with the NCIX or not, Chuck, but are you at NCIX?

DR. FISHER: No, sir.

DR. HAMRE: Okay, good to see you.

Agenda Item: Discussant Panel - Dr. Chuck

Fisher, Department of Defense

DR. FISHER: As Dr. Jim pointed out both of us kind of had a mission given to us by Dr. Hamre several years ago. Currently I teach at our Joint Counterintelligence Training Academy, my function there up until very recently was director of the CI support to research technology protection program.

And essentially in a nutshell what we're trying to do is educate our Department of Defense counterintelligence agents, those representing the Navy, Air Force, and Army, to operate effectively in a research technology protection environment and that does segue into working within the academia environment as well when we're talking about identifiable, critical technologies that are handed off to academia that require enhanced protection controls, whether that be classified information, i.e., a classified project, or those specific technologies identified as critical for export controlled reasons.

And the counterintelligence function in that environment is to increase the awareness within the university setting, particularly the principle investigator, of the potential threats or intelligence

information that they need to be aware of as they make their decisions with respect to information release, pre-publication review, and consult with the Department of Defense to ensure that no leakage, unnecessary leakage gets out that we didn't want to have happen before hand. And that's essentially the role of the Department of Defense Counterintelligence in a nutshell in terms of the academic environment, one of increasing awareness.

The idea that in some concept way shape or form we're going to preconceive or have a prediction of a threat to a technology that does not yet exist I think is fiction. I don't think it's possible to do that, the other thing is as Jim pointed out, what the department is undertaking is a robust attempt to not only identify those programs where a national security decision 189 has been made, i.e., this needs to be classified, and of course that's made by the department.

But also extending the bubble a little bit out to try and identify those specific technologies in the basic or fundamental research area that are significant and may require some additional protection, but very, very narrow, you're probably talking about a very, very narrow occurrence and universities are taking extraordinary steps, Georgia Tech, University of Virginia, Virginia Tech University, MIT, to develop technology control plans, to

separate and segregate the classified programs the department has provided them to work on from those programs that are truly fundamental or basic research. And those are tremendous initiatives because you're educating your staff, the researchers, particularly the PIs, on export control requirements to process for licensing and so forth, and that has helped us in counterintelligence because what we're looking for, what sets us off if you will is an anomaly, some behavior that's outside the norm.

And all of you as researchers, you know what your norms are for your programs, and if you establish policies and firewalls and someone attempts to circumvent that in some way shape or form, that's an anomalous behavior, it can be reported to campus security, looked at as a security event.

Or if it's in a DOD project and DOD has an equity that can be reported to either DOD counterintelligence or Defense Security Service counterintelligence if you're under the National Industrial Security Program. All we're going to do is examine that from a foreign intelligence perspective, that's it, is that act, is that individual acting on behalf of or for a foreign power, that's the counterintelligence function in this country, to prevent and detect threats from foreign intelligence trying to penetrate our systems, our government, or institutions.

Nine times out of ten you're probably not going to cross the threshold into a foreign intelligence service. But we have to be able to examine that so getting the information flow is what we're looking for at this particular stage of the game and in so doing that enhanced national security protection.

But that's the role of the Department of Defense counterintelligence in this particular environment and as Jim did point out it changes when you move into the advanced technology development programs, at that point technology is more identifiable in terms of its application, it's not notional, the concept has borne some fruit and then it comes enhanced, even more enhanced protection requirements, not only on behalf of universities in conducting this research on behalf of the department, but the role of counterintelligence would thereby increase as that technology becomes more sensitive or is identified as more critical.

That's all I have, thank you very much.

[Applause.]

DR. HAMRE: Since you were all so good about time and because both Chuck and Jim mentioned my role, I'd like to just say one brief word if I could. I was the deputy secretary of defense before I left in 2000 and went over to CSIS and I have had to sign FISA(?) petition requests

because we've had spies, there are spies in this country, let's be honest, there are spies in this country. And they do not wish us well, they are working very directly to harm our national interests.

But what I've learned is that 9/11 as universalized our paranoia, we're now just afraid of everything in this country, and we've got to be sophisticated about this, we've got to be very precise about what it is that really is a threat to us. And that requires discipline on our part to think through the problem, not just fall back susceptible to generalized paranoia in this country that bad people are out in the world and are trying to hurt us. They are, but far more important, the vitality of America, our national security is really based on the vitality of our society by the dynamism and productivity of our economy, I mean that's what's really astounding in this country. And we have got to pursue security solutions that don't impinge upon that larger national security thing, the vitality of our society, the dynamism of our economy, the capacity to invent new ideas and bring those new ideas to make a better and safer world. That's real national security and we've let 9/11 universalize our paranoia and we have got to start becoming very focused and very disciplined about what it is that we care about, what really represents a threat.

I don't believe we should fall back to very general vague representations that there are bad people out there that want the technology, we got to keep it from them, well, that's patently true, it's also doesn't help you as a security guide and we've got to be far more focused, far more disciplined on this.

Second thing, I learned this when I was up on Capitol Hill, don't write laws that force people to break them. As a rule of thumb you shouldn't write a law if people are going to have to break it to live. Then you haven't done your job right in writing the law. So think very carefully about what you're trying to do that it really solves a problem and that it's the most efficient way to really solve a problem.

The third thing then I will stop, I'm sorry, I'm interposing my own personal views here, you really have to be very careful not to impose a regulation that's so extraordinary that it just induces people to take their word elsewhere. And if you look at what we've been doing in this country, we inspect 100 percent of the people that come from China, we inspect two percent of the containers that come from China, and zero percent of the electronics. Right? What does that tell you? We've created a tremendous incentive to send our best jobs to China. Is that stronger national security in the long run? No, just

got to be honest. So I mean we have got to be, we have got to take a very sophisticated and integrated view of this problem and that's why I think it's so important to have sessions like this and I'm grateful you're all here.

Now we're going to turn to our fans out there in cyberspace, they've been patiently listening, waiting to interrupt us, so we're going to give them the first question. Please, Tabitha.

Agenda Item: Open Q&A

DR. BENNEY: Thank you very much. My name is Tabitha Benney, I'm National Academy staff, we've selected a few questions off our web cast viewers, we'd like to invite the rest of the web cast viewers to continue submitting questions if they'd like. The first question is from Patrick Slasinger(?) from University of California, he asks rather than beginning by classifying equipment doesn't it make more sense to first determine if there is an export controlled and proprietary information that is not allowed to be publicly disclosed in a lab? If there is not and a university would not have to classify equipment or start closing its open campus to certain individuals, isn't this right? So I imagine this is directed directly at you Peter.

MR. LICHTENBAUM: I was afraid of that. I think the premise of the question is correct that what you're

trying to do is to determine the classification of technology, if that can be done by focusing specifically on the technology that you want to transfer without classifying equipment that will merely be used and not exported, that's certainly fine from an export compliance standpoint. I think the reason why universities have felt it useful to classify equipment is in order to know what technology might be transferred it's sometimes useful to know what equipment you have that you're training people to use but whatever works best for you is the approach that you ought to follow in order to classify your technology.

DR. BENNEY: and then the second question we'd like to read is from Donald Weden from principle Weden and Associates, his question, and this has been edited. The threat of technology theft has not materially changed since the 1970s, only that there are more actors on the stage. Does it not make eminent sense to revisit the NAS Course and Report of 1982 and its update of 1984 first and then see if adjustments need to be made in our balancing of scientific communication and national security? Merely imposing problematic prescriptions will not materially remedy matters by thinking it may, what are your comments?

MR. LICHTENBAUM: Well, if I could start on this one and others may have some thoughts as well, because it did, this question does to my mind relate well to some of

the presentations that were made just now. I think many of the concerns that we just heard relate generally to the deemed export program and not specifically to the Inspector General recommendations, and therefore the question that the community ought to consider is if that's, if the questions that exist and issues that raise in terms of the proper balancing of openness versus control, are significant and in your view are not being dealt with adequately by the current controls, then perhaps a broader look at this issue is appropriate by the private sector such as under the auspices of the National Academies or otherwise in order to provide us with your assessment of the current controls.

But we are, our immediate task is to address the Inspector General Report, which is not to impose a deemed export program which we already have. So I just think if there are fundamental disagreements about the existence of our deemed export program we can have that discussion, we welcome your thoughts on that, but that's not the immediate, our immediate focus in responding to the Inspector General Report.

DR. HAMRE: Any of the other colleagues want to speak to this?

DR. RICE: Well, I just wanted to echo Peter's division of the question here, and I think it's very

important that we do have to deal most immediately with what BIS has put on the table for comment. But I think more broadly we are headed inevitably toward a much more fundamental discussion as this more fundamental discussion that's already underway within the U.S. government progresses. And earlier in the day there was a comment as well, it may or may not see the light of day, perhaps so, but nevertheless it does, some of us are convinced that it is underway and I think there's going to have to be a forum to discuss that within the public sector as well.

DR. HAMRE: Okay, let's open it up, Tabitha, you keep track of cyberspace here and let's open it up the floor for people, just come up to the microphone and pose your question if you would to the panelists.

Do you want to say something? Jump in.

MR. LICHTENBAUM: I just wanted to address one point that came up, maybe a couple points that came up. Don't worry, I won't engage in hostile fire or anything. With respect to your comment about the paranoia that we ought to guard against, I couldn't agree more, and I think that's a very important contribution to this issue that we all ought to keep in mind. To me that works both ways, that is we ought not rush into imposing controls based on paranoia of what the Chinese or any other country or organization is seeking to obtain in this country but we

ought to base our actions on evidence and reasons, conclusions, based on that evidence.

Conversely though on the other side of the ledger, we ought not eliminate controls based on paranoia about how they may effect the community and rather we ought to as I think many companies, many schools are doing, understand the specific impact of the current controls on them, the proposes changes that the IG has suggested, because in my experience if we look to facts and we apply principles, agreed principles in a reasonable way to agreed facts, we're likely to come up with a debate that's between the 40 yard line and the 60 yard line rather than between the two end zones. So I would hope that we can proceed in this debate over the next few months in that way, looking to facts rather than rhetoric or assumptions.

The other point I wanted to make is with respect to the question of if we are approving 85 percent of the licenses and returning without action another 14 percent so that were only denying one percent, does that mean we have a program that's fundamentally out of kilter. And I respectfully think not, that indeed if you compare the deemed export program to our export control program as a whole, I think our overall denial rate is between one and two percent for export licenses as a whole, so this point certainly if it were true would apply to our export control

program as a whole --

PARTICIPANT: It does.

MR. LICHTENBAUM: Okay, and I might say it probably applies in the ITAR world as well, that I would suspect the vast majority of ITAR licenses are granted because people who want to say export arms to the People's Republic of China where we have an arms embargo and therefore would deny a license are not likely to apply for licenses. So the export control program does to me survey function even if because people through the services of lawyers, etc., learn what licenses are likely to be granted and only for licenses that are likely to be granted, we end up approving the vast majority of licenses.

That doesn't mean that export controls don't serve a function, the controls that we have are based on a multilateral agreements reaching back 20, 30 years based on agreement of ourselves in the interagency process, with other countries, our closest allies, and it would be foolhardy to suggest that we have universally got it wrong, that we're controlling far more than needs to be controlled. Now certainly the lists need to be kept up to date, we welcome specific suggestions for doing that, we have a process for doing that, but it is not in our experience, is is a vast surgery that needs to be done on these lists.

DR. HAMRE: God, I'm so tempted but not going to, because this is something I actually feel quite strongly about but I don't think it's appropriate. Let me first, let's get questions first, I think that'd be more appropriate. Henry.

PARTICIPANT: Well, my comment really more than a question, or I can phrase it in the way of a question, is really related to the point you made, it seems to me your logic that we have an immediate question to answer and the broader issue therefore is to some extent irrelevant to answering that immediate question, I think one could turn that logic around and say that since there are very basic questions about the current structure that now adding an additional hundred cuts to the thousand cuts if you like in the context of the concern that is already existing and of the data that is already existing that these plus other kinds of restrictions on foreign nationals may be harming our enterprise, it seems to me an appropriate response to the Inspector General's Report could be let's not perturb the system even more until we face some of these fundamental questions.

MR. LICHTENBAUM: I actually share that perspective, in other words I'm not saying that the broader concerns that apparently exist with respect to the deemed export program are out of bounds in your comments or on the

IG Report nor on our response to the IG Report. I just am saying that I think those, well, those are fairly taken into account as you suggest, sir, in our response to the IG Report and in your comments on the IG Report. But I mean to say that we are unlikely to be able to deal in our response to the IG Report with the broader issues that are raised, for example, there are those in this room who feel that we ought not have a deemed export program, that's a more fundamental debate about our export control system then we will take on in our response to the IG. In this country we don't take any issues off the table so if the industry and the academic community wishes to suggest a fundamental reexamination of the deemed export rule that's their prerogative and the administration would listen very closely to those concerns.

PARTICIPANT: Two previous questions addressed the subject of proprietary information. 21 years ago when the publicly available regulation was developed there were those who thought that one element in it did have the effect of limiting controls to what was proprietary because of the portion of the regulations that says if it's available, either freely available to the public or available at a cost which does not exceed distribution, reproduction and distribution, it is publicly available. The thought being that if the cost was higher then that it

would be proprietary. Perhaps however this is not as clear as people 21 years ago thought, apparently it's not in the eyes of some of the questioners. Perhaps someone on the panel would like to comment whether that is an inadequate or an adequate description of what is proprietary and not proprietary because there seems to be a hope that this evaluation of whether or not you're effected can be simplified by the word proprietary.

DR. JOHNSON: Well, actually, I don't really have a comment on that per se, I would say that during the break I was talking to one of my colleagues who's sitting in the second row and I'm hoping will jump to the microphone and speak to this issue and also to the complexity of trying to comply with this. Tim, I don't know if you'd mind saying something?

DR. HAMRE: Would you step to the microphone and identify yourself so our friends in cyberspace can know you.

DR. DEVENCHENSO(?): This will teach me to not talk to Cynthia on the break. I'm Tim Devenchenso, I work for IBM, the export regulation office, I've got my PhD in metallurgy and material science from the University of Pennsylvania and I noticed on the list there are three people from Penn, I wonder why. Why? Why a technical guy in the export office? Because of these regulations. I

must talk to well over 1,000 IBMers a year, I've got a chart which if I knew you were interested in I would show you because I show it to them. I put these regulations in colors, it's a pyramid chart, red at the top, that's where ITAR is, crime control related things, things that we're mostly not involved in.

But then we go to orange, we go to green, we go to blue. Orange is that peculiar set of technology that only the 22 countries can have in their foreign nationals. Green is available to all the free world. By the way I put that on that chart once and I went to Beijing and they said oh, that must be us. I said no, no, you're not in the free world, so we revised the chart and used the jargon in the regulations and put down the B countries, the Group B countries, now no one knows what that means.

And then we sort of stopped there at one point and said that's fine, we don't have to go to blue because blue is the AR-99 and that's where 95 percent of our stuff is. Well, when we didn't do that that's what we were barraged with, questions on where's my technology, it's not on your list. So that's why we talked to 1,000 people, over 1,000 people out of our office in IBM per year.

And let me give a little bit of an anecdote to show you what level of detail we go into sometimes to classify what we call blue zone. Our Zurich lab came to me

a couple months ago and said we're going to ship a gyroscope to China, and first I said what are we doing with gyroscopes in the IBM Corporation, and I said you're not going to ship a gyroscope to China. That's all right, we're shipping it to our China Research Lab. I said no it's not all right, we have to classify it.

To make a shorter story of it believe it or not we finally found somebody in our Almaden lab who knew that technology and was able to go through category seven of the regulations, which we normally don't find ourselves in. And he determined that we did not have a controlled gyroscope, but why are we dealing with gyroscopes at all. Well it turns out our retail sales solution people who are trying to track carts that go through the Giants and the Safeways, they want to know where they are on the aisle so that when they hit the Pepsi display a little jingle will come up.

Fortunately we did not find ourselves, when we went through the details of the parameters, to be in controlled gyroscope navigation equipment territory. But we must have spent the better part of a month trying to figure that out and this is just one example and this is why we can tie up so much resources. So university types, welcome to the world of export controls.

Thank you.

DR. HAMRE: We're not feeling better here.

Terry.

DR. MURPHY: I actually hope, Terry Murphy again, I'd actually hoped I might get the last word in but I can't forebear given that one. First of all I would like to acknowledge that present here today are Drs. Colglazer, Cal-Tech, PhD, theoretical physics, Dr. Short, Berkeley, PhD, mechanical engineering, munitions and explosives, and Dr. Mote, Mr. President, Berkeley, PhD, mechanical engineering, dynamic systems, etc., etc. It's nice to know that the real talent is on the West Coast. But I have to quote again, much as it burdens me, to somebody from Cambridge, and that is Patricia Wrightson when she invited me to this to help chair this group reminded me of a marvelous conversation, event we had here several years ago when the superstar professor at MIT of space science or whatever he called himself said the following which I have dined out on all over the world, this quote, his quote, rocket science is easy, I can do rocket science, export controls is really hard.

DR. HAMRE: Other questions from the audience here or Tabitha, do you have some, David, just a second, let's do Tabitha and then I'll call on you next.

DR. BENNEY: This is from Patrick Slasinger from the University of California, he asks in the current

political environment it appears that many manufacturers are over warning by stamping all kinds of materials export controlled. This includes materials that are publicly available by being provided to every customers of the product. Does BIS agree that the real question is not whether an operating manual is stamped with a particular warning whether it is provided to the recipient under a duty not to disclose, for example a non-disclosure agreement?

MR. LICHTENBAUM: Well, I think if you're contemplating disclosing technology then you've got to evaluate all the facts and circumstances that you have relating to that technology. If you are told by a company that provides you technology that the technology is export controlled that's not the end of the study but it does give you reason to look into the technology and make your own determination about whether it is in fact export controlled or not. You are not bound by their classification and I imagine there may be situations where companies over classify out of an abundance of caution, especially if it won't be their problem. But in the end it is the responsibility of the individual institution involved who wishes to disclose the information as to whether a technology is export controlled or not and whatever statements are conveyed along with the manual or the

equipment are not binding on you whether it's via a stamping as export controlled or as information that's subject to a non-disclosure agreement, you may have contractual obligations under a non-disclosure agreement but the export control rules govern and you make your independent determination from an export control perspective.

DR. HAMRE: Ed, do you want to speak to this as well? Is there any comment you want to make?

DR. RICE: No, I'll pass.

DR. HAMRE: Okay. Any other questions? Let me turn to David.

DR. ROSE: I'm David Rose with Intel Corporation. One of the issues that I think has been framed here is the notion of having to work from generals to particulars in the licensing process where you may start with a very large universe of items and you have to classify to be able to come up with a very select target. And I would not just as a matter of experience that companies like ours have really pretty massive export compliance groups and their job is to work from generals to particulars and it's really incumbent upon companies to take a look at activities that are occurring across its global expanse, look at all the various technologies and so forth and there's really a lot of due diligence that's involved in that respect.

One other issue, I was wondering if BIS or other agencies might be looking at the implications of applying a deemed export rule to foreign nationals in third countries, are there legal implications with respect to say the EU personal data directive or Australian privacy laws and the like or are there any folks here that might be able to address that question. Thank you.

MR. LICHTENBAUM: Thank you, David, for your comment and the question. I think that the question of application to the overseas operations is an important one, the same question was asked recently at the American Conference Institute event where I spoke, and I'd encourage the community to address that, indeed it was one of the requests I made in my presentation for information on how these proposals of the IG if adopted would effect the overseas operations of U.S. companies.

I don't want to speak for the IG but when I read the IG Report it appears to me as if their recommendation would potentially apply in the deemed re-export context as well, that is I don't know to use too much jargon here, deemed re-export is a transfer of technology in a third country, so outside of the United States, but that technology is U.S. origin technology so our rules apply to the transfer of controlled U.S. origin technology wherever that occurs, in a foreign country or here. And the way in

which the IG's recommendation therefore might apply is say you have a manufacturing operation that's located abroad and you have folks there who have established permanent residency in that country but were born in Iran let's say or China, as I read the IG's Report the impact of adopting their proposal would be that you could no longer treat those persons who are permanent residents of the UK as UK nationals for purposes of compliance, but you must treat them as Iranian or Chinese or wherever they were born. I don't think they draw a distinction between deemed exports here in the U.S. and deemed re-exports that occur in other countries.

So obviously we'd be very interested in understanding the interaction of that proposal with your business operations and foreign laws such as the EU Data Privacy Directive that you mentioned.

DR. JOHNSON: I would just say that a couple of people have raised this question and I appreciate David raising it here, so far as we've been able, we're asking the question internally and we don't have an answer yet but we do intend to address that. My understanding also is that the ABA will be addressing that in their comments but it does raise some serious issues. And I will say also that country of birth is not something that we would typically track right now, so it's possible, actually

probable, that we would have to create a whole new system to try and track and capture that information.

DR. RICE: Just by coincidence the OECD has issued a report on immigrant and expatriates in OECD countries that goes directly to the importance of David's question, and if you just look at, just to pick out several that are close to the United States in a variety of areas, if you look at the European economic area, that includes Switzerland plus the EU, ten percent of the population was born outside of that area that are now resident there, Canada 19 percent, one in five, Australia, 23 percent, nearly one in four, and the longer report breaks that down between those who will become citizens of those countries versus those that are there as non-citizens but could be working for a sub of a U.S. company and therefore subject. So there's an extraordinary reach if you start looking at this in other countries, particularly ones that are close U.S. allies.

MR. LICHTENBAUM: I was wondering actually, that's interesting information and I was wondering if I could ask a question and see if anybody has any assessment of it since a number of you have foreign operations, whether companies or campuses I imagine might have foreign campuses as well. And the question would be what is your assessment of whether the permanent residency requirements

in other countries are more or less stringent than U.S. permanent residency requirements, how do they compare? As I mentioned in my remarks I did not see an analysis of that in the IG Report and it is clearly something that is relevant to our determination of whether our current approach, put aside the country of birth approach, but whether our current approach sufficiently protects our national security. So I would be interested in any comments from the audience or from cyberspace about whether other countries such as the ones Ed mentioned, Canada, the EU, have controls in order to obtain permanent residency that are broadly comparable, more stringent, less stringent, any views that people have would be of interest.

DR. HAMRE: Is there anyone here that would like to address that?

DR. FISHER: Just to comment on that, it's kind of hard to quantify because you've got to get into details, but I can just, just hypothetically as an intelligence officer if I want to create a loophole and I know that you have a particular country you're concerned with, and I know I can get access through another country, that's where I'm going, that's where I'm going. That's why country of birth, country of citizenship is important but country of birth is also critical from a national security perspective if you're concerned with your national security, you're

concerned with your loss of information that you did not intend to lose. So from that perspective country of birth becomes very critical in terms of evaluating threat, and not just country of citizenship. I'm speaking as an intelligence officer, that's just kind of a hypothetical.

PARTICIPANT: Peter's already heard this question, it's a Jeopardy question, I guess I'll ask it of Mr. Fisher. The answer is Zbigniew Brzezinski, Henry Kissinger, Madeleine Albright, Albert Einstein, Neil Bohr, can you tell me what the question is?

MR. LICHTENBAUM: Who are some of our greatest research and education --

DR. HAMRE: I think what Eric has raised is a particularly complicated question which is what is the reliable screening basis for security and is nationality any longer a reliable basis for it. I think that's at the core of it and it's an important question, I personally think that we put far too much reliance on nationality as an indicator of trustworthiness, frankly we've had so many spies in this country that were born American, so to automatically presume that foreign origin constitutes vulnerability or national birth in the U.S. represents security is I think, really I don't think that ought to be the primary test of our starting point.

I do believe what we need is knowledge so that we

can do sophisticated risk modeling and then determine if that represents a path we should explore. But we're not using it that way, we're using it really as just a screen to say yes and no rather than as really a pointer toward intelligence security. And I do think we do need to know, I don't agree that with the proposition that approving 99 percent of the licenses is a good thing, that tells me we're wasting resources on at least 90 percent of them, we really need to conserve those resources on things that really matter rather than on just simply rule compliance.

But we do need to know what's going on and we then on the government side have to be very smart users of that knowledge. And I don't think we're very smart users of that knowledge on our side, I don't think we have, we seek information and I have yet to find really sophisticated use of that information on our side. And that it seems to me ought to be the, I think we'd be much better placed, we as a government, I'm speaking as a government guy here, we'd be much better placed to ask for intrusive knowledge if we can demonstrate how we use it effectively. And I think we're really demonstrating compliance of the governed rather than effectiveness of the government.

DR. RICE: This just triggers a thought, in this room there are some extraordinarily talented and well

placed people, both in academia as well as in think tanks, etc., and if you think about the task that our counterintelligence people are handed in trying to deal with the outgrowth of the U.S. government's assessment of threats, I think they're doing the best they can with the tools that they believe are available. But it may well be that some of you ought to take back from this meeting an assignment to try to figure out how to answer the question that Dr. Hamre has just posed and it may be that there could be some good work done that would help the government do that. Having worked on the other, when I was in the Congress in following a number of these issues from the national security side very closely you really have to take into the account the difficulty that people who are trying to do their jobs in the U.S. national security community have and I think that we're headed into territory now with these latest assessments of where the external threats are that's going to require a lot of help to try to figure out how to do it better.

DR. MOTE: I was very pleased with commerce decision to go out and ask for comment and today's in the morning session Peter asked for very specific information to help decide their severity of control requirements in terms of the dollars of cost, technologies, students involved and so on and really in a number of times pressed

for specificity about how compliance would be undertaken, what the costs would mean and so forth. And I think that's a very important approach, especially for technical and scientific people who really need specificity as they go forward with a solution to a problem.

I think the flip side is the first question the scientific or technical person wants to get on the table is what's the problem before they try to solve it. And I'm still waiting for the same kind of specificity in terms of what's the problem. I'm still waiting for someone to jump all over me and say well here, these five things happened in the last year and the threat of disclosure of technology to these graduate students working in these labs and what we know they have taken back and the consequences, or something, just some, even an anecdotal description of something.

And I think Jim talked about some things that came up to him when he got excoriated before various committees and so on which turned out to be saved, I don't think, we just don't see any of that surrounding these things so we have this elaborate effort, very expensive and possibly very destructive, at least expensive, yet we don't have the problem actually.

And I'm very sympathetic by the way with the security issue here, we have a lot of security work going

on at the University of Maryland, we have a number of very important projects on security side that we have committed to and we're very much behind and so on so it's not a lack of interest in security. And we're very supportive of all the compliance issues, we have a compliance office and we have done, do a lot of this sort of thing.

So it's not a lack of sensitivity to the severity of this problem at all, but just looking at the problem we're currently confronted with, this deemed export expansion, and we really would like to see a problem here that we're trying to solve that's actually quantitative. And just as we've heard to not give anecdotal descriptions about what the costs are going to be and we've been somewhat criticized, not criticized but suggested that maybe we're expanding the severity of this problem too much and maybe I would like to expand the problem that we're trying to solve a little bit before we try to solve it.

I still think if we had that sense of severity of the problem that it actually exists in a quantitative sense rather than an anecdotal sense or even a possibility sense, it would help us all I think take on these enormous challenges that we're being faced with these new regulations.

DR. SHORT: I'd like to add to what Dan just said and that is I gave three specific examples where I've run

afoul of the export rules. In my career I've done hundreds of thousands of things that might have run afoul of the export rules and I made decisions, I made a decision that do I need to apply for a license for the thing I'm about to do, I looked at the facts, it's easy as the individual to make a decision, I understand it's hard for a university or a corporation to make decisions. I looked at the rules and I made a decision that I didn't need to ask for an export license for what I was doing. And in those three instances where through no fault of my own my decision was examined by others it was corroborated as being a good decision and so I'd say to the universities that are working on fundamental research programs, for the Department of Defense anyhow, I would urge you simply to look to your Department of Defense funding official, your scientific officer, it's our job to watch out over what you're doing and I feel that the universities in large have done a better job than I've done in the number of export licenses that I've needed to ask for. And as I said in my career I've asked for none and there's never been a founding that I've needed to ask for any and I think the same is true for universities doing fundamental research.

MR. LICHTENBAUM: If I can comment as well on what Dan has stated, first I do want to say I strongly appreciate the compliance commitment that the University of

Maryland and all of you here in this room share, I think the standing room only attendance is testament to the importance that the community places on compliance and I very much appreciate that and think that our interactions with the community have always reflected that sentiment.

I also want to say that I completely agree that our policies as a government and I hope your perspectives as the regulated community need to be based on facts rather than assumptions and it gets back to the point that Dr. Hamre made at the outset about not just acting based on paranoia but rather based on facts. And as I said that operates both ways. We want to get facts from you about the compliance impact, we have an obligation ourselves to come up with facts as to what the necessary rationale for the program is.

Now on that, as I said we have sought a current assessment of the threat that has been alluded to a few times by a few people, there are spies in this country, as Dr. Hamre said. We do have to be extremely cautious but we don't want to act based on assumptions, we want to understand specifically what is the threat of control, of transfer of controlled technology in the U.S. high technology sector and specifically with respect to the university and research community. We expect to get that information very shortly but as all of you will realize to

a significant degree that information will be classified. Now we have an obligation to try to find a way to share the, at some level the rationale for the control program with the regulation program, but we'll have to work through how we can do that in a way that doesn't compromise classified information.

Finally I want to say that the lack of repeated instances of compromise of controlled information to me would not demonstrate that we ought not have a control program because it would to me as someone charged with protecting the national security, it would be irresponsible for me to say all right, well let's lift the controls, see what happens, and only when we have repeated instances of illegal, it wouldn't be illegal anymore, transfer of sensitive information, then we'll go ahead and re-impose the program. I mean we can't wait for national security to be compromised before we have the controls. What we need to do is base our actions on the threats that we have evidence to exist such as specific attempts by foreign governments to gather technical, controlled technical information in this country. We fully accept our obligation to base it on evidence of threat rather than paranoia of threat but what we can't do conversely is to say we're going to wait for evidence that our national security has actually been compromised because by that time

it may be too late.

DR. HAMRE: We are, I'm surprised not to see more interest in interacting here with the panel but if there is no more interest I'm going to let panelists have a final summation if they would like. So let me start with you, Dan, do you want any final summation remarks that you'd like to offer?

DR. MOTE: No, I think I've probably talked quite enough but naturally given a present you have to say something give the chance. I think we do need to see that there's a problem before we try to solve it. I gave five recommendations that I still stand behind at the moment, after hearing this and thinking about this for a long time, and I agree with the undersecretary that this is a very critical problem that we need to get right, we need to get the balance right between our scientific leadership, our economic development, and our security and this balance is very critical, we do not want to destroy our technological future.

The only thing I would emphasize is that we are a lot more dependent on international postdocs and graduate students for our future as a nation than I think is commonly understood by many people discussing this topic and I think that's a very, very critical issue.

DR. JOHNSON: Thanks, and again thanks to the

audience and to the National Academies for holding this, but I didn't get to my conclusion slide so I'll just go over that now. And a lot of these points have been made before but we do have a lot of questions about whether the current rule is a significant contributor to the national security and we raised some of those questions and we will continue to raise those questions and in fact David probably knows we've been raising these questions since 1994 so we will continue to raise them. And at the same time, particularly in an expanded version, it directly conflicts and impairs our ability to maintain technological leadership so we are very, very concerned about it.

We have put proposals on the table that we believe will streamline the deemed export program in the past and we've worked with your office on those and we continue to try and push things in that direction rather than the direction it's going in now. And finally we feel very strongly that it should not be expanded at this time until, and I think this gentlemen pointed out, until the fundamental weaknesses in the rule are remedied.

Thank you.

DR. RICE: Just very quickly, we're, we being academia and industry, I think are headed into a mode of playing whack-a-mole on these various proposed changes and I don't think it's going to be in the long run a good

outcome if we deal with each one of these things simply on their own, such as the Inspector General recommendation. I doubt very much that the IG himself dreamed up these particular proposals, I think they are a reflection of a more fundamental discussion underway in the government as I laid out and I think that both academia and industry need now to try to cause a more fundamental discussion of where these various policies are headed because step by step they are going to conflict increasingly with U.S. technological integration around the world.

DR. SHORT: I'd like to say that over the past several weeks and months I find myself frequently in the presence of Peter Lichtenbaum and his fine staff here and I've been very pleased with the way that Peter has been trying to calm the waves, I guess I feel that there's no huge issue about the change in the word and/or, I'm a guy who actually read the regulation in 1994 because my sensitivity was raised to it through my personal experiences and I confess not being a lawyer, when I read the word and I actually thought the word or. And so I think that my observation is is that what we're worried about is something that we should have started worrying about back in 1994 and it just sort of went over our head.

My personal opinion is that, at least in programs that I've been associated with, the compliance has

been very good. I'm glad today that we focused on the commerce section of the report and not on the interagency section of the report because there are DOD actions in there from the DOD IG for which I'm personally responsible and we are doing due diligence to respond to those things and I can say that in the Department of Defense building on Dr. Hamre's question, we're doing due diligence because we want to understand what the problem is and then determine if our solutions are viable solutions that will actually address the problem.

And then the promise that I make on behalf of the Department of Defense is that when we do respond to our IG that if there are collateral consequences, unintended consequences, that we will turn around and change our findings and change our policies and procedures. And I hope, Peter, if there's collateral damage that the Department of Commerce would be as wise as the Department of Defense.

MR. LICHTENBAUM: Just very quickly, first as a lawyer I might say that the word and sometimes does mean or so you're excused for reading and as or, but more seriously I just want to say that if and when we do take action in response to the Inspector General Report it will be via a proposed rule rather than a final rule, so that there would be further opportunity for comment and hopefully we would

manage to avoid such collateral damage rather than imposing it and cleaning it up later.

And otherwise I just want to thank the National Academies and the participants in the panel, I have found it a very useful session and we look forward to continuing the discussion in the future.

Thank you.

[Applause.]

DR. HAMRE: If I might just take three minutes, and I apologize to my colleagues here for this, but I spent 25 years in government and I'm very proud of it, I'm very proud to have been a government worker. And I'm a security guy, I got cop's blood in my veins and I'm a security guy at heart. But there was one key thing, I mean us security guys have to keep in mind is that ultimately we can't secure the country if the country doesn't trust us, I mean it really, it's that basic, it's that fundamental, our capacity to really do our job inextricably is tied to our having the confidence of those we work for.

I'd had an experience when I was, the Department of Energy asked me to head up a commission to look at the standoff between the scientists and the security types in the Department of Energy a couple of years ago. I went to Brookhaven Labs and this was when we were at the height of all of this and you could just sense the deep tension

between the cops and the scientists. And at the time the Department of Energy, the counterintelligence people were trying to push a regulation to require very detailed counterintelligence assessment on foreigners that were coming into the labs, before they'd be allowed to do an experiment. And the scientists were telling me how absolutely boneheaded this was, this was not going to do anything, and on and on.

So then I turned to the scientists and I said well let me ask you, you just gave me a tour of that big bevitron(?) or cyclotron(?), whatever the hell that thing was out there. Do you let anybody go out there and do a little experiment on it? Oh, hell no. Why not? Well, they could kill themselves or they could destroy the equipment. Well, what do you do to check? Well, we check to make sure that they've had bonifide laboratory experience, that the team that's coming from this foreign entity really does, has been screened by the host. I said that is extraordinarily valuable counterintelligence information but you don't trust the cops well enough to share it with them and the cops aren't smart enough to ask for it.

That's the nature of our problem here, we have such a profound gap between the government thinking its trying to solve a problem and the private sector not even

understanding it is a problem. And frankly the government can't articulate very well that it is a problem. That's the core of this problem with deemed exports, that at the core of our modern society.

And it is not going to get better when we see this as a test of wills one way or the other and that's where we are with these kinds of regulations and each side, I've listened this morning, it's been kind of a dialogue of the deaf, to be honest, and we're not going to fix the problem. And if the government insists it's going to squelch off very good and important and promising things. And if the private sector wins we're going to let spies work around us, I mean we really do have to fix this problem together and it requires a lot more trust and I would just plead with my very dear friends in the government, I still like I said, I'm very proud to have been there and I want to work closely with them to this day, that it really starts with having that trust on the part of the governed for us to be effective as a government.

So anyway, I'm done with my lecture, I appreciate everybody coming, we're going to give you some time back. Thanks for coming today.

[Whereupon at 11:40 a.m. the meeting was adjourned.]