AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. Hrg. 106–596

# EXPORT CONTROL IMPLEMENTATION ISSUES WITH RESPECT TO HIGH-PERFORMANCE COMPUTERS

## HEARING

BEFORE THE

COMMITTEE ON
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

MAY 26, 2000

Printed for the use of the Committee on Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE
65–171 cc WASHINGTON : 2000

For sale by the Superintendent of Documents, Congressional Sales Office
U.S. Government Printing Office, Washington, DC 20402

COMMITTEE ON GOVERNMENTAL AFFAIRS

FRED THOMPSON, Tennessee, *Chairman*

WILLIAM V. ROTH, Jr., Delaware
TED STEVENS, Alaska
SUSAN M. COLLINS, Maine
GEORGE V. VOINOVICH, Ohio
PETE V. DOMENICI, New Mexico
THAD COCHRAN, Mississippi
ARLEN SPECTER, Pennsylvania
JUDD GREGG, New Hampshire

JOSEPH I. LIEBERMAN, Connecticut
CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
RICHARD J. DURBIN, Illinois
ROBERT G. TORRICELLI, New Jersey
MAX CLELAND, Georgia
JOHN EDWARDS, North Carolina

HANNAH S. SISTARE, *Staff Director and Counsel*
CHRISTOPHER A. FORD, *Chief Investigative Counsel*
MARK T. ESPER, *Professional Staff Member*
JOYCE A. RECHTSCHAFFEN, *Minority Staff Director and Counsel*
LAURIE RUBENSTEIN, *Minority Chief Counsel*
DARLA D. CASSELL, *Administrative Clerk*

# CONTENTS


| | Page |
|---|---|
| Opening statements: | |
| Senator Thompson | 1 |
| Senator Lieberman | 3 |
| Prepared statement: | |
| Senator Akaka | 39 |

WITNESSES

FRIDAY, MAY 26, 2000

| | |
|---|---|
| Harold J. Johnson, Associate Director, International Relations and Trade Issues, National Security and International Affairs Division, U.S. General Accounting Office | 4 |
| Robert J. Lieberman, Assistant Inspector General for Auditing, Office of the Inspector General, U.S. Department of Defense | 6 |
| Gary Milhollin, Director, Wisconsin Project on Nuclear Arms Control | 8 |
| Dan Hoydysh, Co-Chair, Computer Coalition for Responsible Exports | 11 |

ALPHABETICAL LIST OF WITNESSES

| | |
|---|---|
| Hoydysh, Dan: | |
| Testimony | 11 |
| Prepared statement | 102 |
| Johnson, Harold J.: | |
| Testimony | 4 |
| Prepared statement with an attachment | 40 |
| Lieberman, Robert J.: | |
| Testimony | 6 |
| Prepared statement | 57 |
| Milhollin, Gary: | |
| Testimony | 8 |
| Prepared statement with attachments | 76 |

APPENDIX

| | |
|---|---|
| Insert for the Record: Response from Mr. Johnson to Senator Lieberman's Question | 119 |
| Responses to Questions for the Record submitted by Senator Akaka: | |
| From Mr. Johnson | 121 |
| From Mr. Milhollin | 122 |
| From Mr. Hoydysh | 123 |

# EXPORT CONTROL IMPLEMENTATION ISSUES WITH RESPECT TO HIGH-PERFORMANCE COMPUTERS

---

**FRIDAY, MAY 26, 2000**

U.S. SENATE,
COMMITTEE ON GOVERNMENTAL AFFAIRS,
*Washington, DC.*

The Committee met, pursuant the notice, at 10:09 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Fred Thompson, Chairman of the Committee, presiding.

Present: Senators Thompson and Lieberman.

## OPENING STATEMENT OF CHAIRMAN THOMPSON

Chairman THOMPSON. The Committee will come to order, please. I welcome everybody to this hearing of the Committee on Governmental Affairs.

Today we are holding a hearing on export control implementation issues with respect to high-performance computers. High-performance computers represent a special challenge for our export control regime, because in many ways they are the king of dual-use technologies; that is, technologies that are subject to national security export controls because they are easily usable for important civilian purposes as well as dangerous military purposes.

High speed computing, of course, is vital to today's knowledge-based economy. Unfortunately, however, as the Cox Report reminded us, powerful computers are also vital to such things as nuclear weapons development, the design and testing of ballistic missiles and advanced conventional weapons, intelligence analysis, code-breaking, military command and control, and cutting-edge warfare applications, such as computer network attack.

This is why high performance computer export control issues are so important. We have to find an appropriate balance between promoting commerce and protecting our national security through export controls. If we get it wrong, however, we either strangle a crucial sector of our information-age economy or we help potential adversaries prepare to defeat our military forces in the field, hold our cities hostage to weapons of mass destruction, or cripple our government and economy through information warfare.

The debate over high-performance computer export controls is particularly important in the Senate this year because of two pieces of pending legislation that affect this balance between commerce and security.

First is the Banking Committee's proposed reauthorization of the Export Administration Act, which appeared briefly on the Senate floor in March. Of most direct relevance to computer export controls, this bill would have written categories of "foreign availability" and "mass-market" status into the U.S. export control law.

That law would require that any control items meeting these definitions—mass-marketing, foreign availability—be made available for export without a license to essentially anyone in the world.

The second pending piece of legislation is a proposal to shorten the current 180-day period which Congress has in order to review administration decisions to decontrol computers at certain performance levels—which are usually measured in terms of MTOPS, or millions of theoretical operations per second.

Both pieces of legislation are supported by U.S. computer exporters, but both have also raised serious concerns in the minds of officials concerned with ensuring that our national security export controls really do protect national security. Our discussions today about high-performance computer export controls will help inform the Senate's consideration of this and other legislation.

So I hope our discussions will help illuminate a number of subjects today, but there are a few that I think are particularly important. First, is it possible, clearly and objectively, to make the kind of foreign availability and mass-market status determinations that the computer industry wants to make the basis of removing controls on many high-performance computers?

Second, according to what criteria have decisions to decontrol high-performance computers been made in the past, and how sound has their analysis been?

Third, even if coherent and objective foreign availability and mass-market status determinations are possible, who should make them? Should this be left to the unilateral discretion of the Department of Commerce, or should our national security community, such as the Defense Department, have to agree to decisions to remove export controls of high-performance computers?

Fourth, if foreign availability and mass-market status decisions are inherently subjective, and especially if they are left solely in the hands of the Commerce Department, is it wise to reduce the congressional review period for such determinations? At what point would a shortened review period effectively eliminate congressional oversight of these decisions?

Fifth, how important are high-performance computer controls to problematic Tier III countries, such as China, to the U.S. computer industry? Does requiring licenses for these sales hurt our industry, given that the major industrialized countries are subject to no high-performance computer licensing requirements and most other countries are subject to restrictions only at much higher levels of computing power?

Sixth and finally, what affect would institutionalizing the concepts of foreign availability and mass-market decontrols have upon other controlled technologies? What additional technologies would we have to make available without a license if we wrote these criteria into our export control laws?

This Committee has been closely involved with non-proliferation policy and export controls issues for many years. Senator Cochran's

Subcommittee has also done excellent work in this field in recent years. I look forward to hearing our testimony from four distinguished witnesses today who can help shed light on these and related export control issues as we continue our Committee's involvement with these important national security matters in the future.

Senator Lieberman.

**OPENING STATEMENT OF SENATOR LIEBERMAN**

Senator LIEBERMAN. Thanks very much, Mr. Chairman, for calling this hearing today, which is another in a series that we have been holding over the past couple of years on the subject of export controls. As you have indicated, at issue here is how we in the Congress can balance our desire for the high-tech industry to remain healthy and robust against the risks of allowing potential adversaries access to technologies they may use against us.

Every time we visit this issue, I am struck, as I know most of us are, by the paradoxes of the age in which we live, which are, I suppose, common to all ages of innovation, but particularly this one, where innovation is occurring so broadly and rapidly. On the one hand, technological innovation has significantly improved our lives, of course, by revolutionizing how we communicate and how we live, speeding up the transaction of business and broadening the information, education and entertain options available to us and our children.

Innovations that most of us could not literally have conceived of a generation ago have fundamentally changed our lives, and we are now so immune or so perhaps numbed by the pace of change that the remarkable and stunning very quickly becomes commonplace, even taken for granted.

On the other hand, the precise factors that have improved our lives have also exposed us to new dangers, because however great technology's promise for good, the risk that it will be used for harm is also great, and we have seen this powerfully and painfully in the century just concluded.

This dichotomy is manifestly apparent with respect to high-performance computers. Levels of performance once powerful enough to qualify a product as a supercomputer now reside on top of our desks, indeed, in our children's PLAY STATIONS. Yet the same power that has transformed our daily lives for the better also has potentially dangerous military applications.

So dealing with this paradox in the context of export controls on high-performance computers is particularly complicated and important, because not only does the technology change at head-spinning speeds, it is disseminated at head-spinning speeds. The difficult question before us in Congress this year, posed specifically in the legislation that Senator Thompson referred to, is whether we can find the appropriate balance between economic and technological dynamism and national security.

Mr. Chairman, these are extraordinarily important questions. They are of great consequence to our lives, to our living, and to our national security, and I look forward to hearing today's witnesses and talking with them in the hope that we can shed some light on these issues.

I should say by way of disclaimer at the outset, protecting one of the witnesses, that I do not now, nor have I, to the best of our knowledge, ever been related to Robert Lieberman.

Chairman THOMPSON. I am sure he appreciates that statement. [Laughter.]

Senator LIEBERMAN. He does. I wanted to clear his name here at the outset. He is not accountable for anything I have said or may say here today, but I welcome him and the other witnesses.

Chairman THOMPSON. Well, we welcome all of our witnesses today. We have some excellent ones: Harold Johnson, Associate Director, International Relations and Trade Issues, National Security and International Affairs Division of the GAO.

Mr. Johnson, do you have a statement you care to make?

**TESTIMONY OF HAROLD J. JOHNSON,[1] ASSOCIATE DIRECTOR, INTERNATIONAL RELATIONS AND TRADE ISSUES, NATIONAL SECURITY AND INTERNATIONAL AFFAIRS DIVISION, U.S. GENERAL ACCOUNTING OFFICE**

Mr. JOHNSON. Yes, I do, sir.

I am pleased to be here today to participate in this hearing. My testimony is based on work that we have completed over the last approximately 3 years. We have issued several reports. We are currently doing some work for the Senate Armed Services Committee. That work is in progress, so for the most part, I will not be discussing that, but will rely on work that we have completed.

You have my prepared statement, so I would like to summarize just briefly a few points that are included in that. One deals with our concern that the Executive Branch has not fully assessed the national security risk associated with the export of high-performance computers. Second, I want to talk about how the Executive Branch has determined that export of computers at existing performance levels can no longer be controlled. And, finally, a few observations on post-shipment verification.

Both you and Senator Lieberman have mentioned the balance that we attempt to strike between our commercial interests and our national security interests, and I will not comment further on that, although one of the underlying problems that we see in trying to achieve this balance and manage the risks associated with export of high-performance computers is that the Executive Branch really has not clearly articulated the specific national security interest it is trying to protect at various computer performance levels, nor has it stated how countries of concern could benefit from using such computers.

We believe that without a clear analysis and explanation of the national security interest in controlling the export of high-performance computers, the U.S. Government really cannot determine what militarily critical computer applications need to be controlled or, second, the most effective way of implementing such export controls.

If such an analysis was made, it might lead to a conclusion that the current reliance on MTOPS as the sole measure of computer

[1] The prepared statement of Mr. Johnson with an attachment appears in the Appendix on page 40.

sensitivity would no longer be appropriate. Indeed, with the rapid changes in computing architecture and the growth of what is called distributed computing, new approaches may be necessary to protect the national security interests in limiting potential adversaries' use of these machines in their research and development programs and in their deployed weapons systems.

In this regard, our September, 1998 report had recommended that the Secretary of Defense make such an assessment of the national security threat and proliferation impacts of high-performance computers to countries of national security concern. We thought that, at a minimum, the assessment should state how and at what performance levels countries of concern use computers for military modernization and proliferation activities, and second, what impact such uses have on our national security interests.

I would like to point out that a critical analysis of the national security applications of concern may lead to conclusions that are very different regarding the export control levels that are currently in place. Indeed, the Executive Branch may conclude that significant national security concerns involve computer performance levels that are at even higher levels than are currently controlled, but that analysis simply has not been done, so we do not know that.

Despite not having done the national security analysis, the Executive Branch has relaxed export controls on computers four times since 1993 because it believed that machines at the previously approved levels had become so widely available on the market that their export was uncontrollable, and we fully acknowledge that the computer technology has grown exponentially. There is no doubt about that.

However, it has not been possible for us to adequately assess the administration's justification for relaxing high-performance computer control levels, because the term "widely available" and "uncontrollable," used in explaining the policy change, has not been defined. Commerce has recently defined controllability, and that definition includes the criterion of volume of sales. Nonetheless, the Executive Branch has relaxed controls based on anticipated, not actual, sales.

The Executive Branch established new computer control thresholds based on the technical performance ratings of those processors the computer manufacturers said would be in their next mass-produced processor and on the estimated dates that they would be introduced in the market, rather than on actual volume of sales.

For example, the control levels for Tier III countries announced by the President in July of last year roughly match the expected performance levels of computers using four and eight Intel Pentium processors that are expected to be on the market in July of this year. Last November, we reported on changes in export computer control levels the President announced in July. We found that the administration's conclusion was correct, that the capabilities of high-performance computers and related components, from both domestic and foreign sources, are generally increasing.

This conclusion was supported by evidence that they presented in a report; however, it was true in part because the United States does not generally control the export of computer processor components. Most sources of this supply are U.S. companies.

Our earlier 1998 review showed that subsidiaries of U.S. computer manufacturers dominate the overseas high-performance computer market, but they must comply with U.S. controls. A 1998 study, sponsored by DOD and Commerce, similarly found that the United States had dominated the international computer market, at least in the mid- and high-range performance categories.

Under current regulations, computer processors that perform up to 3,500 MTOPS can be directly exported to civilian end users in many Tier III countries, including China and Russia, and exports of these processors to users in other Tier III countries, such as Israel and Saudi Arabia, are not subject to any MTOPS levels that require a license.

Exports of other key components for systems with four and eight processors are also generally not controlled, and these parts can be shipped to Tier III countries for civilian end users who can then use them to assemble computers.

Just a brief comment on the government's end-use monitoring through post-shipment verifications. While post-shipment verifications are important in detecting and deterring physical diversion of computers, they simply do not verify computer end use.

According to Department of Energy officials, it is quite easy to conceal how a computer is being used, and although it is possible to verify how a computer is being used by reviewing the internal operations of computer data, this is very costly and intrusive and requires some very sophisticated computer analysis.

With that, I will conclude my summary and be prepared to respond.

Chairman THOMPSON. Thank you very much. Our next witness will be Robert Lieberman, Assistant Inspector General for Audits, U.S. Department of Defense.

Mr. Lieberman.

**TESTIMONY OF ROBERT J. LIEBERMAN,[1] ASSISTANT INSPECTOR GENERAL FOR AUDITING, OFFICE OF THE INSPECTOR GENERAL, U.S. DEPARTMENT OF DEFENSE**

Mr. LIEBERMAN. Thank you, Mr. Chairman. I appreciate the opportunity to be here this morning. In my written statement, I have attempted to recap the most important findings from recent IG reviews of the export control processes. Now I would like to highlight four factors that my office believes merit consideration in terms of new dual-use export control legislation. I want to emphasize that these views are ours and do not necessarily reflect those of other IGs or DOD managers.

First, we believe that the Export Administration Act, which expired in 1994, needs to be reenacted, rather than having the government continue to operate under the current patchwork of emergency declarations, other laws and executive orders. However, any legislation in this area is going to send very strong signals to every exporting country in the world, so it is imperative that the law be well-thought out and the entire spectrum of views here be carefully considered.

[1] The prepared statement of Mr. Lieberman appears in the Appendix on page 57.

Second, it is vitally important that the export license review process be properly applied. By this, I mean that it should not be easily circumvented. In accordance with that precept, I urge particular attention to formulation of the control list, commodity classification requests, determinations of foreign availability or mass-market status, and other issues bearing on licensing exemptions. I will return to those specific points in a moment.

Third, we believe that all available government expertise must be brought to bear on export license application reviews. Therefore, the current requirement in Executive Order 12981 for Commerce to refer all dual-use license applications to Defense for review should be made a matter of law by including it in a new EAA.

Likewise, the exporter appeal process on licensing decisions should be formalized in a new EAA and provide for participation by all interested agencies.

Fourth, no program will be credible unless there are viable inter-agency dispute resolution procedures with final adjudication by the President, if necessary. We believe it is particularly important to provide statutory underpinning to the inter-agency dispute resolution process.

Furthermore, we strongly recommend that a new EAA specify that this process be applicable to all inter-agency export control issues, including the composition of the control list, commodity classification determinations, licensing exemptions, etc.

Returning, if I may, to safeguards against circumventing the licensing process, I would like to underscore our conclusion that the current process, wherein a DOD-developed list of militarily critical technologies is integrated into the overall control list, is working reasonably well.

No official, except the President, should be able to override the determination of the Secretary of Defense that an item belongs on the control list. Similarly, it is important for the national security community to be involved in the commodity classification process, which matches a prospective export item with an export control classification number.

Those determinations are extremely important because they indicate whether an item requires an export license for a given destination, and if so, whether it is licensable by Commerce or State. On pages 14 through 16 of my written statement, I describe the joint IG review finding from last year that Commerce was referring very few commodity classification cases to Defense for review. This was occurring despite current policy that requires Commerce to share with State and Defense all commodity classification requests for items or technologies specifically designed, developed, configured, adapted and modified for military application.

Of thousands of requests received in a recent 3-year period, only 12 were referred by Commerce to Defense for review. This is an issue that actually bears on export controls for both dual-use and munitions items. Similarly, I would like to emphasize the need for careful controls over any process for exempting items from licensing requirements because of foreign availability or mass-market status.

Again, we believe that no determination to exclude or drop an item from the control list should be possible without Defense con-

currence, unless the President directs otherwise. We would not support any proposed legislative or regulatory language that would allow, for example, items that would help proliferate weapons of mass destruction to be exported without export licenses, merely on grounds that similar items are available from other sources.

Finally, I think it bears noting that dual-use export license applications made up only 22 percent of the nearly 58,000 applications for export licenses received by the Federal Government last year. Most applications go through the munitions control process, and that is where the most concern about excessive delay and red tape appears to have been warranted.

That concludes my statement, Mr. Chairman. Thank you again for considering our views.

Chairman THOMPSON. Well, thank you very much.

Our next witness is Gary Milhollin, Director of the Wisconsin Project on Nuclear Arms Control. Thank you for being with us.

## TESTIMONY OF GARY MILHOLLIN,[1] DIRECTOR, WISCONSIN PROJECT ON NUCLEAR ARMS CONTROL

Mr. MILHOLLIN. I am pleased to testify before this distinguished Committee, Senator. In my written statement, I have requested that three items be submitted for the record. They are articles that I have recently written. I assume there is no objection to that.

Chairman THOMPSON. It will be made a part of the record, without objection.

Mr. MILHOLLIN. You have requested that I discuss foreign availability and mass-market status, in particular you have asked whether these concepts are useful or not for use in export control implementation or policy.

In order to respond to that question, I took five items that have been controlled for some time by the United States and our allies, and I compared the criteria for mass-market status and for foreign availability status to those items, and I have indicated in my written statement how that turns out.

I believe that all five of these rather sensitive things would be decontrolled under the sweeping language that this bill contains. I am not sure that its drafters intended for this result to occur, but it is of great interest to compare the criteria, for example, to high-precision switches—these are switches that are incorporated into a nuclear weapon firing circuit. Recently, Saddam Hussein tried to obtain 120 of these switches as spare parts for kidney treatment machines.

He did not get them, at least according to Siemens, from whom he ordered them, but he certainly tried. And so, what that shows you is countries like Iraq are still trying hard to procure items that are controlled, and I think if you look at the criteria and you compare it to high-precision switches, these switches would fit that definition. The bill says that if they do, the Secretary of Commerce must decontrol them. It gives him no discretion, and the same is true of many other items that we have controlled for a long time.

[1] The prepared statement of Mr. Milhollin with attached articles appear in the Appendix on page 76.

Glass and carbon fibers are another example; these are used to make the rotors for centrifuges to enrich uranium for nuclear weapons; they are used for rocket cases; they are used for rocket nozzles; they are used for rocket nose cones; they have been controlled for a long time. We apprehended a person here who was trying to send this material to Cairo for use in a missile that the Iraqis were never successful in building. They were building it in cooperation with the Egyptians and the Argentines.

If that had succeeded, then when we deployed our troops in the Gulf War, it would have been a very different scenario. If Iraq had had the kind of missile that it was building with these fibers, history would have been different. So we are not talking just in theory here about dollars and cents. We are talking about actual threats to our troops.

Maraging steel is another item I looked at. Maraging steel, as well, it was one of the few materials that can make high-speed rotors for centrifuges to enrich uranium. Maraging steel is also used in missile applications. We have protected it for a long time. We apprehended a Pakistani who was trying to export this steel to Pakistan some time ago. It, too, in my judgment, would be caught by the sweeping language of this bill.

The other things that I looked at were corrosion-resistant valves. Those are used to resist the corrosive material in uranium enrichment plants. Iraq and Iran, when they go the last step in building a uranium enrichment plant for nuclear weapons, will need lots of these valves. You cannot build a plant without them. That is why they are controlled for export.

If this language passed in its present form, I think these would be decontrolled. High-performance computers also would fall under this category, and the reason for the presence in the bill of these concepts is because the computer industry has pushed for them to be included. I think it would be a very dangerous thing to decontrol high-performance computers just because they are made in large quantities domestically.

We have always used—the United States has always used its highest-performance computers for designing nuclear weapons and for cryptography. It is reasonable to expect other countries to do the same. The Russians, after they illegally imported supercomputers from us—that is, from IBM and Silicon Graphics—announced that they were planning to use those computers to design nuclear weapons after the test ban came into effect—that is, the present moratorium on testing.

So we know these items have great national security significance. To decontrol them under a vague criterion, such as mass-market status, in my opinion, would be a big mistake.

The other concept that you have asked me to discuss is foreign availability. That, too, would, I think, decontrol many things that its drafters did not intend to decontrol. Just for purposes of illustration, I compared North Korean rocket motors to the criteria in the bill for foreign availability. If you look at those criteria, I think you will see that, actually, North Korean rocket motors would be decontrolled; that is, they are foreign-available under the definition in the bill.

The criteria say that for something to have foreign availability status, it must be available to controlled countries from sources outside the United States. North Korean rocket motors obviously are. Lots of countries are buying them. Also under the criteria, the motors can be acquired at a price that is not excessive and they are available in sufficient quantities so that the requirement of a license or other authorization with respect to the export of such item is or would be ineffective.

I do not think the drafters of this bill intended to decontrol motors, but it looks to me as if they have, and they have swept in a lot of other things, as well. I do not think that the definition of foreign availability, as now written into the bill, is really tolerable. It would require the United States to decontrol things that our allies control under regimes that the United States has built up—the missile technology control regime; nuclear suppliers group guidelines—all the regimes that have been built through U.S. diplomacy since World War II.

If we apply this language literally to the things now on the list of those regimes, our government would be required to decontrol a great many of them. This would leave our allies aghast, and it would—well, I do not want to go so far as to say it would make us into a rogue supplier, but it would certainly break our international obligations and it would give a signal to the rest of the world that we really did not care about export controls.

I think the reason that the bill is so sweeping is because it has adopted a principle that really is not sustainable, and that principle is that if somebody else is doing it, we should do it, too. The United States has never followed that kind of a principle in our own actions or in our diplomacy toward other countries.

I had the dubious honor of being on CNN a lot during the Gulf War, and testifying before Congress about scuds and about other things that turned out to be a big surprise to the world. One of the things I remember was the Israelis holding up pieces of scuds that they had found in the debris of destroyed buildings in Tel Aviv. They found German markings on some of those scud fragments.

If you adopt the idea that our industry should be able to sell anything any other industry should sell, then you have to accept the idea that somebody is going to hold up a fragment with a U.S. marking on it. I cannot believe our industry really wants that to happen.

We also should remember that a scud supplied by Russia and enhanced in range by Germany killed our troops in Saudi Arabia, sleeping in their barracks. I cannot believe that the United States would want our industry to be able to participate in the market that caused that to happen, even if it means losing sales and even if it means that the countries like Iraq, who are doing these things, can get it from somebody else. You simply cannot go down the road in which you say, "If somebody else is going to do it, our guys should be able to do it, too," unless you are prepared to sustain the criticism and the shame that would result from seeing your products used to achieve the things that were achieved by Saddam Hussein.

So I think that is the main problem we are getting into, is that we have these arguments that if somebody else is going to do it,

we should do it. That is not a position you want to take. It would make export controls, as a practical matter, impossible in the world if everybody adopted that point of view.

The last thing I would like to mention here is that in the latter portion of my testimony—other portions of my testimony refer to things that have been covered by other witnesses—in the last section of my testimony, I recommended that one of the ways around the dilemma that Senator Lieberman mentioned would be simply to use transparency; that is, if we put more light on the export control process, I think it would cause us to do a better job. It would allow our government to deny things that are dangerous and allow legitimate trade to go forward.

I have attached to my testimony a proposed list that is a first step toward more transparency. I have attached a list of 50 Chinese companies that I believe, based on very reliable open-source information, are dangerous buyers for high-speed computers and for other dual-use technologies. I recommend that the Committee submit those names to the State Department for review; and if the State Department agrees that they are dangerous buyers, then they should be put on the warning list to U.S. exporters.

I must say that I am glad that Dan Hoydysh is here today, because when I interviewed him for an article in *The Washington Post* that I wrote not too long ago about this subject, he agreed that the industry would welcome more guidance on who the bad guys are, who are dangerous buyers. I am not suggesting this list as an embargo list. I am suggesting it simply as a warning list; that if an exporter gets an order from one of these buyers, the exporter should check it out.

What I am recommending is that it should trigger an export license application. I am not saying that these recipients should be denied U.S. exports. I am just saying that it merits a look if they are going to buy something that can conceivable contribute to a nuclear weapon or missile program.

Thank you very much.

Chairman THOMPSON. Thank you very much.

Our last witness will be Daniel Hoydysh, Co-Chair of the Computer Coalition for Responsible Exports.

Mr. Hoydysh.

## TESTIMONY OF DAN HOYDYSH,[1] CO-CHAIR, COMPUTER COALITION FOR RESPONSIBLE EXPORTS

Mr. HOYDYSH. Thank you very much, Mr. Chairman, for the opportunity to testify on this important subject. I have submitted my full testimony and in the interest of time I would briefly summarize a few highlights. Before I get to that, I would like to make two points in response to what my good friend Gary has said.

One, I believe that in the Export Administration Act, no decontrol is automatic. There are provisions for presidential overrides, and that is something that at least ought to be looked at carefully. Two, we do not advocate decontrolling computer exports to any of the rogue or terrorist nations.

[1] The prepared statement of Mr. Hoydysh appears in the Appendix on page 102.

I would like to make a couple of other major points. Something often gets lost in the heat of debate is that our industry cares very deeply about national security. We are responsible citizens of the United States and would not do anything to jeopardize the security of the country in which our workers and families live. We believe, however, that our national security is directly dependent on the technological leadership of the U.S. computer industry.

To maintain this leadership, we must compete in the global market and we must export. Exports equal profits. Profits are used to fund R&D, and R&D drives technological leadership. The U.S. computer industry is the world leader and we want it to stay that way. But we do have substantial foreign competition. If I accomplish nothing else in this testimony, I would like to lay to rest the myth that there is no foreign competition for the business computers that we are talking about in terms of decontrol.

According to a recent report by the International Data Corporation, four of the top 10 server vendors are foreign. They include companies from Japan, Germany, and France. We are not proposing that controls on supercomputers be abolished. Again, I would like to dispel the myth that this debate, is about the export of supercomputers.

We are proposing that restrictions be eased on business servers with two, four, and eight processors. These machines are the basic building blocks of the new digital Internet economy.

Supercomputers, such as those used for sophisticated nuclear simulations, consist of thousands of processors. For example, in the Sandia Labs, Intel has installed a machine called the ASCII–RED, which has 9,632 processors. Recently, the French Atomic Energy Commission ordered a supercomputer from Compaq for simulation programs to ensure the reliability and safety of the French nuclear stockpile without the need to conduct new nuclear tests. The Compaq system will use 2,500 alpha processors, will take a year to install and operate roughly at 5 million MTOPS. Now that is a supercomputer.

Finally, Fujitsu recently announced that it would provide the world's most powerful supercomputer to the Toyota Corporation for automobile design purposes. In its maximum configuration, this system has 512 vector processors and can operate at over five million MTOPS. And please note that this system is replacing a U.S.-made Cray supercomputer.

While we do not come to praise the export control system, we certainly do not come here to bury it. We support effective export controls. However, we think the current system is broken. It is broken because it is inefficient, it is ineffective, and it is counterproductive.

It is inefficient because it takes too long to process export licenses. The reviewing agencies do not have the resources, either in personnel or equipment, to do the job.

It is ineffective because it is largely unilateral. Our controls are much stricter than those of our foreign competitors. It is counterproductive because it wastes government and industry resources in trying to control the uncontrollable. Therefore, efforts to police truly sensitive items are diluted, and this undermines national security.

Dr. Steve Bryan, a respected expert on export control, who served in the Reagan Administration and is in large measure the architect of a lot of the systems that we have, described the current export control system best when he testified before the House Armed Services Committee last year. And I quote: "I do not think there is any point in having an export control system that tilts at windmills. I think you have to have controls that makes sense, that can be enforced, and that protect our strategic interest."

Another quote that is right on point in terms of evaluating the export control system is contained in this report which I recommend to the Committee, "Final Report of the Defense Science Board and Task Force on Globalization and Security." The basic premise of this report is that rather than trying to restrict exports of widely available technology, we have to concentrate on trying to run faster than our adversaries.

And a quote that is particularly on point here from this report, "Protection of capabilities and technologies readily available on the world market is, at best, unhelpful to the maintenance of military dominance and, at worst, counterproductive by undermining the industry upon which U.S. military technological supremacy depends."

So what do we need? We need to fix the export control system. We need an efficient, effective, and credible control system that reflects competitive and technological reality. In the short-term, we would like to reduce the congressional review period from 6 months to 30 days.

We also need to increase control thresholds now to reflect advances in technology and competitive reality. In the long-term, we want to work with the Executive Branch and the Congress to develop an effective approach to controlling exports that fit national security concerns of the 21st Century. This would require a thorough evaluation of the threats posed to the United States in this century, the effect of globalization of markets technology and knowledge, identification of choke-point technologies and techniques for how we can run faster than our potential adversaries.

Thank you very much.

Chairman THOMPSON. Well, thank you very much. This testimony, from all of you, really lays excellent groundwork for our discussion today, and it is a classic case of two competing interests. Both of them are valid interests, but I was just thinking yesterday about what was happening here in the process, as we are trying to balance our commercial interest and our competitiveness—and keeping our own capabilities where we want them to be—versus national security.

It seems to me all the movement—we can argue about this later—but it seems to me all the movement seems to be on the side of the export industry. The administration, of course, periodically and quite often increases the MTOPS levels at which computers can be sold without a license. They were changed in April, 1994; October, 1995; July, 1999; February, 2000; and again in August, 2000, as I understand it. So we are moving in that direction.

We have gone from 2,000 MTOPS for military use in October 1995 to conceivably as much as 40,000—according to what some industry folks were saying earlier this year—in August 2000. You might ask, compared to what, because some computers have

MTOPS levels in the millions, but we are moving certainly in that direction. Congress has a right to review whether or not we are moving too fast or perhaps not fast enough. Up until, I believe, 1999, Congress had what was in practice an 18-to-24 months review period. So until recently, we had 2 years. Now we have got 6 months.

Now it is being suggested by proposed legislation that we reduce that review level to 30 days. I think it is important to keep in mind this has nothing to do with the holding up of an individual export. It just has to do with whether or not exports at particular levels even need licenses at all. So that may be reduced.

Then we have the Export Administration Act, which interjects new concepts in terms of statutory law, derived and greatly expanded from what previously were only to be used by exporters who were denied licenses and so forth. Basically, the concepts and statutory law of "mass-marketing" and "foreign availability" are new, and this bill would propose to take whole categories of items, even above the MTOPS levels that are allowed, out of the control regime completely on the basis that everybody supposedly has got or can get them anyway.

So there is quite a bit happening here, and it seems to me that it is all moving in the same direction. Now, perhaps the case could be made that this is good and that it is valid. If we err too far on one side, we are perhaps hurting ourselves somewhat commercially. If we err too far on the other side, we are perhaps hurting ourselves somewhat from a national security standpoint.

And one of the things that concerns me from your testimony, Mr. Johnson, it that as the administration makes this determination as to when and how much to raise these MTOPS levels, they are not making any kind of national security assessment. It is strictly based on what is deemed to be controllable or uncontrollable. Is that correct?

Mr. JOHNSON. That is basically correct. They have not done a national security analysis to know what impact the relaxation or the change in the control levels might have on our national security and how the recipient governments, may use the computers in their military modernization programs, and we think that that is a serious deficiency.

Chairman THOMPSON. And the GAO, of course, has been dealing with this for some time, and you have had occasion to criticize the administration in times past because of some of the analyses and studies that they were relying upon, such as the Stanford analysis, in making their decisions to raise the MTOPS levels.

Mr. JOHNSON. Correct.

Chairman THOMPSON. So the justification for their decision is one of the things that we can look at in trying to determine where we should go and how fast we should go as an administration is increasing these MTOPS levels. I am certainly not arguing that they should not be increased. But the question is to what levels and how fast? Reasonable people can disagree on that, but one of the benchmarks that I think we can look at is the nature of the material they are relying upon in order to make those increases.

The fact of the matter is that in times past, in dealing with these nebulous terms of foreign availability or uncontrollability or what-

not, they have relied on studies that you did not feel supported the conclusions that the administration came up with. Is that not accurate?

Mr. JOHNSON. Well, it was unclear whether the studies really supported the conclusion, because the studies themselves lacked empirical data to support the conclusion that was in the study. And mainly in the area of controllability, the study simply did not have sufficient data to come to a conclusion that—I think the initial Stanford study indicated that computers at 4,000 to 5,000 MTOPS were, at that point in time, which was 1995, uncontrollable.

There simply was not data to support that, so whether or not they came to the right conclusion, we did not reach that conclusion. They may have serendipitously come to that conclusion properly——

Chairman THOMPSON. It would seem to me, that there's so much anecdotal evidence—so many statements that we hear from time to time about the clear availability of computers when you walk into Radio Shack, etc. If that is so clear, you think they would be able to come up with a study that the GAO would say at least is a valid study in order to support that conclusion.

Mr. JOHNSON. Well, at certain MTOPS levels, I am sure they could do that. But, we are talking about MTOPS levels that are generally higher than what you would find at Best Buy or Radio Shack.

Chairman THOMPSON. And the administration deals not just in terms of what is perceived to be the case at the time of the analysis, but also of the anticipated availability.

Mr. JOHNSON. That is a major concern that we have had in the last couple of—in our current study, as well as the study that we did of the President's July, 1999 report; that the decision was based on anticipated mass-market, rather than on what existed at the time the decision was made.

Chairman THOMPSON. Correct me if I am wrong, but it seems to me that this anticipated mass-market, in turn, is based upon what our domestic producers intend to manufacture in the future.

Mr. JOHNSON. That is correct, what they say they are going to produce and when they are going to——

Chairman THOMPSON. So foreign availability——

Mr. JOHNSON. That is not a factor in that kind of judgment.

Chairman THOMPSON. Well, is controllability?

Mr. JOHNSON. Well, projected controllability, yes; but suggesting that because they are going to have a particular type of processor available 6 months hence does not necessarily mean that we should be decontrolling now in anticipation that the processor will be available.

If you are looking at what is mass-market, I mean, that is something that exists, you can count—I do not want to put numbers on what the criteria ought to be, but you can determine what a mass-market is, rather than what is anticipated.

Chairman THOMPSON. All right. Let's make sure we are talking about the same thing. Let's talk about not what it ought to be or what you think it should be. Let's talk about what the current situation is, as it is applied now, as these determinations are made to raise these MTOPS levels. It is based in part on anticipated levels.

Mr. JOHNSON. That is correct.

Chairman THOMPSON. And that, in turn, helps to reach a determination as to what is going to be controllable.

Mr. JOHNSON. What the control levels ought to be.

Chairman THOMPSON. Ought to be?

Mr. JOHNSON. Right.

Chairman THOMPSON. So it sounds to me like a self-fulfilling prophecy. If your supposed ability to control or the controllability of a type of item is determined primarily on the basis of what our domestic manufacturers intend to produce, that seems to be a self-fulfilling prophecy. I mean, that begs the question: Should they be controlled, should they be available? And certainly we have something to do with that. That is my assessment.

I mean, that is my comment. Do you have any problem with that?

Mr. JOHNSON. I think that is a fair analysis, yes.

Chairman THOMPSON. All right, sir. One more thing, on the reduction of the time of the analysis. You mentioned you were doing some work for Armed Services.

Mr. JOHNSON. Right.

Chairman THOMPSON. Is part of that work an analysis of the last MTOPS level proposal, I will call it, of the administration's——

Mr. JOHNSON. Yes.

Chairman THOMPSON [continuing]. Increase?

Mr. JOHNSON. Yes. It is an analysis of the President's February, 2000 announcement that——

Chairman THOMPSON. All right. I will just ask you, do you have any anticipated date of release of that?

Mr. JOHNSON. Well, probably within 4 to 6 weeks.

Chairman THOMPSON. Probably within 4 to 6 weeks.

Mr. JOHNSON. Right.

Chairman THOMPSON. So the GAO does that. Do you traditionally do that? I mean, is this your first time?

Mr. JOHNSON. No, we have done this twice now.

Chairman THOMPSON. OK.

Mr. JOHNSON. And it is anticipated—we have had some discussion at the staff level that GAO might be requested to do this on a routine basis.

Chairman THOMPSON. All right. Now, my information here—you correct me if I am wrong—that from September 1993 through October 1995, the review time period was in practice for 18 to 24 months. From July 1999 till now, it is 6 months. The proposed legislation would cut that review time back to 30 days. As the entity that is doing that review, what is your opinion of that?

Mr. JOHNSON. I think 30 days would reduce unreasonably the amount of time the Congress has to look at the President's report. In terms of our work, we do not require the full 6 months. I mean, we have been—we have had this study underway now for probably 6 or 8 weeks, but if we had immediate access to information from the Commerce Department when the announcement is made, that would shorten our time frame.

So I am not suggesting that it needs to remain 6 months. It can be shortened from that, possibly, but I think 30 days would be overly-restrictive for the Congress to deal with it.

Chairman THOMPSON. So you have had this review underway for about how long so far?

Mr. JOHNSON. Probably about 8 weeks.

Chairman THOMPSON. And you anticipate, you said a few minutes ago, how many more weeks?

Mr. JOHNSON. Well, I would say 4 to 6 weeks, until the report is published; but, I mean, under other circumstances, that time could be shortened to some extent.

Chairman THOMPSON. All right. Now, that is just your time to produce a report. That is not congressional review or analysis or hearings or anything else.

Mr. JOHNSON. That is correct. That is our time.

Chairman THOMPSON. I see. All right. Well, I have taken up more than my time.

Senator Lieberman go ahead.

Senator LIEBERMAN. No problem. Thanks, Mr. Chairman, very interesting discussion.

Mr. Milhollin, let me start asking you a question that goes back to something you said and at least helps me get into this discussion and the competing interests and values involved here. At one point, you quoted one of the common responses to this dilemma, which is, "Well, if everybody else is doing it, we should, too," and you were critical of that.

In one sense, of course, you are appealing to America's better nature. We like to believe that we are not like everyone else, both in terms of values and hopefully the extent to which we are prepared to protect our national security interest. But I want to just start my discussion with the panel by asking you whether that criticism of that response, if everyone else is doing it, we should, too, you mean it comprehensively?

In other words, if you were convinced that, in fact, some high-performance computer was really quite widely available—let's assume for a moment that the facts were proven—but that it really could be used to endanger our national security, would you still say we should not do it—and, of course, we all remember those moments in the Gulf War when the shards of different systems were held up—to avoid in some measure, to having blood on our hands?

Mr. MILHOLLIN. I would answer your question by saying first that it is not simply a moral position I am taking, although I think it principally is—that is most of it—but it also is a functional point. If every member of the regime operated on the assumption that everybody else was going to sell anything he did not sell, it would be pretty hard to have a regime.

It is really a question of keeping the faith. Somebody has to be the leader. It has always been the United States. We have gone to our allies and said, "Here is what we think ought to be controlled." We did that in COCOM. We said, "Here is what we think is important. Here is what we think ought to be controlled. We are going to control this and we hope that you will join."

In fact, that was President Bush's approach to the Gulf War. I mean, we did not wait for everybody else to decide, "Yes, we are going to roll this back." President Bush said, "We are going to roll this back," and then he invited everybody else in to come in and help out.

Senator LIEBERMAN. Right.

Mr. MILHOLLIN. As a practical matter, that is how you have to do it. So it is not just a moral issue. It is also a practical question of how you achieve things diplomatically, and unless somebody is going to step out there and take the lead, nothing happens.

Senator LIEBERMAN. But what if they do not follow on these commercial questions, on the sale of high-performance computers?

Mr. MILHOLLIN. They will never follow 100 percent.

Senator LIEBERMAN. Right.

Mr. MILHOLLIN. What you have to do is decide how much is enough. Under COCOM, the Russians could always get things.

They could always—if they wanted something enough, they could figure out a way to get it. But, often, they did not get training; they did not get manuals; they did not get spare parts; and 6 months later, it wound up being a piece of junk because they could not service it. They admitted that after the Cold War ended and there was sort of a look at how COCOM had functioned.

COCOM was a giant success not because it was airtight—we had the *Toshiba* case. We had lots of situations where people violated COCOM and undermined our industries, but overall it worked, and if you visit the former Soviet Union now, you can see the impact it had on their infrastructure.

Go to Russia and try to make phone calls from one village to another. COCOM really did have a big negative impact, on Russia primarily, even though it was not airtight; that is, it did not work 100 percent. So you will always have situations where somebody will not follow. What I am worried about is that we have to maintain the faith here or we will not have anybody following. That is really the question.

It is not the question of whether you can get 100 percent compliance. The question is, if you decide that we are going to send the world a message that we do not care about this anymore, then you are certain to get zero compliance.

Senator LIEBERMAN. That is very interesting. So is it fair for me to conclude that what you are saying is that even if a particular dual-use item is available in foreign markets to foreign countries, to countries that we would put in one of the tiers that we worry about that you would say that we should still try to control its export from here, even if that does some damage to our high-technology companies, because the effect will be that we will make it harder for those who would threaten us to get hold of it; so that this is a balance and maybe there will be some economic damage here, but when you balance it against the national security threat, because we are the leader, it is worth it.

Mr. MILHOLLIN. Yes, it is worth it. You are going to take some hits. You are going to take some losses, but nothing is free.

Senator LIEBERMAN. Right.

Mr. MILHOLLIN. So you have to be willing to say to the U.S. industry, "You are going to lose some sales here and there from this system, but overall, it is worth it."

There was a recent case in which a rather sensitive Chinese company was tried to buy a five-axis machine tool from us and they did not get it. I must admit, because I have an activist hat, that

the deal happened to be exposed in the newspapers and it made it much harder to approve.

Well, I was told that an European company filled that order. I suppose that pro-export forces would say, "Well, there is an example. You know, you made it hard for us to approve this. It got held up. We did not approve it and then the Chinese got tired of waiting and they bought it from somebody else." Well, I think that is a victory. If this company is going to make missiles and military aircraft at this plant, and they want to do it with a German or a French or a Swiss machine tool, I think it is better than having them do it with ours, because if we had sold that machine tool, then the message would have been clear, because this was a very dubious end-user. The message would have been, "Look, guys, if America—if we are going to do it, then the signal is, we really do not care that much."

Senator LIEBERMAN. So, your reasons are both moral and functional or practical?

Mr. MILHOLLIN. Yes.

Senator LIEBERMAN. Both, we do not want that on our hands, but also that, so long as we exercise some restraint, even though in that case that Chinese company got what it wanted, that we send out a message to the world that makes it less likely that this stuff will be more widely available.

Mr. MILHOLLIN. That is right. The next time the Iranians want something and we go to a European company and say, "We discovered that the Iranians are about to buy this from you and we think you ought to stop it," they are not going to say, "Yes, but what about the machine tool you guys just sold to the Chinese?"

Senator LIEBERMAN. Right.

Mr. MILHOLLIN. And, believe me, that happens. It happens all the time. So unless you are willing to be clean in your own behavior, you are not going to get anywhere with anybody else.

Senator LIEBERMAN. Mr. Lieberman, from a Defense Department perspective—I know you are not here to speak for the Defense Department—but from within the purview that you have, how do you react to that standard that Mr. Milhollin establishes? I know from your testimony that you obviously feel that the Department of Defense should be involved more in these export control decisions, but he is posing a tough standard, I think. I am interested in your reaction to it.

Mr. LIEBERMAN. I believe that it serves no purpose to have any export control regime if we do not enter into that process with expectations of having a pretty tough standard. I would point out that when a buyer decides to purchase a product, they make their choice based on what they think the best product on the market is and perhaps best price.

So what we seem to be talking about here is selling products that could create national security threats, and we are providing the best product at the best price to whomever that other party is, which, to me, creates a problem. You used the word balance in your opening statement, and clearly that is what we are talking about here.

I believe that the current process is somewhat inefficient, but the inefficiencies in the process can be fixed, because those are mostly

bureaucratic procedures and resourcing questions that can be addressed.

Senator LIEBERMAN. In some of the delay involved.

Mr. LIEBERMAN. Yes. Absolutely.

Senator LIEBERMAN. In reaching a decision.

Mr. LIEBERMAN. But the basic feature of the existing review process, which is multi-agency deliberation over the wisdom of granting a license, I think is really the thing that we need to retain. That is why I said that we need to be extremely careful about exempting products or classes of products from the process, because I think ultimately the process needs to be applied to anything where there is even a smidgen of a national security implication.

That does not mean when something has to go through the process, that a license is going to be denied. In fact, very few licenses are denied. So I think that is an important distinction that I would try to make.

Senator LIEBERMAN. I would take it that you believe the bill before the Senate, S. 1712, is somewhat imbalanced, that it tilts too much toward the commercial interest.

Mr. LIEBERMAN. Yes. That has been our testimony to the Senate Armed Services Committee and there is some of that in my statement today.

Senator LIEBERMAN. Mr. Hoydysh, how about Mr. Milhollin's standard? I presume you find it too stringent and, in some senses, unrealistic.

Mr. HOYDYSH. Well, Senator, before I get to that, could I just take one point to deal with a factual issue that Senator Thompson raised earlier about the review period going from 180 days to 30 days?

Senator LIEBERMAN. Yes. Sure.

Mr. HOYDYSH. Senator Thompson mentioned something about an 18-month or 2-year review period. In my knowledge, there was no review period before the current 180-day review was enacted in 1997. I spent 7 years in the Reagan Administration (from 1982 to 1989), in the Export Control Bureau, and there was no congressional review period whatsoever. So I am not sure what it is factually that the Chairman is referring to.

Chairman THOMPSON. I think the difference has to do with the policy and the law. As I look at this, my chart indicates that the 18 to 24 months was the policy during that period of time. The 6 months was put into law, so——

Mr. HOYDYSH. Fair enough.

Chairman THOMPSON. Whatever conclusions we want to draw from that, I think that is what the situation was.

Mr. HOYDYSH. To get back to the standard, Gary raises a very difficult question. Moral questions are always very difficult. I think the answer is in how you draw the balance and where you actually draw the line. We could all agree that no one wants to sell items to someone who is going to do damage to this country.

In fact, the system, as currently structured, has safeguards built into it.

Senator LIEBERMAN. Would you say that even if the item is available from other countries? In other words, that is part of the challenge that is posed here.

Mr. HOYDYSH. Senator, we are not permitted under current law to sell to an end-user in China or anywhere else if we have knowledge that that end-user is going to use that equipment for proliferation purposes.

Senator LIEBERMAN. Right.

Mr. HOYDYSH. Most of the enforcement cases that have been handled over the years generally result from tips that are provided by the industry. So, with a few exceptions which have been publicized in recent years and which are under investigation the industry, I think, has a very good record on that.

The real question is where do you draw the line and at what level do you have to either control things by having the government review each export, and where do you allow industry to make that ultimate choice?

Senator LIEBERMAN. That is exactly the question. So, in other words, if Mr. Milhollin has drawn the line in one place, which is that even if a particular dual-use item is available in foreign markets, we ought not to be selling it, if we are reasonably confident that it is going to be badly used, not only for moral reasons, but because we set a standard. So that is a tough standard. Where would you draw the line yourself?

Mr. HOYDYSH. I would not remove the requirement that if there was knowledge that the equipment was going to be used for some inappropriate purpose, that we should not sell.

Senator LIEBERMAN. Forgive me for interrupting, but how do we enforce that? That is a reasonable standard, but how do we make it real?

Mr. HOYDYSH. Well, in some cases, it is easier to enforce. I mean, most of the companies—most of our companies that deal in countries like China, for example, have a fairly complex process in terms of searching for customers. Generally, we just do not go off and sell someone 50 boxes of something and leave it there. Generally, it is involved in providing an airline reservation system or some kind of banking system.

So we have a good idea of what the end-use is. If somebody comes to us and says, "I want you to help me automate the missile factory," we will not do it. In fact, we are not permitted to do it. So there is just, in the normal way of doing business, a certain amount of security in how these products are used. Where it begins to break down is if you have a product like the Macintosh PowerG3 or whatever the nomenclature is, and you want to sell that in a Radio Shack or a Best Buy-type environment in China, where you provide 50 of these to people who walk in off the street, as a practical matter, it becomes almost impossible to monitor where those sales are going to go to.

There is a big difference between delivering 150 boxes to the People's Liberation Army missile base and delivering them to Best Buy. So, I mean, these are just practical issues and, at some point, it simply becomes impossible to actually do it in practice, no matter how well-intentioned the idea is.

Senator LIEBERMAN. In your testimony, you talked, and we all have, about the extraordinary advances, rapid advances in the capability of high-performance computers. Now, as you mentioned, we are into millions of MTOPS. But isn't it true that some of the appli-

cations that we have made that are most significant of high-performance computers have been done at much lower MTOPS levels, some under the limits we are now establishing?

The question is, is the MTOPS number an adequate and appropriate standard to use?

Mr. HOYDYSH. It is becoming clear to people in industry and people at the Defense Department, as well, that MTOPS alone may not be an adequate standard to measure the strategic significance of a computer.

The computers that we are talking about are basically designed for transaction processing; that is why they have many processors, so that Visa or a bank can handle 100,000 phone calls a minute coming in. They really are not specially designed to be used for military applications or for nuclear weapons or any of the prohibited purposes.

That is not to say that they cannot be used for prohibited purposes, because any computer can be used for that, but they are really not designed primarily for that. There may be other technological parameters, in addition to MTOPS or in place of MTOPS, to better measure what it is that we are concerned about. I understand that the Commerce Department Technical Advisory Committee is looking at this and also the Defense Department is looking at this.

Senator LIEBERMAN. Well, that is a very important point and obviously we would be interested in the results of that inquiry, because that may help us come to a more practically-effective standard.

Mr. Johnson, you said some things in your testimony I want to just ask you to amplify a bit which interested me, which was that the Executive Branch has not clearly stated what the national security interest is in controlling exports of high-performance computers, and, in a way, this may touch on the last point of exchange with Mr. Hoydysh, that maybe MTOPS are not the appropriate, certainly not sole standard, for determining what should be exported. I just wonder if you could talk about that a little more.

Mr. JOHNSON. Sure. Yes, we have basically come to the same conclusion. In fact, another study that we have been requested by the Senate Armed Services Committee to do is to follow these studies that are ongoing within industry, as well as Department of Defense and Commerce, on what other standards might be appropriate, other than MTOPS, because MTOPS clearly does not address the concern that has been raised about distributed computing; in other words, where you can line up several computers and tie them together and distribute the calculation process among them.

It just does not address that issue. But in terms of our concern that the Defense Department has not clearly addressed the national security interest it is trying to protect, obviously, they have looked at how computers are used in their own processes, and have come to conclusions that there are a number of applications that are important applications that are required from a very low level of performance to a high level of performance.

Our concern is that there are a number of applications, computer applications, that are of such critical importance that we need to

do whatever is required to protect our ability to deal with those applications, and that is what the Defense Department has not done. They have been requested now, through legislation, to do that.

I think the National Defense Authorization Act of last year laid that requirement on. My understanding is that they will have that study completed in August, and hopefully that will resolve that concern; but what we have held is that if they looked at all the applications that are of extreme importance, they may come to a conclusion that the level that we are trying to control computers at now just does not make any sense. It may be much higher than what we are trying to control. It may be lower, too, but——

Senator LIEBERMAN. It may be lower, if we add in other standards, other factors to consider.

Mr. JOHNSON. Yes. Right.

Senator LIEBERMAN. Could you give us an example of one or two other factors that, to you at this point, seem relevant besides the MTOPS standard?

Mr. JOHNSON. Well, just basically, looking at the architecture of the computer, what it is designed to perform, and I am not a technician myself, but what the computer is designed to—the application is designed to perform—would be one way of measuring it. I know it is fraught with all kinds of problems and we have already had some discussions with industry on that, but——

Senator LIEBERMAN. Mr. Johnson, a final question. You also said that you thought that two very central terms to this discussion, particularly of the legislative proposal before Congress, are not adequately defined; that is, the terms widely available and uncontrollable.

Mr. JOHNSON. Controllability, yes.

Senator LIEBERMAN. Controllability. So tell us what is lacking and, if you had your druthers—you were drafting—how would you define those two critical terms?

Mr. JOHNSON. Well, I basically—the Commerce Department, in response to our raising that issue, did define controllability, and I think their definition of controllability is not a bad standard. Unfortunately, they did not apply that standard. But in defining controllability, they included factors like the volume of sales, and I think that is a critical aspect.

I do not want to try and attach numbers to it. It is very difficult to do that, and it would differ depending on what the component is. But the way Commerce defined controllability to us, which implies widely available, it is not a bad standard, and I think we have included that statement in our prepared testimony.

Senator LIEBERMAN. OK. Thanks, Mr. Chairman. I am going to give it back to you.

Chairman THOMPSON. Thank you very much. We have been looking at the front end of the process as we increase the MTOPS levels and we propose to shorten the amount of time Congress has to review, but we have also touched on the back end of the process—and that is, who winds up with these so-called supercomputers?

Everything we are doing is based on an assumption that we have something to do about that or that we can in some way affect that or control that. In our tiered process, for Tier III countries such as China, we have an export-license free computer performance level

for military use and one for civilian use. But, in listening to you, I was reminded of a point that the staff had made earlier to me, and that is about the difficulty in dealing with a country like China, and being able to rely upon the proper end-use of an export to a civilian company with assurances that it will not have military use.

There is also a Russian angle to this problem. In 1996, both Silicon Graphics and IBM illegally exported high-performance computers to Russian nuclear weapons laboratories without licenses. They claimed that they had not known that these facilities were weapons labs, even though the two locations, Chelyabinsk 70 and Arzamas–16—which I have been to, by the way—should have been well-known to anyone with any knowledge of the Russian nuclear program. I do not know. It seems like I knew about Arzamas a long time ago.

Anyway, after these illegal sales were revealed, the head of the Russian program bragged that he had planned to use these machines to design nuclear weapons. I guess it is impossible to keep something like that from happening every once in a while. But, again, we need to look at the process, because we are relying upon industry to make the initial determination of whether a Tier III end-user is civilian or military.

That might be more than industry really has the capability of doing. It might be an unfair burden to be putting on them. Some in industry might be tempted to hedge. In the China situation, there was a period of time there when they were allowing no post-shipment verification checks at all. Isn't that true?

Mr. JOHNSON. That is correct; yes.

Chairman THOMPSON. A period of time, up until the agreement in, what, 1998?

Mr. JOHNSON. June 1998.

Chairman THOMPSON. June 1998. They would not allow us——

Mr. JOHNSON. Right.

Chairman THOMPSON. Here we are trying to export these computers to them, and they would not allow us to check with regard to post-shipment verifications. Then, we supposedly entered into an agreement with them in 1998 that would allow post-shipment verifications. Is that correct?

Mr. JOHNSON. Yes, that is correct, but they had to comply with certain requirements that were laid out in the agreement, and not all high-performance computers that were shipped without a license to the civilian sector complied; so that was also a problem.

Chairman THOMPSON. Have you seen this agreement?

Mr. JOHNSON. No.

Chairman THOMPSON. Who has seen this agreement?

Mr. JOHNSON. Well, it is a classified agreement, and we do have access to classified information, of course; but I have not personally read the agreement.

Chairman THOMPSON. Well, are you familiar with the Cox Report's reference to this?

Mr. JOHNSON. Yes, I am.

Chairman THOMPSON. Is it not true that the Cox Report says there is such an agreement; that the administration would not release the agreement because the Chinese would not allow it; and

that the Cox Committee had reviewed the agreement and found it to be wholly inadequate?

Mr. JOHNSON. I read that in the Cox Report, yes.

Chairman THOMPSON. Do you know of any national security reason why the American people should not see the agreement that allows us to do post-shipment verifications for high-performance computers?

Mr. JOHNSON. Not to my knowledge.

Chairman THOMPSON. Does anybody else know who might have access to this agreement or know anything about what is in the agreement?

Mr. JOHNSON. No, sir.

Chairman THOMPSON. Well, I think that this is something that we might want to inquire about, because a large part of what we are doing is supposed to be in reliance upon the fact that computers that are sent for civilian purposes, for example, do not wind up in civilian hands. If the Cox Committee has concluded that this agreement is wholly inadequate and the administration will not release the agreement because of Chinese objections, I think that raises serious concerns. I think it might be a good idea perhaps to inquire of the administration whether they would let us review that agreement to see whether there are any legitimate national security purpose for withholding portions of it, and that certainly can be dealt with. But I see no reason on something like a post-shipment verification arrangement and the extent to which we should be able to rely upon who the real end-user is going to be in any given situation, why this information should be withheld from the American people.

Mr. Hoydysh, what is the economic effect of what we are talking about? I have seen numbers that seem to indicate that, right now anyway, there are only a limited number of high-performance computers sold to Tier III countries. Obviously, you have large domestic sales. You have large international sales, most of which are not controlled because they are not of a certain level.

Can you give us some feel in terms of numbers of sales or potential sales that we are talking about—again, not that you cannot export to Tier III countries, but that for some items you have to go through a license process? I guess you have the delay issue and then you have the denial issue, both; but can you give us some better idea as to what the commercial impact of this is for the computer industry, which clearly has millions of sales domestically and internationally?

Mr. HOYDYSH. Senator, in terms of the absolute volumes and the absolute sales, this is not an overwhelming market for us at this time. Depending on the company, depending on how you slice it, it is anywhere from 10 to 15 percent of company sales; that is all of Tier III. Now, China is the fastest-growing market in Asia, and I believe is, after Japan, the second-largest market. It certainly has tremendous potential.

We do not—again, just to clarify—we do not object to licensing requirements for truly high-end systems. In fact, I do not believe that any truly high-end system has ever been approved to China. What we are concerned about is competition at the lower end with

commodity machines which are available from a wide variety of sources, including from companies in China.

The problem is one of delay, even without licenses, you have a 10-day delay. But, on top of that, the United States is the only country that requires our vendors to get an end-user certificate from the Chinese government; so that a comparable sale from anyone else would not require an end-user certificate, and this is a bureaucratic process that can take anywhere from 2 to 6 weeks.

Chairman THOMPSON. Have you been following any of the hearings and debates that we have been having here on the PNTR with regard to China, and national missile defense? And are you familiar with the testimony that we have heard from this table, from our intelligence officers, including the CIA, giving their biennial estimates on weapons of mass destruction and nuclear proliferation, in which they said that China still is the greatest proliferator of weapons of mass destruction, and that Beijing is continually supplying the rogue nations that are increasingly becoming a threat to this country with regard to biological, nuclear and chemical capabilities?

We hear that testimony all the time. That is why I consider it more than a bureaucratic quibble to require some kind of end-user satisfaction with regard to the Chinese. This is why it concerns me that the administration wants to keep under wraps the agreement that we supposedly have entered into as to the way we are supposed to have some satisfaction on post-shipment verification.

So it is not just strictly a Chinese deal. It is a complicated world out there, and part of what is happening is that the Chinese are supplying dual-use items, technicians, technology, raw materials, and components, to a host of rogue nations. Now, that is not your business, but that is our business, and I just want you to know that we are not trying to be unduly restrictive or anti-competitive, and we understand the genie is out of the bottle. But this is part of what we have got to balance, and this is why we have got to be careful as, on the one hand, we try to embrace these countries, and trade, and get along as best we can, and, on the other, we remain mindful of their threats and of information revealed by our own intelligence analyses, whether it be by the Rumsfeld Commission or the Deutsch Commission or our own intelligence assessments. These assessments are continually saying that this country is doing things that pose a threat to our national security, albeit, in some cases, in a roundabout way through the rogue nations.

So that is a part of this process, too, and that has got to enter into the balance. It looks to me like this has front-end and back-end ramifications in terms of this process. It is the process, it seems to me, that is most important here. No one can sit here—I cannot sit here—and say what the MTOPS level ought to be. But I do not think somebody within the bowels of the Department of Commerce ought to be the unilateral determiner of what that MTOPS level should be, either.

I think we need a process that includes all of the relevant people at the table. I will make a final point here. It seems to me that we should not overlook the fact that our allies, our economic competitors and other countries in which these computers are made and so forth, they have licensing processes themselves. It's also

worth remembering that when you are looking at something like foreign availability or mass-marketing, some are proposing taking whole categories of things out of the process—decontrolling them because of alleged foreign availability.

We are not even looking at the question of whether or not "foreign available" computers are available perhaps only to our competitors' licensing process. If they have a licensing process and they control these items, even if it is "foreign-available," do we want to totally decontrol this item? When they have got a licensing regime and we will not have one anymore, aren't they going to immediately do away with their licensing regime too? It is going to be a race to the bottom.

So those are the sort of things that concern me. I am making more of a statement. Anybody can comment on any of that, if you want to.

Mr. HOYDYSH. Let me just make a comment on the question of foreign availability, and I think that has to be split into two parts. There are two issues here; one, can other countries make these products? And I think that, we can demonstrate very clearly that almost anyone can make them. There is no technological impediment to making them—it is a economic impediment.

Everyone can make them, but not everyone can make money making them; so that is what keeps people from getting into the business. The other question is whether they have equal export controls. My experience, and I have been doing this for 17 years, including attending COCOM for 7 years, that our allies stayed in COCOM only by the force of the will of the United States. If we had opened the door, they would have been out of COCOM way before it was formally dissolved.

One of the big differences between COCOM, which at least worked fairly well, and today is that there was then general agreement about a common threat. Right now, there is little agreement on the common threat. There is agreement on the rogue nations, but there is no agreement that China poses a threat. In fact, the other COCOM countries explicitly—the other Wassenaar countries explicitly rejected putting China on a target list.

Another complicating factor that one of our targets in Tier III, Russia, is a member of Wassenaar. In addition, other members of Wassenaar are actually trying to get China to join Wassenaar.

So if you have China and Russia as members of Wassenaar, which is the organization that is supposed to control exports to these countries, you end up with some very strained relationships and situations.

Chairman THOMPSON. Well, that is interesting you should mention that, because I just came back a few weeks ago from a trip. I went to Vienna, talked to the Wassenaar Arrangement people there, talked to several of our allies about the Wassenaar Arrangement and what they thought about it, and ran into some of the things that you are talking about. There is more than one view as to the COCOM situation and as to who the leader was in disbanding that, however, and a lot of people think it was the United States. Some people think it should have been, and certainly something different should have come about.

So we have got something that really is dysfunctional in many respects, and that is the Wassenaar Arrangement. You are right; Russia is a part of that. And some of our allies too: Oftentimes, we have particular problems with the French, amazingly enough, and we and they do not see eye-to-eye on many things. The question is, what kind of example are we going to set; and, what are we doing particularly with regard to these high-performance computers?

I was surprised to hear from some of our allies while I was over there that far from playing catch-up to our competitors, the United States is leading the way in decontrolling these high-performance computers, much to the chagrin of some of our Japanese friends and our European allies. I was also surprised to learn that our allies still, in some cases, maintain some controls on these computers that we are not controlling; and that we are constantly the ones that are pushing the limit because of the competitive advantage we have there.

So I do not think that this is a totally black-and-white picture. The other thing I would ask is whether or not there is any validity to the notion that it makes a big difference whether one secretly steals a computer or whether one buys it legitimately. Sure, many countries have substantial capabilities in terms of high-performance computers, whether they are making them themselves or import into them, either legally or illegally. But that is much different than having a formal relationship with a legitimate supplier, in which you are exporting mass quantities and where the recipient is able to receive the technical support and training.

Does it not slow them down to be denied such support? I think many times maybe this is what we are talking about, what we are trying to do while we are building the national missile defense system and reconfiguring our military and all that. Perhaps we are just talking about slowing down the proliferation process with regard to problem countries. Does it not slow down the process if you deprive them of the technical support and training?

We maintain our ability to track who gets what by having a control system—track what is going out of the country; we do not wholly decontrol; we do not give to just anybody the technical support and training that would go with a traditional commercial transaction. Is there any validity to that concept, do you think?

Mr. HOYDYSH. Absolutely, Senator, there is validity to it. But just to put this in context, we are not asking to release all high-performance computers. We are only asking for easing of restrictions on the lowest level of high-performance computers, assuming for the moment they can be still called high-performance computers. These are common business servers which are used in electronic commerce, and we have talked about a level of four-to-eight processors. Each of our companies make computers that have 32, 64, and above, and the highest computers, the most powerful ones, have thousands of processors.

So we still believe in strict controls on that level of technology, and not even a question of licensing. We do not even think that the highest end should be exported to Tier III, period. What we are talking about is the large-volume, lower-end, which is absolutely essential if China is going to develop its Internet infrastructure, if it is going to develop its e-commerce capabilities, which would

allow it to have more information, and more interaction. These computers provide the backbone for that system infrastructure.

We are not talking about all computers. We are talking about the lowest slice of technology that is widely available.

Chairman THOMPSON. And we are not talking about stopping the sale of those computers. We are talking about a review process.

Mr. HOYDYSH. And that is where the difficulty lies, because at this level of processor, you are talking more and more about direct sales, about delivery in a matter of days. These are not things that take a long time to build. Most of these things are built within a few days of receiving the order; so speed of delivery is essential.

One of the biggest problems with the review process that we have is that even if it lasts 10 days, you have to add the Chinese end-user certificate process to it. Then you have to add the fact that each of these exports requires, by law visitation by government official on top of that. Foreign rendors can deliver the same product at relatively the same price with the same performance without all of this bureaucratic baggage.

It makes our stuff less competitive and, in addition to which, we cannot utilize third-party distributors because we cannot ship the product into China unless we have the end-user identified at the time of shipment; so that we are deprived of a whole channel of distribution of these systems.

Chairman THOMPSON. There are a lot of distribution problems in selling goods to China that have nothing to do with our controls on this end.

Mr. HOYDYSH. No, but this is a specific aspect of the way some of our companies do business. They identify someone who will provide the service, who will hold the product and distribute it to individual end-users. We cannot use that channel.

Chairman THOMPSON. One more thing. Your criteria seems to be the sale of processors. We have been talking about MTOPS levels.

Mr. HOYDYSH. What I wanted to do was de-mystify the question of MTOPS, because everyone is fixated on the 2,000 MTOPS level which, in the mid-1900's or early 1990's, represented a powerful machine. Today, an Intel personal computer, the Apple personal computers, have MTOPS rating of almost 2,500. In addition, as some of the other folks here have testified, MTOPS may not be a valid measure of national security concern. Just because——

Chairman THOMPSON. Excuse me. But for better or for worse, the MTOPS level still is the criteria we are having to deal with here. So what are you suggesting be decontrolled in terms of MTOPS levels?

Mr. HOYDYSH. At MTOPS levels now, coming out with the newest processors that will be available later this summer——

Chairman THOMPSON. Again, we are looking into the future a little bit.

Mr. HOYDYSH. Well, you see, you are right, we are looking into the future; but what makes it so much more difficult for us is, because of the 6-month delay and because it takes at least 3-plus months for an interagency process to come up with a number, we are required to forecast what would be available anywhere from 9 months to a year in advance.

In the last go-round, we actually missed the fact that the Apple Macintosh arrived sooner than expected and could not be sold through these distribution channels. So that one of the reasons for shortening this 6-month congressional review period is to make that forecast less prospective.

We are not saying decontrol today that which will be available 6-months from now.

Chairman THOMPSON. I understand. I did not mean to get you diverted. We were getting back to the MTOPS level. Can you translate what you would suggest?

Mr. HOYDYSH. We are suggesting that if the MTOPS level is announced in July, let's say, and it becomes available 6 months from now, which is still the current law, then we need to be able to sell four-processor systems, which are large-volume systems made with the new Itanium microprocessor, and that number, and I could be off by several hundred, is somewhere on the order of 27,000 MTOPS. That is a four-processor system.

Later on next year, and this is January 2001, mid-July, 2001, that number goes up to somewhere on the order of 33,000 or 34,000 MTOPS. And I do happen to have a prop——

Chairman THOMPSON. I thought as of February of this year, you were at the 20,000 MTOPS level for civilian use anyway for Tier III countries.

Mr. HOYDYSH. Well, the level that we are talking about is the lower level. That is the level below which government review is not required.

Chairman THOMPSON. Right.

Mr. HOYDYSH. So, right now, that level is 6,500 and the civilian level is 20,000. But above 6,500 we have to submit it to the government for a 10-day review, so that the government still has the ability to review the end-user above 6,500 MTOPS.

Chairman THOMPSON. Maybe February was an announced date instead of an effective date.

Mr. HOYDYSH. It is an announced date. That does not——

Chairman THOMPSON. That was 12,500 for military.

Mr. HOYDYSH. That becomes effective August.

Chairman THOMPSON. OK.

Mr. HOYDYSH. Because of the 6-month delay.

Chairman THOMPSON. All right.

Mr. HOYDYSH. Any announcement in July would become effective in January 2001.

Chairman THOMPSON. Thank you very much. Senator Lieberman.

Senator LIEBERMAN. Thanks, Mr. Chairman. I want to come back to Mr. Johnson and Mr. Lieberman briefly. Mr. Johnson, you said at one point in your testimony that post-shipment verifications are important, but if I heard you correctly, they do not always tell us what the end-use of the computer is.

Mr. JOHNSON. That is correct.

Senator LIEBERMAN. So what I wanted to ask you was what system would you put in place—or would you—to help us better do verification after shipment to see exactly how these items are being used?

Mr. JOHNSON. Well, I think our conclusion is that post-shipment verification is an important process, because it does identify the lo-

cation of the computer. You can tell what kind of facility it is in, but you cannot necessarily determine what it is being used for. That requires some highly-trained technicians to be able to go in and look at the data that is in the computer, the computer codes, the programming and all, to determine how that computer is being used.

We do not have a fix for that, but we do think the process of just identifying having that verification that the computer is there does at least help keep the system honest. There may be some occasions when the Department of Commerce would want to, and I think it has on some occasions, used highly-trained technicians from the national labs to look at how computers are used, but that would be one alternative.

It is a very expensive process. These people are highly paid and it takes time to do that.

Senator LIEBERMAN. Is it clear that we have the authority under law to do that next level of post-shipment verification to see exactly how the computers are being used?

Mr. JOHNSON. I would have to research that. I think that we do have that authority, but whether or not we would be able to get the cooperation of the——

Senator LIEBERMAN. The purchaser?

Mr. JOHNSON [continuing]. Government, the purchaser, to do that, is another thing.

Senator LIEBERMAN. So, in a way, you are saying that the difference here is between determining where the computer ends up and how it is used.

Mr. JOHNSON. How it is used; yes.

Senator LIEBERMAN. OK. I would welcome any response you have to that in writing afterwards.[1]

Mr. JOHNSON. Sure.

Senator LIEBERMAN. Which is whether the authority is there. Mr. Lieberman—every time I say that, I feel as if I am having a conversation with myself, which are some very good conversations I have, of course, regularly. You talked about the fact that you do not want to see any items dropped from the control list without DOD approval at one point in your testimony.

Just help me remember to what extent DOD participates with Commerce in the construction of the control list; that is, the dual-use items that are on the control list?

Mr. LIEBERMAN. Well, currently, DOD basically generates a national security list that is a list of militarily-critical items, and then gives it to Commerce to be incorporated into the Commerce control list, and we think that process works pretty well. So, basically, what we are suggesting is simply that this process be retained, or at least the essence of the process be retained.

Senator LIEBERMAN. You are really right at the heart of this dilemma that we have talked about all morning, which is here are these extraordinarily capable computers and other items, and how do we determine how they are going to be used and whether, in fact, they are—so how does the Department of Defense make that judgment? Is it a cautious judgment? In other words, is it a sort

[1] The information referred to appears in the Appendix on page 119.

of worst-case scenario judgment, that here is something that of course can be used for peaceful, commercial purposes, but, in these circumstances, it is possible that it could be used in a way that would threaten us?

Mr. LIEBERMAN. Well, I would hesitate to make a general characterization like that. Certainly Defense is subject to the same pressures in terms of different opinions, different inputs, from across the spectrum. Industry certainly provides input to the department, and right now, a lot of the department's efforts to re-engineer its own internal review processes for export controls are largely driven by complaints from industry that our process is inefficient and takes too long.

So we are aware of that end of the spectrum. Of course, we have several Defense agencies involved. The intelligence community certainly inputs. But we are talking about a dynamic situation where what it makes sense to control today may not make a whole lot of sense down the road; and, in fact, the control list does change over time.

I think there is certainly a legitimate case to be made that the control list ought to be under constant scrutiny and evaluation from the standpoint of advancing technology.

Senator LIEBERMAN. And maybe that is not happening frequently enough now or regularly enough now.

Mr. LIEBERMAN. Well, I do not have enough knowledge of that to say whether it is happening—we really have not made any attempt to look into individual determinations of what has gone on the list and what has come off the list. In fact, that is the primary subject of next year's interagency IG review. You may recall that the authorization act last year requires the IGs of several Federal agencies to look at this whole process annually for 7 years; and this year, we looked at what are called deemed exports. Next year, we are going to be looking at the composition of the control list, and I hope that I can give you a much better answer perhaps this time next year.

Chairman THOMPSON. Excuse me. And also, would that include who decides what goes on and comes off of it?

Mr. LIEBERMAN. Yes, sir.

Chairman THOMPSON. OK.

Senator LIEBERMAN. Thank you. We will look forward to that.

Mr. Milhollin, I want to come back to something you said, which is if the current definition of foreign availability—I presume, in 1712, continues—that we will, in fact, be required—the United States will be required—to decontrol certain items that our allies now control. Could you just develop that thought a little bit more?

Mr. MILHOLLIN. Yes. Well, to begin with, there is a generally agreed list of things which we control in common with our allies for each kind of technology.

Senator LIEBERMAN. Right.

Mr. MILHOLLIN. I am sure the Committee is familiar with those. The five items in my testimony that I selected as examples are controlled by our allies, as well as ourselves. I think some of them are probably controlled for missile, as well as nuclear, reasons. In my judgment, I think that it would be very likely that foreign avail-

ability determinations would be made for all of them, because they are made by manufacturers in more than one country.

Senator LIEBERMAN. Right. These are all again controlled now by our major allies and ourselves?

Mr. MILHOLLIN. Yes, and I think you could probably find cases where foreign countries or countries that we are worried about, say controlled countries, had managed to buy these things on the world market. So, again, if you come down to the position that if a controlled country can buy these things from somebody, then they should not be controlled here, you run into the problem that you would have to go down the whole control list to see which items are available to a rogue from some rogue supplier—I am sorry—available to a controlled country from a rogue supplier, then you would have to make a judgment in each case to what extent it is available, and our experience shows that the controlled countries can get some of these things some of the time from rogue suppliers.

For example, the Pakistanis have been quite successful in importing missile technology of all kinds from China, and Iran has been successful in importing poison gas technology from China. In fact, lots of countries have been successful in importing lots of things from China; and if you use that as a standard, then you are going to have to decontrol a fair number of items that our allies and we now control.

Senator LIEBERMAN. Do you have a recommendation for a better definition of foreign availability?

Mr. MILHOLLIN. Well, we have a foreign availability procedure now that has been criticized. I question whether—it seems to me that if an exporter can go through the present process and prove that something is foreign-available, then he is entitled—then the exporter is entitled to some consideration.

I have not sat down and tried to draft standards of my own. I mean, it took me a fair amount of time to go through the standards that are in the bill and compare these items to that standard.

Senator LIEBERMAN. Sure.

Mr. MILHOLLIN. But I could say one thing, that the standard that the Banking Committee has adopted seems to me to be entirely too broad and too sweeping. Senator, if I could, I would like to comment on something.

Senator LIEBERMAN. Before you go there, let me just say that if you have the time and inclination, I think it would be very helpful if you had some suggestions about what a better standard might be than the one that is in the Banking Committee bill.

Mr. MILHOLLIN. Very well.

Senator LIEBERMAN. Please go ahead with what you were going to say.

Mr. MILHOLLIN. I was going to say a couple of things in response to Mr. Hoydysh's answers to the Chairman's questions. The most recent data on the amount of supercomputer exports to Tier III countries is about 5 percent.

Senator LIEBERMAN. Five percent of?

Mr. MILHOLLIN. Five percent of the supercomputer market or the high-performance computer market.

Senator LIEBERMAN. And that is the world market or the American share of the business?

Mr. MILHOLLIN. The American, I guess—5 percent of what we, the United States, export.

Senator LIEBERMAN. OK.

Mr. MILHOLLIN. Because there are some numbers on that, and the most recent ones I have seen put the share at about 5 percent. Second, I think we have talked a fair amount about delays. The Commerce Department is now meeting its time requirements in over 90 percent of its cases. So the Commerce Department now has a pretty good record of getting dual-use items turned around in a pretty good period of time.

The primary reason for that is that we are only controlling about a tenth as much dual-use equipment as we controlled during the Cold War; that is, in about 1989, we were controlling about ten times as much as we are doing now. So, with the lighter licensing burden, Commerce is able to turn around the applications within its time restraints in about 90 percent—over 90 percent of its cases.

The third thing I would like to point out is we are not talking about barring exports; we are talking about licensing them.

Senator LIEBERMAN. Right.

Mr. MILHOLLIN. And, again, over 90 percent of the applications are approved. So, for Mr. Hoydysh's purposes, I would suggest to him that it is a good thing, if you are exporting a sensitive item, to get the government to tell you whether it might be going to the wrong place; that is, if I were an exporter and I had the government giving me a free bureaucrat that would tell me within 10 days whether my customer was a problem, I think I would want to take the government up on that, rather than read in *The New York Times* or *The Washington Post* that my product had gone astray.

I think we are providing a good service; that is, a 10-day review to tell an exporter, "Look, you know, there is a problem with this guy," or there is not. It seems to me an exporter would—I do not understand why exporters do not want that service. Let's put it that way.

Senator LIEBERMAN. Mr. Milhollin, I want to finally just ask you to respond to two other points made here, in some ways, both by Mr. Hoydysh, but the first one is a general point that is certainly made by those who support the current movement of our export control system, which is to turn the national security argument around, if you will, and say that at the heart of our national security today is our technological capability.

Part of the way the high-tech industries in America stay strong is by enjoying a good share of the global market, and if, in some sense, export controls are applied so rigidly or demandingly that we deny them that market, that the effect will be that they will have less resources with which to develop the capabilities that make us a strong Nation. So how do you respond to that?

Mr. MILHOLLIN. I think that argument would be a valid argument if the countries we are worried about were a major part of their market. But, in fact, they are not.

Senator LIEBERMAN. Including China?

Mr. MILHOLLIN. Including China. Again, the most recent figures I have seen show that Tier III, that is, the countries we are wor-

ried most about for supercomputer exports, are taking about 5 percent of our sales.

Senator LIEBERMAN. Tier IV are what we more typically call the rogue nations, Iraq, Iran, and Libya?

Mr. MILHOLLIN. That is right.

Senator LIEBERMAN. And then Tier III is China, Pakistan——

Mr. MILHOLLIN. India, Israel, and Russia, that sort of thing.

Senator LIEBERMAN. Right.

Mr. MILHOLLIN. I believe that in the supercomputer industry, the companies—there are not very many companies. There are six, eight, or ten. They are going to survive or not depending on how they do in the big market; that is, the U.S. market, the Japanese market, the European market, the markets for truly civilian applications of high-speed computing.

They are going to make it or not with respect to each other depending on how they do in those markets, not whether they make a marginal sale to Tier III or not. So I think that it is a good argument that we have to be strong and maintain our competitive edge, but it is just that the numbers are not there. Who makes it or does not is not going to depend on sales to Tier III. That is my response.

Senator LIEBERMAN. The second one was the very interesting exchange between Senator Thompson and Mr. Hoydysh, and it goes back in a way to something you said earlier in the initial argument you made about America setting the standard, which is that we did during the Cold War. That is part of why COCOM worked and why, though there was naturally some leakage, nonetheless, the former Soviet Union was impeded in its development of some sophisticated systems.

And, of course, the argument would be as it was made by Mr. Hoydysh, which is that the world has changed and we are post-Cold War. Not only is it not a bipolar world anymore, but more to the point here, though we have a rough consensus with our allies about the rogue nations, the Tier IV nations—and, again, there is some leakage there about Iran, Iraq, and Libya, from some of our allies, in Europe particularly—the real controversy seems to be over China and our differing attitudes, notwithstanding some of the testimony today, from you particularly, about China's proliferation activities.

So I wanted to give you a chance to update your argument about the effectiveness of COCOM because of our American leadership in a world that is quite different from the one in which COCOM existed and, most particularly, in which we seem to have some fundamental disagreements with our allies, sophisticated, well-developed allies, about China.

Mr. MILHOLLIN. I think that Mr. Hoydysh's point is a good one. He argues that we do live in a different world and it is true, there is less consensus and the targets of our activities are not as well-defined, and, in particular on China, there is a debate. But, you know, there is also a debate on Iran. I have talked to German export control officials high up who do not see Iran as a threat. In fact, one of them told me that Iran was his favorite country.

We are in a world where one country's rogue is another country's good customer.

Senator LIEBERMAN. Right.

Mr. MILHOLLIN. So this whole effort is much more difficult and it is going to require much more aggressive and more effective diplomacy by us than in the old days when it was easier. But if you look at the alternatives, do we have an alternative to doing it? I do not think we do. I think we have to do the best we can in a new world which is more difficult, but I do not think we can just say, "Well, gee, the world is really difficult now. It is very dangerous. We are just going to throw up our hands and everybody is going to sell everything to everybody and we are going to have total democracy in all the technologies that are necessary to build weapons of mass destruction." I fear that that is the tendency we are seeing, but I do not think we are ready to live in the world of 1914 in which everybody has the bomb.

Nuclear weapons grew up during the Cold War, which was a pretty stable period, looking back on it now. If you postulate the kind of—lots of countries with lots of different alliances that we had before World War II, and you imagine lots of those folks with nuclear weapons, we are not ready for that, but I think that is where we are going. And what I am trying to argue is that we should slow it down as much as we can.

Senator LIEBERMAN. Sure. Understood. Mr. Hoydysh, do you want a word to respond?

Mr. HOYDYSH. Yes, very briefly. I am not going to argue about whether it is 5 or 6 percent of the market. If we believed that what we were doing was hurting national security, it would not matter whether it was 5, 10, or 15 percent of the market. We are convinced, though, that even the 5 percent, which is bound to grow—Tier III countries represent about half of the population of the world—we cannot afford to give up those markets without having some serious impacts on our technological leadership and on the health of our industry. Five percent sounds like a small number, but what if someone proposed to cut the defense budget by 5 percent? That has significant impacts on our R&D and significant impact on where we can compete.

We are proposing what we are proposing because we think on balance it helps us more than it helps any potential enemies, and that, even if we did not sell a single one of these items that we are talking about—and I am not talking about high-end computers, only the ones that we are talking about decontrolling—that the target countries could get as many of these as they wanted from other sources and we would have accomplished nothing, other than losing 5 percent of the market.

Senator LIEBERMAN. That frames the issue and the difficulty of our decisions. Thanks very much to all of you and to you, Mr. Chairman. I think it has been for me a very helpful morning.

Chairman THOMPSON. Well, thank you. Listening to you and Mr. Milhollin, it seems to me what happened was that during the Cold War, we had this pretty tough regime, this COCOM regime. Then, the Cold War was over. We disbanded COCOM and we had a lull period there. Now what has happened is that a new, more diverse threat has emerged, in terms of the rogue nations. And all we are left with is Wassenaar, which is very, very weak, and we are struggling to see how much further we want to or can go in terms of

something less than COCOM, but more then Wassenaar. It seems to me that this is what we are struggling with.

There is one more point I would like to make before concluding, one that I think is a very, very important one. It concerns the idea of reducing the congressional renew period for computer decontrols to 30 days, that is 30 calendar days that is being proposed. If we were out of session, there would be no review time at all. GAO would not even get it, presumably. So that is somewhat unusual and, I think, absolutely undesirable.

But finally, on a note of harmony, we had IG reports last year, and we had an array of all the inspector generals before us who looked at our export situation with regard to various departments. There are clearly some things that we ought to be doing that we are not doing, and that are not or should not be controversial. We do not have enough licensing officers. They apparently are not sufficiently trained. The law requires training programs for these agencies. It is not being complied with. The law requires a cumulative effect analysis that is not being done. Nobody knows what the cumulative effect of all this is. We look at these things one at a time.

We have in our export control bureaucracy, as we do in most all the other government agencies, totally inadequate information systems. Our computers do not talk to each other with regard to this licensing process. Our law enforcement people, who might have information on some of these entities that our exporters are trying to deal with, and not integrated sufficiently into the process. It is either not there, or not used, and there is no coordination. It's a real management problem.

That is what we ought to be doing first, I think. There is an awful lot of stuff that we could do that would speed up the process and also improve the safety of the process and help fix some of the things that we are concerned about. So that should be on the table, also. So, with that, we will cease and desist. Thank you very, very much for this very enlightening hearing that we have had today and your testimony.

The record will remain open for a week after the close of the hearing. So, we are in recess.

[Whereupon, at 12:20 p.m., the Committee was adjourned.]

# APPENDIX

## PREPARED STATEMENT OF SENATOR AKAKA

Mr. Chairman and Senator Lieberman thank you for holding this hearing.

How to control exports critical to our national security in a world of rapid technological innovation is one of the most serious issues we face.

I hope that this Committee will hold more hearings on this topic and I would recommend looking at the administration's new proposals on export controls announced just this week.

Most of us would consider computers to be on the cutting edge of technologies which we should control. But at the same time the definition of "cutting edge" is constantly changing. Sometime this year Intel will introduce a new chip which will more than double the current level of computer processing capability.

Efforts to control this technology sometimes become ridiculous. For example, this fall Sony will introduce its new PLAY STATION II which contains a processor above the performance levels set by current Japanese export controls. Rather than restrict PLAY STATION exports, the Japanese redefined how to control such items.

We are in a similar situation in this country. Every few years—with increasing frequency—every administration since President Reagan's has had to revise controls on computer exports.

This has become an even more critical question as the American computer industry earns more than 50 percent of its revenues from exports. With the speed of innovation and the need to protect market share from foreign competition, I can see why the industry is eager to raise the level of permissible exports and speed up the license review process.

This is an industry in which innovation is the key to market success. American manufacturers do not have a monopoly on production. For example, 80 percent of all computer motherboards are manufactured in Taiwan. One of the fastest growing computer companies in the world is in Beijing. To keep pace with this competition, American manufacturers need the revenues to plow back into research and development.

In December 1999, the Pentagon's Defense Science Board Task Force on Globalization and Security concluded that "if U.S. high-tech exports are restricted in any significant manner, it could well have a stifling effect on the U.S. military's rate of technological advancement."

In effect, this is the heart of the problem: How do we control critical defense exports without stifling the innovation necessary to national security in a world in which the globalization of technology can outstrip our ability to control it?

I look forward to the witnesses today and their answer to this question.

United States General Accounting Office

GAO

Testimony

Before Governmental Affairs Committee, U.S. Senate

For Release on Delivery
At 10:00 AM May 26, 2000

# EXPORT CONTROLS:

# Challenges and Changes For Controls on Computer Exports

Statement of Harold J. Johnson, Associate Director, International Relations and Trade Issues, National Security and International Affairs Division

GAO/T-NSIAD-00-187

Mr. Chairman and Members of the Committee:

I am pleased to be here today to discuss export controls for high performance computers. My testimony is based on work that we have conducted over the past 3 years, particularly the reports we issued in 1998 and 1999.[1]

U.S. policy with respect to the export of sensitive technology, including computers, is to seek a balance between the U.S. economic interest in promoting exports and its national security interests in both maintaining a military advantage over potential adversaries and denying the spread of technologies used in developing weapons of mass destruction. The United States has long controlled the export of high performance computers[2] to sensitive destinations, such as Russia and China. These computers have both civilian (dual use) and military applications and technological advancements in computing power have been rapid. The Department of Commerce has primary responsibility for managing the licensing of these dual-use items and weighing the promotion of commercial interests in exporting items against the protection of national security interests. For the past several years, there has been continuing congressional concern about and debate over whether our national security is being harmed by relaxing export controls on high performance computers and over the rationale for subsequent revised controls.

Today, I will discuss our observations about how the executive branch (1) assesses the national security risks associated with the export of high performance computers going to countries of concern, (2) determines when the exports of computers at existing performance levels can no longer be controlled, and (3) has addressed arrangements for post-shipment verifications of high performance computer exports.

---

[1] Export Controls: Information on the Decision to Revise High Performance Computer Controls (GAO/NSIAD-98-196, Sept. 16, 1998) and Export Controls: Statutory Reporting Requirements for Computers Not Fully Addressed (GAO/NSIAD-00-45, Nov. 5, 1999)

[2] The Commerce Department considers a high performance computer to be one that exceeds a defined performance threshold, thus requiring an export license.

RESULTS IN BRIEF

The executive branch has not clearly articulated the specific national security interests to be protected in controlling the export of computers at various performance levels, nor has it stated how countries of military concern could benefit from using such computers. Without a clear statement of these interests, it is unclear how the executive branch determines what are the militarily critical applications that may affect U.S. national security. In addition, the executive branch has relaxed export controls on computers because it believes that machines at the previously approved levels, had become so widely available in the market that their export is uncontrollable. Commerce defines controllability to include the "volume of sales" for certain types of microprocessors that can be easily assembled and maintained by foreign end users. The executive branch, however, relaxed controls based on what computer manufacturers asserted would be their next mass-produced processors, not on actual sales.

Post-shipment verifications confirm the physical location of high performance computers and, to the extent practical, verify if they are being used as intended. However, while post-shipment verifications are important for detecting and deterring physical diversions of computers, as traditionally conducted, they do not verify computer end use. Although the National Defense Authorization Act requires post-shipment verifications on all high performance computers exported since November 18, 1997, to tier 3 countries--whether licensed or not--Commerce has not visited high performance computers exported to China prior to an end-use arrangement reached in June 1998, and believes that to seek to do so would be futile.

BACKGROUND

The U.S. export control system is about managing risk; exports to some countries involve less risk than to other countries and exports of some items involve less risk than do other items.

Under U.S. law, the President has the authority to control and require licenses for the export of items that may pose a national security risk or foreign policy concern. The President also has the authority to remove or revise those controls as U.S. concerns and interests change. The U.S. export control system is administered by two agencies. The Commerce Department, through its Bureau of Export Administration, licenses sensitive dual-use items (items with both civil and military uses) under the Export Administration Act of 1979, as amended (P.L. 96-72).[3] The State Department, through its Office of Defense Trade Controls, licenses munitions items under the Arms Export Control Act (P.L. 90-629). Since the end of the Cold War, the number of items subject to export controls has been significantly reduced. For example, while 10 years ago, the Commerce Department reviewed about 100,000 license applications annually, today that figure is down to about 12,000 applications per year.

The U.S. government controls the export of high performance computers to certain countries based on foreign policy and/or national security concerns. High performance computers and related components (such as, processors) are controlled under the Export Administration Act, as continued by executive order, and the Export Administration Regulations. Executive Order 12981 authorizes the Departments of State, Energy, and Defense to review export applications and to consider export control policy.

Since 1993, the President has revised U.S. export control requirements for high performance computers four times, including a revision announced in February 2000. A revised export control policy implemented in January 1996 removed license requirements for most exports of computers with performance levels up to 2,000 millions of theoretical operations per second (MTOPS)[4] (an increase from 1,500 MTOPS). The policy also organized countries into four computer "tiers," with each tier after tier 1 representing a

[3] The Export Administration Act terminated on August 20, 1994. Pursuant to Executive Order 12924, issued on August 19, 1994 (59 Fed. Reg. 43437) the President, to the extent permitted by law, extended the application of the act indefinitely. In addition, the Nuclear Regulatory Commission licenses exports of nuclear reactors. Dual-use nuclear exports are licensed by Commerce in consultation with a number of other agencies.

[4] High performance computers are regulated based on their composite theoretical performance as measured by MTOPS.

successively higher level of concern related to U.S. national security interests.[5] A dual-control system was established for the 50 tier 3 countries, including China, Russia, India, and Israel: a license for potential military end-users is required at a lower MTOPS threshold than the threshold for civilian end-users. High performance computer exports to countries in tier 4 (for example, Iran, Iraq, and Libya) were essentially prohibited because of national security and foreign policy concerns about these countries.

The Fiscal Year 1998 National Defense Authorization Act (P.L. 105-85) modified the policy for determining whether an individual export license is needed and required exporters to notify the Commerce Department of any planned sales of computers with performance levels greater than 2,000 MTOPS to tier 3 countries. This level subsequently was increased to 6,500 MTOPS effective January 2000 and is scheduled to be increased to 12,500 MTOPS effective August 2000. If the Department of Commerce, Defense, State, or Energy, each of which reviews these notifications, objects to the export within 10 days, the exporter must then submit a license application.[6]

In addition, the act required the President to submit a report to Congress justifying any changes to the control levels for the notification process for the export of high performance computers to tier 3 countries. The act requires the report, at a minimum, to (1) address the extent to which high performance computers with capabilities between the established level and the new proposed level of performance are available from other countries, (2) address all potential uses of military significance to which high performance computers at the new levels could be applied, and (3) assess the impact of potential military uses on U.S. national security interests. We reviewed the report submitted by the President on July 27, 1999, proposing changes to the current export control levels for high performance computers. We reported in November 1999 that the

[5] The policy placed no license requirements on tier 1 countries, primarily those in Western Europe and Japan. Exports of high performance computers above 10,000 MTOPS to tier 2 countries in Asia, Africa, Latin America, and Central and Eastern Europe continued to require licenses.
[6] In addition to reviewing notifications, State, Defense, and Energy also review export license applications that are submitted directly to Commerce.

report did not fully satisfy the reporting requirements of the act.[7] In particular, it did not assess the impact of the military uses of high performance computers on U.S. national security concerns.

On February 1, 2000, the President announced changes to the current export control levels for high performance computers. These changes included raising the performance threshold for computer exports that require a license for (1) tier 2 countries from 20,000 MTOPS to 33,000 MTOPS and (2) tier 3 countries from 6,500 MTOPS to 12,500 MTOPS for military end-users and from 12,300 MTOPS to 20,000 MTOPS for civilian end-users. The announcement indicated that the changes for tier 3 military end-users are to become effective in 6 months, while the changes for tier 3 civilian end-users became effectively immediately. The changes also raised the performance threshold for computer exports that require a notification to Commerce for tier 3 countries from 6,500 MTOPS to 12,500 MTOPS. By law, Congress has 6 months to review this decision, after which the change in notification levels will go into effect. We are currently assessing the justification for the February 1, 2000, changes to computer export control levels at the request of the Senate Armed Services Committee.

## ASSESSING NATIONAL SECURITY RISKS FOR COMPUTER EXPORTS

Under U.S. export control policy, an analysis of establishing or revising controls on computers and other sensitive commodities generally is made in the context of the U.S. desire to limit the spread of technologies useful in both developing weapons of mass destruction and protecting the military capabilities of the United States and its allies. In many ways, the threat posed by an export is a relative one; that is, the threat depends on the U.S. capability to respond to enhancements the export would bring to the potential adversary's military capabilities. In order to maintain military superiority, the United States needs not only to control the spread of militarily sensitive technologies, but also to

[7] Export Controls: Statutory Reporting Requirements for Computers Not Fully Addressed (GAO/NSIAD-00-45, Nov. 5, 1999)

invest in leading edge technologies. However, this investment leads to the leading technologies of today becoming the "mass market" items in the future. Therefore, the United States must also quickly incorporate existing technologies into current and next generation weapon systems and manage the release of technology into the world market to "stay ahead of the curve."

While there appears to be general consensus that controlling high performance computers at some level is important to maintaining U.S. national security, DOD and the executive branch have not clearly articulated the specific national security interests to be protected in controlling the export of computers at various performance levels. In addition, they have not stated how countries of concern could benefit from using such computers. Without a clear analysis and explanation of the national security interest in controlling the export of high performance computers, the U.S. government cannot determine (1) what militarily critical computer applications need to be controlled or (2) the most effective way of implementing computer export controls. If such an analysis were made, it might also lead to a conclusion that the current reliance on MTOPS as the sole measure of a computer's sensitivity would no longer be appropriate. Indeed, with the rapid changes in computer architectures and the growth of what is called "distributed" computing,[8] new approaches may be necessary to protect the national security interests in limiting potential adversaries' use of such machines in their research and development programs and their deployed weapon systems.

To illustrate the importance of identifying potential national security risks of computer exports, let me briefly highlight for you some of the military applications of high performance computers that have been identified in some Commerce- and Defense

[8] "Distributed" or "parallel processing" means breaking computational problems into many separate parts and having a large number of processors tackle those parts simultaneously. Greatly increased processing speed is achieved largely through the sheer number of processors operating simultaneously, rather than through any exceptional power in each processor.

Department-sponsored studies. These studies were conducted in 1995 and 1998 to support decisions on revising export controls over these computers.[9]

- The Joint Strike Fighter has been designed using computers with 4,000 to 6,000 MTOPS of capability. Computers in this range now can be exported to military end-users in Russia or China without a license. Licenses for military end-users in these countries are required only for computers with performance levels above 6,500 MTOPs.

- Computers at 8,000 to 9,000 MTOPs are used for algorithm development for shipboard infrared search and track systems and modeling of submarine bottom designs for shallow water operations. While these computers currently require a license for export to military end-users in tier 3 countries, they would not be controlled under newly revised controls announced by the President on February 1 of this year. Under these new controls, only computers with more than 12,500 MTOPs that are to be exported to military end-users in countries like Russia and China would require a license.

- Designing submarines involves simulations of transmitting sounds through structures and in water, which are conducted at computer performance levels that are only slightly greater than the thresholds for which tier 3 countries may receive computer exports without a license. A Commerce- and Defense Department-sponsored study identified the use of a 21,000 MTOPS machine for this purpose. Some other related applications, such as acoustic sensor development and associated acoustic modeling, are executed on computers with performance only slightly greater than 20,000 MTOPS.

More generally, the 1995 Commerce- and Defense-sponsored study stated that there are research, development, test and evaluation applications at or above the 20,000 MTOPS

[9] Building on the Basics: An Examination of High-Performance Computing Export Control Policy in the 1990s (1995) and High-Performance Computing, National Security Applications, and Export Control

level of great national security significance, the proliferation of which should be strictly controlled. With the executive branch's February export control change, high performance computers up to 20,000 MTOPS will be available to countries like Russia and China without a license. The appendix to this statement provides additional information on selected military applications for high performance computers.

DETERMINING WHEN COMPUTER EXPORTS
CAN NO LONGER BE CONTROLLED

The previous examples illustrate the basis for our 1998 report's conclusion that the executive branch should clearly articulate the specific national security interests in limiting computer exports to potential adversaries when revising controls on high performance computers. In this regard, our September 1998 report[10] recommended that the Secretary of Defense assess and report on the national security threat and proliferation impact of U.S. exports of high performance computers to countries of national security and proliferation concern. We specified that, at a minimum, the assessment should address (1) how and at what performance levels countries of concern use these computers for military modernization and proliferation activities, (2) the threat of such uses to U.S. national security interests, and (3) the extent to which the export of such machines is controllable. The President's July 1999 report justifying changes to the control levels for computers did report that computers at all computing levels are important from the lowest performance levels to the highest. This conclusion, however, is general and was not supported by the level of analysis we recommended in our report, and does not address the serious concerns about the growing availability of high performance computers raised in the Commerce- and Defense Department-sponsored study issued in November 1995.

Although the examples just provided use MTOPS, this should not be construed to mean that MTOPS is the benchmark that should be used. Such a measure does not take into account advances in computer architectures that now allow the development of a large-

---

Policy at the Close of the 20th Century (1998).

scale, massively parallel computing resource from a cluster of commodity computing and networking components. In essence, by combining a number of readily available computers and networking components that would not require an export license, an organization can produce a very high powered computing resource. The operating system software that is necessary to utilize this resource is readily available from the Internet. However, a high performance computer by itself does not convey the ability to solve complex problems because application software is also necessary to conduct the proper analyses.

The task I have just described for the executive branch is not an easy one. It involves addressing difficult issues in an area of rapid technological change. Questions about the use of technology, the computer market, and DOD's own acquisition programs must be answered. Some key questions include the following: Does U.S. national security interest include maintaining a relative computing power advantage in deployed weapon systems (for example, air defense radar or command and control systems)? Are different strategies necessary to respond to the threats posed by the use of high performance computers in research and development and in deployed weapon systems? Will the availability of high performance computers help other countries develop and deploy new weapons or allow them to counter U.S. superiority in certain military applications? Does the growth of distributed computing make the use of MTOPS obsolete as an export control measure by which to restrict computer exports?

Before leaving this topic, I want to point out that a critical analysis of national security applications of concern may lead to conclusions that are very different regarding export control levels than are currently in place or being proposed by the executive branch. Indeed, DOD may conclude that significant national security concerns involve computer performance levels that are higher than current control levels.

---

[10] Export Controls: Information on the Decision to Revise High Performance Computer Controls (GAO/NSIAD-98-196, Sept. 16, 1998).

While the executive branch has not clearly articulated the national security interests in controlling high performance computers, it has developed a general explanation for its export decontrol decisions. In short, these decisions are based on conclusions that these computers are becoming widely available and, therefore, are uncontrollable.

It is important to note that the President's 1999 report to Congress concluded that there are militarily significant applications in the new control range, and, if not for their widespread availability, these applications would need to be controlled. These applications include advanced aircraft design, antisubmarine warfare sensor development, and radar applications. Consequently, the new control levels were not based on an assessment that these higher computing performance levels do not involve national security applications but rather that computers in this performance range are so widely available that they are uncontrollable.

Our November 1999 review of the changes in export control levels indicated that the administration's conclusions that the capabilities of high performance computers and related components, from both domestic and foreign sources, are generally increasing were supported because the United States does not generally control the export of computer processors and components. However, most sources of this supply are U.S. companies. Our earlier 1998 review reported that subsidiaries of U.S. computer manufacturers dominate the overseas high performance computer market and they must comply with U.S. controls. The 1998 study sponsored by DOD and Commerce[11] similarly found that the United States dominates the international computer market, at least in the mid- and high-range performance categories. Under current regulations, computer processors that perform up to 3,500 MTOPS can be directly exported to civilian end-users in many tier 3 countries including China and Russia. Exports of processors to such users in many other tier 3 countries, such as Israel and Saudi Arabia, are not subject to any MTOPS limit that requires a license. Exports of other key components for computer systems with four and eight processors are also not generally controlled; these

[11] High-Performance Computing, National Security Applications, and Export Control Policy at the Close of the 20th Century (1998).

parts can be shipped to tier 3 countries for civilian end-users, which could then use them to support the assembly of computers.

The administration's latest changes in the control levels for high performance computers were based on a determination that high performance computing capability is becoming increasingly available. For example, the 1999 changes in control levels were based on the conclusion that these capabilities are widely available and are therefore uncontrollable. The President's July 1999 report to Congress explaining these changes stated that due to the rapid advances in processor speeds and related technologies, foreign countries can obtain high performance computers directly or indirectly from a vendor, a reseller, or another third party or assemble such a computer using U.S. processors and components. According to administration officials, the specific export control levels announced in July 1999, and that went into effect in January 2000 for tier 3 military end-users, were based on the expected performance levels of computers using four and eight Intel Pentium processors that are projected to be on the market in July 2000.

While we found evidence to support the report's conclusion that computers with greater capabilities and related components are becoming increasingly available, we could not assess the administration's determination that computers rated below the new control levels are so widely available that they are effectively uncontrollable. An assessment of controllability involves critical evaluations of when and in what quantities an item should be considered so widely available as to be uncontrollable, and is dependent upon the resources applied by government and industry to control such exports. However, "widely available" and "uncontrollable" are terms not defined in current export control laws or regulations. Defense and Commerce Department officials stated that the analysis they prepared in support of the President's report relied on definitions that were developed in 1995 and 1998 studies they jointly sponsored. However, the discussion of the terms in these studies is general and without measurable criteria. Further, there is no mention in the President's 1999 report to Congress justifying the announced computer control revisions that defines how these concepts have been applied in setting the new export control levels. Thus, except to agree with the general conclusion in the President's report

that the availability of computing power in the commercial marketplace is increasing, we could not determine if the executive branch is correct in concluding that export controls had to be relaxed for high performance computers. Consequently, our 1999 report recommended that the administration develop specific criteria defining both "widely available" and "controllability." In response to this recommendation, Commerce defined "controllability"—but not "widely available"--

> "as a function of (1) the volume of sales, particularly through mass market distribution channels, (2) the types of microprocessors used in HPC configurations (and in particular whether these are general purpose microprocessors suitable for mass market applications), and (3) the extent to which multi-processor configurations using such microprocessors and other widely available components (such as boards, chipsets and operating systems) could easily be assembled into finished computers and maintained by foreign end users."[12]

This discussion brings me to one final point. The Senate bill (S. 1712) to establish a new Export Administration Act uses the terms "mass market status" and "foreign availability status" as determinants for relaxing export controls. The first term is defined very similarly to how the administration appears to use the term "widely available" as it relates to high performance computers. Both terms imply that an item is so commercially available that it cannot be controlled, but without providing the quantifiable measures necessary to make such an analysis. S. 1712 does provide a number of general criteria that might be helpful in making decisions about controlling the export of high performance computers. However, in developing the implementing regulations, Commerce may wish to provide more objective and empirical criteria to use in making these decisions. If it does not, then when this rather subjective standard is applied in the future to items controlled under the act, it will be difficult to assess whether this standard was applied appropriately.

The concept of "foreign availability," while part of the current Export Administration Regulations, would be changed to some extent by S. 1712. S. 1712 would authorize the Secretary of Commerce to determine that an item has foreign availability status—and thus be excluded from export controls—if three conditions were met: (1) if the item is available to controlled countries from sources outside the United States, including countries that participate with the United States in multilateral export controls; (2) can be acquired at a price that is not excessive when compared to the price at which a controlled country could acquire such item from sources within the United States in the absence of export controls; and (3) is available in sufficient quantity so that the requirement of a license or other authorization with respect to the export of such an item is or would be ineffective. A proposed revision to S. 1712 would authorize the President to designate certain items on the national security control list to require enhanced security and, thus, to have them excluded from the mass market and foreign availability provisions.

Although the Export Administration Act does not mention price of an item as a criterion for determining foreign availability, it does set forth two additional factors that are not covered by S. 1712.[13] Thus, S. 1712 does not include the two factors of "availability without restriction" and "comparable in quality to [items] produced in the United States" for determining foreign availability of an item.

POST-SHIPMENT VERIFICATIONS

Post-shipment verifications confirm the physical location of high performance computers and, to the extent practical, verify if they are being used as intended. However, there are

[12] The Under Secretary for Export Administration in a February 16, 2000, letter to the General Accounting Office stated that, in consultation with the Department of Defense, the Commerce Department had defined "controllability."

[13] The Act prohibits export controls for foreign policy or national security purposes on the U.S. exports of goods or technology which the President determines are (1) available *without restriction* [emphasis added] from sources outside the United States (2) in sufficient quantities and (3) *comparable in quality* to those produced in the United States so as to render the controls ineffective in achieving their purposes. Even when these conditions are met, the President may determine that adequate evidence has been presented to him demonstrating that the absence of such controls would prove detrimental to the foreign policy or national security of the United States.

limitations to determining end-use. Although the National Defense Authorization Act requires post-shipment verifications on all high performance computers, whether licensed or not, exported since November 18, 1997, the date of the statute's enactment, to tier 3 countries; Commerce has not visited high performance computers exported to China prior to an end-use arrangement reached in June 1998[14] and believes that it would be futile to seek such visits. Also, Commerce stated that doing such post-shipment verifications would not be a good use of the Department's limited resources. As of September 1999, Commerce had completed verifications on 104 computer exports, or about 27 percent of those verifications required for the computers exported during fiscal year 1998, and 73 percent had not been completed. Two-thirds of the computers that had not then been verified involved exports to China. Chinese authorities would not allow post-shipment verifications to be conducted on computers shipped before the June 1998 arrangement because of sovereignty concerns. Also, verifications could not be conducted on 82 computers shipped after the June 1998 arrangement because the exports did not conform to the arrangement. Commerce regulations published in January 1999 established a mechanism for all future computer exports to comply with the arrangement so as to be eligible for a post-shipment verification.

While post-shipment verifications are important for detecting and deterring physical diversions of computers, verifications, as traditionally conducted, do not verify computer end use. According to Department of Energy officials, it is easy to conceal how a computer is being used. Although it is possible to verify how a computer is being used through such actions as reviewing internal computer data, this would be costly and intrusive, and require experts' sophisticated computer analysis. Furthermore, the U.S. government makes only limited efforts to monitor exporters' and end users' compliance with explicit conditions attached to export licenses for computers. It relies largely on

[14] The arrangement provides that China (1) considers requests from the U.S. Commerce Department to verify the actual end use of a U.S. high performance computer to be non-binding; (2) insists that any end-use verification, if it agrees to one, be conducted by one of its own ministries, not by U.S. representatives; (3) takes the view that U.S. Embassy and Consulate commercial service personnel may not attend an end-use verification, unless they are invited by the Chinese government; (4) argues that scheduling of any end-user verification—or whether to permit it at all—is at the discretion of the government; and (5) will not permit any end-use verification of a U.S. high performance computer at any time after the first six months of the computer's arrival in China.

computer exporters for end use monitoring. Commerce Department officials said that, ultimately, monitoring safeguards plans is the exporters' responsibility.

- - - - -

Mr. Chairman, this concludes my prepared testimony. I would be happy to respond to any questions you or other members may have.

CONTACT AND ACKNOWLEDGEMENT

For future contacts regarding this testimony, please contact Harold J. Johnson at (202) 512-4128. Individuals making key contributions to this testimony included, F. James Shafer and Jeffrey D. Phillips.

APPENDIX PERFORMANCE LEVELS OF COMPUTERS THAT SUPPORT SELECTED APPLICATIONS OF MILITARY SIGNIFICANCE

| Computer performance level (MTOPS) | Applications |
|---|---|
| 4,000 to 6,000 | Joint Attack Strike Aircraft design; nonacoustic antisubmarine warfare sensor development; advanced synthetic aperture radar computation |
| 8,000 to 9,000 | Bottom-contour modeling of shallow water in submarine design; some synthetic aperture radar applications; algorithm development for shipboards' infrared search and track |
| 10,457 to 21,125 | Nuclear blast simulation |
| 15,500 to 17,500 | Computational fluid dynamics applications to model the turbulence around aircraft under extreme conditions |
| 20,000 to 22,000 | Weather forecasting; impact of blasts on underground structures; advanced aircraft design |
| 21,125+ | Submarine design; shallow water acoustics analysis |
| 24,000+ | Automatic target recognition template development |
| = 120,000 | Multi-line towed array signal processing |

Sources: Building on the Basics: An Examination of High-Performance Computing Export Control Policy in the 1990s (1995) and High-Performance Computing, National Security Applications, and Export Control Policy at the Close of the 20th Century.

Hold for Release
Until Delivery
Expected 10:00 a.m.
May 26, 2000

**Statement by**


# Robert J. Lieberman

**Assistant Inspector General for Auditing**
**Department of Defense**

**before the**

## Senate Committee on Governmental Affairs

**on**

## Export Licensing Processes for Dual-Use Commodities

**May 26, 2000**

Mr. Chairman and Members of the Committee:

I appreciate the opportunity to discuss the Federal Government's export licensing processes for militarily sensitive, dual-use commodities and technology. As you know, in response to a request from this Committee in August 1998, Inspector General teams from the Commerce, Defense, Energy, State, and Treasury Departments and the Central Intelligence Agency reviewed a series of issues related to export controls for both dual-use items and munitions. The results were contained in an interagency report and six individual agency reports issued in May and June 1999, and were the subject of your hearing on June 23, 1999. Some of those results are pertinent to the ongoing dialogue on renewing the Export Administration Act of 1979, so I will recap the principal findings on dual-use items as a prelude to commenting on factors that merit consideration in terms of new export control legislation.

Interagency Inspector General Report in June 1999

Dual-use commodities are goods and technologies with both military and commercial applications. The current dual-use export licensing process was established by the Export Administration Act of 1979, as amended. Although the Act

expired in 1994, its provisions are continued by Executive Orders 12924, "Continuation of Export Control Regulations," and 12981, "Administration of Export Controls," under the authority of the International Emergency Economic Powers Act. Munitions exports are controlled separately under the provisions of the Arms Export Control Act.

The dual-use export licensing process is managed and enforced by the Department of Commerce. The Departments of Defense and Energy review the applications and make recommendations to Commerce. The Central Intelligence Agency and the U.S. Customs Service provide relevant information as well. Customs also enforces licensing requirements for all export shipments except outbound mail, which is handled by the Postal Service.

The 1999 interagency IG report included findings in seven areas. Three of those areas are pertinent to new dual-use export legislation.

The first area related to the adequacy of export control statutes and executive orders. We concluded that, in general, the Arms Export Control Act and the provisions of the Export Administration Act, as clarified by Executive Order 12981, were consistent and unambiguous. However, the Commerce and Defense

IG teams stressed that the dual-use licensing process would be best served if the Export Administration Act were reenacted, rather than to continue to operate under a patchwork of other laws and executive orders. In addition, policy and regulations regarding the export licensing requirements for technical information "deemed to be exports" needed clarification, and the exporter appeals process should be formalized.

The second area pertained to procedures used in the export license review processes. The Commerce, Defense, Energy and State IG teams concluded that processes for the referral of dual-use license applications and interagency dispute resolution were adequate. Officials from those Departments were generally satisfied with the 30-day time limit for agency reviews under Executive Order 12981; however, not every agency could meet that limit. Several Defense organizations and the CIA indicated they would benefit from additional time to review dual-use license applications. Another major point was that the Commerce commodity classification process could benefit from additional input on military-related items from the Departments of Defense and State. The commodity classification process matches a prospective export item with an export control classification number. Those determinations indicate whether an item requires

an export license and, if so, whether it is licensable by Commerce or State.

The third area pertained to the cumulative effect of multiple exports to individual foreign countries. The U.S. Government lacked meaningful cumulative effect analysis. Some of the agencies involved in the export licensing process performed limited cumulative effect analyses, but to varying degrees. The Commerce, Defense, Energy and State IG teams concluded that additional cumulative effect analysis would benefit the license application review process.

The IG teams made specific recommendations relevant to their own agencies. Those recommendations and management comments are included in the separate reports issued by each office.

Department of Defense IG Report in June 1999

Now I would like to change focus from the interagency report to the report issued by my office on June 18, 1999. Although our report addressed 14 separate issues posed by Chairman Thompson's August 1998 request, for this testimony I will cover only those that relate to the Export Administration Act.

One issue was whether Commerce was properly referring export license applications for review by other agencies.

Defense officials expressed general satisfaction with referrals of dual-use export license applications from Commerce. Conversely, they were concerned that Commerce referred too few commodity classification requests to Defense for review. In FY 1998, exporters submitted 2,723 commodity classification requests containing 6,161 line items to Commerce. From April 1996 through March 1999, a mere 12 of those requests were referred to Defense for review.

Another issue concerned the interagency dispute resolution process for appealing disputed license applications.

The current interagency dispute resolution process provides multiple appeal levels and has given Defense a reasonable opportunity to appeal disputed dual-use license applications. Executive Order 12981 provides for multiple appeal levels. Agencies can escalate disputes regarding applications successively to the Operating Committee, the Advisory Committee on Export Policy, the Export Administration Review Board and the President. Appeals have been infrequent. For example, the Advisory Committee on Export Policy reviewed an average of

48 cases annually from FY 1996 through FY 1998 and there have been no recent appeals to the President.

Other issues related to whether the current licensing processes adequately took into account the cumulative effect of technology transfers.

We found that the licensing process at the Defense Threat Reduction Agency occasionally took into account cumulative effect, but participants in the licensing process did not routinely analyze the cumulative effect of proposed exports or receive assessments to use during license reviews. In addition, Defense organizations did not conduct required annual assessments that could provide information on the cumulative effect of proposed exports. The Defense Threat Reduction Agency has initiated actions to increase the degree to which cumulative effect analysis is incorporated into the licensing process. We recognize that organizing and resourcing a meaningful cumulative effect analysis process pose a significant challenge, but continue to believe that this is clearly an area warranting more emphasis.

Inspector General Reports in March 2000

We recently completed the first of seven annual interagency audits of technology transfer issues mandated by Section 1402 of the National Defense Authorization Act for Fiscal Year 2000. In conjunction with the Inspectors General of Commerce, Energy and State, we focused this year's review on "deemed exports." The results are included in an interagency report dated March 24, 2000. The DoD portion of the results was included in the interagency report and was also issued by us as a separate report on March 24, 2000.

We reviewed controls related to foreign visitors to Government and contractor facilities. For example, foreign nationals visit Federal research facilities for various reasons, as well as under various international agreements and programs. During those visits, foreign nationals may have access to export-controlled software or technology. The release to foreign nationals of technical data that meet the criteria of the Export Administration Regulations or the International Traffic in Arms Regulations is considered an export. According to those regulations, the oral, visual, or written disclosure of technical data to a foreign national may require a "deemed" export license. In general, there is inadequate awareness of

licensing requirements for "deemed exports" and widespread noncompliance by both Government and industry. This is an area needing more explicit statutory or regulatory guidelines.

Separate classified reports were also issued in response to the additional Authorization Act requirement for a review of counterintelligence issues related to technology transfer.

A New Export Administration Act

In commenting on issues related to a new Export Administration Act, I emphasize that these views are those of the IG, DoD, and do not necessarily reflect the positions of DoD managers or the managers and IGs of other Federal agencies.

As previously mentioned, we believe there is a clear need to reenact the Export Administration Act. During the two decades since that law was enacted, commercial technologies and products have become vastly more applicable to military systems and capabilities, especially in the information technology arena. The Cold War has ended and international trade has expanded. It is vital for our national security that the export control regime for dual-use commodities be firmly grounded in a comprehensive, clear and up to date statute. We further

believe that S.1712, the Export Administration Act of 1999, is a good start toward such a statute; however, it needs to be improved in a few areas. We respectfully offer the following observations and suggestions regarding the control of dual-use technology transfers.

General Process Challenges

Any process prescribed by law or regulation for export controls must strike difficult balances related to efficiency (timeliness) and effectiveness (reasonable and prudent decision making).

Controlling technology transfer is what might be termed a horizontal issue for the Federal Government, in the sense that several agencies and multiple components of those agencies need to participate in any meaningful process. Both within large organizations like the DoD and on an interagency basis, horizontal issues are particularly hard to deal with because Government is organized on a vertical basis. For a cross-cutting process to be effective, there must be objective mechanisms or procedures in place to coordinate agency efforts, resolve conflicting advice and make decisions. It would be

prudent to provide explicit statutory underpinning to the interagency dispute resolution process.

The export control license review process must be able to handle a very large number of transactions expeditiously, but without sacrificing the quality of reviews. The Department of Commerce received 10,696 dual-use export license applications in FY 1998 and 12,650 in FY 1999. We do not have a good insight into the potential for reducing the number of controlled items without undue national security risk, but we are aware that the issue is being discussed within both the Administration and Congress. In addition, the next interagency IG review will focus on both of the existing Control Lists to examine the procedures by which items are added to or deleted from them. Regardless of any changes made to licensing requirements, however, it is virtually certain that the number of export license applications will remain very large. This high volume is a major consideration when both timely processing and due diligence on all application reviews are concerns.

A high volume process will bog down if it is overly complex and if agencies are not willing and able to apply enough resources to execute it effectively. In addition to the sheer volume of export issues to be reviewed, agencies will be continually

challenged by the entry of new technologies and products into the market. This will severely challenge the technical expertise of licensing officials, intelligence analysts and other supporting personnel. Agencies should be required to do sound workforce planning, with emphasis on determining required specialties and training, and to develop mechanisms for rapidly augmenting permanent in-house staff when necessary. Efficient information sharing through the use of the best available information technology is also essential. These kinds of management considerations probably are best addressed through regulation, rather than by statute, to provide flexibility.

National Security Control List

The most meticulously designed and carefully executed export control process will fail if it is easily circumvented. Therefore we urge particularly close attention during the consideration of new statutory and regulatory guidance on determining the makeup of a Control List and on granting exceptions to export license requirements for controlled items.

The Export Administration Act of 1979 required that a list of DoD-developed militarily critical technologies be integrated into the overall Control List of items requiring an export

license. Any disagreement between the Secretaries of Commerce and Defense over the integration of an item on the list of militarily critical technologies into the Control List was to be resolved by the President. We believe those provisions were prudent and any new Export Administration Act should continue to allow appeal, through the interagency dispute resolution process, to the President. No Department should have unilateral control over adding items to the Control List or deleting them.

Determination of Foreign Availability and Mass-Market Status

One potential reason for deciding not to control the export of a technology or product could be that an equivalent item is already widely sold on the international market. In our opinion, a determination not to put or keep an item on the Control List because of foreign availability and mass-market status should never be made without prior consultation with the national security community and, unless the President directs otherwise, the concurrence of the Secretary of Defense.

Although it is unlikely that Defense would do mass-market and foreign availability analyses, the methodology for doing those studies should be clearly defined and well understood by all

agencies that would be interested in the study results. Likewise, all analyses should be well documented and agencies should have formal internal quality assurance procedures to ensure the reliability of their study results. The same principles hold true for cumulative effect analyses.

It would not be the normal role of the IGs or General Accounting Office to perform studies on mass-market and foreign availability or on the cumulative impact of exports to specific countries. However, auditors and evaluators could periodically test the controls for quality assurance for studies. A rigorous peer review program could also be appropriate as part of the quality assurance effort.

Other License Exceptions

We believe it would best serve the national interest to keep any license exception authority fairly limited. Certain high-risk items, for example, those that could contribute to the proliferation of weapons of mass destruction, encryption technology and certain components of jet engines, never should be exported without an export license, regardless of destination.

Commodity Classification Requests

As identified in our 1999 report on the Defense export licensing process, a formal interagency process is needed in determining the commodity classification of an item on the Control List, so that all perspectives can be considered.

Last year, as part of the joint IG review, a statistical sample of 100 commodity classification decisions made by Commerce as well as 3 additional items that were designated as "no license required" were reviewed to determine if a proper commodity classification decision had been made for those items. While Defense was satisfied with Commerce's decision on 90 of the 103 commodity classifications, they felt the remaining 13 were either misclassified or lacked sufficient information. The Commerce and Defense IG teams asked officials to jointly reexamine these 13 decisions. The officials agreed that Commerce had properly classified 4 items and misclassified one item.

There were varying degrees of disagreement on the other 8 decisions. For example, Defense officials questioned a Commerce decision regarding a ruggedized, portable, encrypted radio. Commerce officials stated that the radio had not been

built to military standards and therefore was not a munitions item under the jurisdiction of the International Traffic in Arms Regulations. Defense officials noted that literature described the radio as militarized and other radios built by the manufacturer were subject to munitions export licenses. The second request was for an antenna. Commerce officials stated that the antenna was not a munitions item, despite company literature describing it as militarized. Defense officials stated that the literature satisfied International Traffic in Arms Regulations criteria for a "defense article" (munitions) and that the manufacturer had a history of exporting products under the munitions export licensing process.

Anecdotal evidence provided to the auditors suggested that Commerce could make incorrect commodity classification decisions if it does not receive Defense advice on those decisions. In 1995 and 1997, Commerce decided that microchannel plates (used in night vision devices) fell under the Export Administration Regulations even though Commerce, Defense and State had decided in 1991 that this type of item fell under the jurisdiction of the International Traffic in Arms Regulations. In 1995, Commerce determined that a U.S. aerospace company's accident report on a failed Chinese rocket launch that contained technical data fell under the Export Administration Regulations

rather than the International Traffic in Arms Regulations. In 1996, Commerce determined that a protective suit fell under the Export Administration Regulations, while Defense and State held that it was a chemical and biological defensive suit subject to the International Traffic in Arms Regulations.

I do not have a basis for affirming which position was correct in these cases; however, I believe it is clear that these are difficult decisions and the full range of opinion from various elements of the Government ought to be elicited and considered.

In our view, either a law or regulation should require the Department of Commerce to refer all commodity classification requests promptly for Defense review and allow a reasonable time period for Defense to review those referrals. If there is no agreement on the commodity classification, an interagency dispute resolution process should be initiated to determine the final outcome.

Application Review Procedures

Executive Order 12981 prescribed additional procedures for export license applications submitted under the Export Administration Act of 1979. Among other things, those

procedures required the Department of Commerce to refer all dual-use license applications to the Department of Defense. Last year's interagency review indicated that those procedures have worked fairly well and we believe a new Export Administration Act should provide for their continuation. It should remain mandatory, under any future procedure, that all applications, unless otherwise delegated by the Secretary of Defense, be referred to the Department of Defense for review.

Summary

The Office of Inspector General, DoD, strongly supports the enactment of a new Export Administration Act. This vital area deserves a comprehensive statutory framework that clearly prescribes the roles and responsibilities of all interested Departments and Agencies. We urge that legislation in this area provide to the Secretary of Defense the authority to ensure that national security concerns are carefully addressed in the dual-use export control process.

The stakes involved in technology transfer decisions are apt to be very high for the applicants, the economy, foreign relations and national security. Therefore the process must provide for clear accountability, as much openness as is possible given that

classified matters are often involved, and objectivity. It is vitally important that the process not be perceived as being inherently biased toward the agenda of any particular agency or faction within Government. The best safeguard in that respect is a viable interagency dispute resolution process, applicable to all facets of the export control program and explicitly underpinned by a new Export Administration Act.

The text of the unclassified reports mentioned in this testimony can be accessed on the Web at www.dodig.osd.mil. The numbers and titles are as follows:

No. 99-186, Review of DoD Export Licensing Processes for Dual-Use Commodities and Munitions, June 18, 1999

No. 99-187, Interagency Review of the Export Licensing Process for Dual-Use Commodities and Munitions, June 18, 1999

No. D-2000-109, Interagency Review of the Export Licensing Process for Foreign National Visitors, March 24, 2000

No. D-2000-110, Export Licensing at DoD Research Facilities, March 24, 2000

Thank you for considering our views.

WISCONSIN PROJECT ON NUCLEAR ARMS CONTROL

# Testimony of Gary Milhollin

Professor Emeritus, University of Wisconsin Law School
and
Director, Wisconsin Project on Nuclear Arms Control

Before the Committee on Governmental Affairs
United States Senate
May 26, 2000

1701 K STREET, NW SUITE 805
WASHINGTON, DC 20006
PHONE 202-223-8299 FAX 202-223-8298

I am pleased to appear before this distinguished Committee to testify on the export of dual-use technology. I would like to submit three items for the record. The first is an article on supercomputer export controls that I wrote for the *Outlook* section of the *Washington Post* on March 12, the second is an article on Iraqi procurement efforts that I wrote for the *New Yorker* magazine on December 13, 1999 and the third is a report entitled "25 Myths about Export Control" that my organization prepared a few years ago but which is still relevant to the issues we face today.

The Committee has asked me to comment on two concepts that have been proposed for use in U.S. export controls. The first is known as "mass market status;" the second as "foreign availability." The Committee has asked what the effect would be on our national security if these concepts were adopted as U.S. policy.

The two concepts are now incorporated into S. 1712, the bill recently reported by the Senate Committee on Banking, Housing and Urban Affairs. In my judgment, if this bill were enacted it would overturn and to a great extent nullify the system of export controls that the United States has built up over the past half-century. Our present law attempts to strike a balance between national security and freedom of trade. S. 1712 does not. Instead, it is a one-sided list of provisions advocated by commercial interests that have long opposed any form of export control. It would be more accurate to call the bill in its present form the "Export Decontrol Act."

**Items used to make nuclear weapons and long-range missiles**

One of the most alarming things about the bill is that it would decontrol a series of items that are used to make nuclear weapons and long-range missiles. It would do so by giving the items what the bill calls "mass market status." The items include such things as electronic devices used to trigger nuclear weapons, materials used to build missiles and produce nuclear weapon fuel, and high-speed computers used to design nuclear weapons and the missiles to deliver them.

*1. Nuclear weapon triggers*

For at least twenty years, the United States has controlled for export the high-precision electronic switches needed to detonate nuclear weapons. These are key components in a nuclear weapon's firing circuit and are popularly known as nuclear weapon "triggers." In 1998, Iraq tried to provide itself with a supply of these switches under the guise of medical equipment. Iraq is allowed to import medical equipment despite the U.N. embargo, so Iraq bought a half dozen machines – called "lithotripters" – to rid its citizens of kidney stones. The lithotripter pulverizes kidney stones inside the body – without surgery. But each machine must be triggered by the same high-precision switch that triggers a nuclear weapon. Iraq tried to buy 120 extra switches as "spare parts."

Iraq ordered the machines and switches from Siemens, in Germany, which sold the machines but passed the "spare parts" order to Thomson in France. The French government barred the sale. Siemens says that Iraq did get one switch with each machine and two more as spares, but to get any additional switches, Iraq will have to turn in a used switch for each new one and will have to allow the United Nations to inspect the use of the machines. The switches were controlled for export because they are on the control list of the Nuclear Suppliers Group, an international regime to which France, Germany and the United States belong.

These switches, however, would have "mass market status" under S. 1712, and would be decontrolled for export by the United States. The switches meet all the criteria listed in Section 211 of the bill, and the bill says that the Secretary of Commerce shall remove them from the control list if they meet the criteria. They meet the criteria as follows:

- They are "available for sale in a large volume to multiple purchasers," because they are used in radar, lasers and rockets as well as lithotripter machines and are advertised on the Internet by manufacturers in a number of different countries;

- They are "widely distributed through normal commercial channels," because they are sold by the thousands each year, including the hundreds sent to hospitals to keep lithotripter machines running;

- They are "conducive to shipment and delivery by generally accepted commercial means of transport," because they are small and easy to handle;

- They "may be used for their normal intended purpose without substantial and specialized service provided by the manufacturer," because they need only to be connected into an electrical circuit by attaching the appropriate wires.

Any bill that decontrols nuclear weapon triggers must be seen as seriously flawed.

Despite the fact that these items are available in volume inside the countries that produce them, they are not easily available to countries that are trying to make nuclear weapons. The reason is export controls. If the United States were suddenly to decontrol them, it would dismay our allies and destroy our credibility on nuclear nonproliferation.

*2. Glass and carbon fibers*

Glass and carbon fibers are used widely in ballistic and cruise missiles. They go into solid rocket motor cases, interstages, wings, inlets, nozzles, heat shields, nosetips, structural members, and frames. Composites reinforced by carbon or glass fibers also form the high speed rotors of gas centrifuges used to enrich uranium for nuclear weapons.

In addition to these military applications, however, they are used in skis, tennis racquets, boats and golf clubs and are produced in a number of countries. This availability would give the fibers "mass market status" under the bill, despite the fact that they have been controlled for export since January 1981.

- They are "available for sale in a large volume to multiple purchasers," because they are advertised on the Internet and can be ordered in large quantities by anyone;

- They are "widely distributed through normal commercial channels," because they are shipped in large quantities to manufacturers of sporting goods;

- They are "conducive to shipment and delivery by generally accepted commercial means of transport," because they do not require special handling except for refrigeration in some cases;

- They "may be used for their normal intended purpose without substantial and specialized service provided by the manufacturer," because they can be incorporated in manufacturing processes in the form received.

In 1988, a California rocket scientist was arrested in Baltimore as he tried to illegally load 420 pounds of carbon fibers on a military transport plane bound for Cairo. The material was intended for the ballistic missile that Egypt was developing with Argentina and Iraq. The scientist was sentenced in June 1989 to 46 months in prison. It would be a big surprise to the world if the United States now decontrolled this material.

*3. Maraging steel*

Maraging steel is a high-strength steel used to make solid rocket motor cases, propellant tanks, and interstages for missiles. Like carbon fibers, it is used to make centrifuge rotors for enriching uranium for nuclear weapons. In 1986, a Pakistani-born Canadian businessman tried to smuggle 25 tons of this steel out of the United States to Pakistan's nuclear weapon program. He was sentenced to prison as a result. Maraging steel has been controlled for export since January 1981.

This steel is produced by companies in France, Japan, Russia, Sweden, the United Kingdom and the United States and it meets all the criteria for "mass market status." Several steel companies list maraging steel on the Internet and can produce maraging steel in multi-ton quantities. Over the telephone, two American companies and one British company explained to my staff how to order 25 ton quantities with delivery in less than a month. Maraging steel is bundled and shipped much like stainless steel, which it closely resembles.

*4. Corrosion resistant valves*

These special valves are essential components in plants that enrich uranium to nuclear weapon grade. Both Iraq and Iran are hoping to build such plants, and will need these valves in great numbers. The valves resist the corrosive gas used in the enrichment process.

These same valves are also used in the chemical, petrochemical, oil and gas, fossil power, pulp and paper, and cryogenic industries. Their size can range from very large gate valves down to tiny globe valves used in instrument and control lines. They are manufactured by companies in Australia, Japan, Russia, the United Kingdom and the United States. Smaller corrosion resistant valves have been controlled for export since October 1994, and larger valves have been controlled since October 1981.

These valves fit all of the criteria under Section 211 for "mass market status." They are advertised on the Internet and are widely available to American buyers. A quick survey by my organization revealed that dozens of companies sell them in the hundreds per year. They would therefore be decontrolled under Section 211, to the great delight of Iraq and Iran.

5. *High-performance computers*

The bill would also decontrol high-performance computers as "mass-market" items. This would benefit nuclear weapon and missile designers across the world. High-performance computers can simulate the implosive shock wave that detonates a nuclear warhead, calculate the multiplication of neutrons in an explosive chain reaction and solve the equations that describe fusion in a hydrogen bomb. For missile design, these computers can model the thrust of a rocket, calculate the heat and pressure on a warhead entering the atmosphere and simulate virtually every other force affecting a missile from launch to impact. Because of the billions of computations needed to solve these problems, a supercomputer's speed is invaluable for efficiently finding design solutions.

The United States has always used its highest-performance computers to design nuclear weapons. It is reasonable to expect other countries to do the same. In 1997, the head of Russia's nuclear program, Mr. Viktor Mikhailov, bragged that Russia would begin using American high-performance computers to design nuclear weapons, after Russia had imported several machines illegally from IBM and Silicon Graphics. The new machines were about ten times more powerful than anything the Russians had previously.

China can be expected to do the same. In a study released in 1998, the Department of Energy found that for countries such as China or India to improve their nuclear weapon designs, they will need computers able to perform about 4 billion operations per second. That performance level is right in the middle of the range of computers that President Clinton just decontrolled. If S. 1712 were to become law, industry would demand that even more powerful computers be decontrolled on the ground that they are "mass market" items.

The Commerce Department has argued many times that one can buy powerful American computer chips and assemble them overseas in computers that are difficult to control. However, that argument ignores the important fact that high-speed computers require maintenance and spare parts. Who would build a manufacturing or research complex around a computer system that could not be reliably serviced? Foreign companies are still buying American high-performance computers to the exclusion of virtually all other makes. The reason is simple: American companies provide both reliable products and reliable service. There is still no evidence that foreign competitors can match it.

**Foreign availability**

Section 211 would also decontrol many sensitive items on the ground that they have "foreign availability status." The definition of "foreign availability" in the bill is so sweeping that it covers virtually anything that a controlled country can buy from a rogue supplier. If Iran or Pakistan or Syria can buy a nuclear weapon component or a missile component or a piece of sensitive equipment from China, Russia or North Korea, then the bill would allow our industry to sell the same thing. Under the language of Section 211, even rocket motors would be decontrolled. North Korean rocket motors meet all of the bill's criteria:

- They are "available to controlled countries from sources outside the United States;"
- They "can be acquired at a price that is not excessive;"
- They are "available in sufficient quantity so that the requirement of a license or other authorization with respect to the export of such item is or would be ineffective."

Today, Egypt, Iran, Syria and Pakistan are importing these rocket motors in "sufficient quantities" without any trouble. Requiring a U.S. license for their sale would obviously be "ineffective." Thus, under the literal terms of the bill, they appear to have "foreign availability status." One could argue that a rocket motor is a munition, rather than a "dual-use" item, but these motors can be used for civilian space launchers as well as missiles. Regardless of the classification, however, any definition of foreign availability broad enough to include North Korean rocket motors should be viewed with great suspicion.

**American leadership on export controls**

Many of the provisions of S. 1712 are based on the same principle that children use to excuse their misbehavior: "others are doing it." Industry has managed to persuade the Banking Committee that if another country sells something, so should the United States. What would happen if this idea were actually put into practice?

First, we should remember the Scud missiles that Iraq launched against Israel during the Gulf War. Those missiles were supplied by Russia and their range was enhanced by Germany.

There were German logos on some of the missile parts found in Tel Aviv. Would our industry prefer to see American logos on those parts?

Second, we should remember that the same enhanced-range Scuds killed American troops sleeping in their barracks in Saudi Arabia. Would our industry be proud of having provided the parts that enhanced the range of those missiles?

Third, we should remember that Germany sold entire, turn-key poison gas plants to Libya and Iraq in the 1980s. These were "dual-use" facilities that Iraq said would make pesticides – but the plants turned out to be for "two-legged flies." Would our companies be happier if they had supplied those plants?

Fourth, we should consider that China is now selling missile equipment to Pakistan and selling poison gas equipment to Iran. These items have "foreign availability" written all over them. Does our industry believe it should share in these sales? Are we unfairly excluding American companies from a lucrative market?

By tying U.S. law to that of other countries, U.S. export controls could be no stronger than those of the most lax foreign supplier. It would then be impossible for the United States to play its leadership role. We would be pegged at level of the lowest common offender. The effect would be to reverse a foreign policy stance the United States has maintained for over forty years. It would be an historic abandonment of America's moral leadership.

It is essential for the United States to be able to adopt strong controls first, and then persuade other countries to follow its example. This is the method by which every export control agreement since World War II has been created. U.S. diplomats are using this strategy today to help create export controls in the former East Bloc.

Congress should give the President broad authority to control the export of any dual-use item that is judged relevant to the national security of the United States. National security should be taken to include combating the proliferation of weapons of mass destruction and maintaining the military advantage that the United States now enjoys. The President should not be limited to controlling only what other countries control.

**The power of the national security agencies**

Under Section 202 of this bill, the Secretary of Defense would lose his existing power to put an item on the National Security Control List. Only the Secretary of Commerce would have that power. The Secretary of Defense has the right to be consulted, but that right could only allow the Pentagon to keep an item <u>off</u> the list that the Commerce Department wants to put <u>on</u> it. Since Commerce has always wanted to reduce the number of items controlled, this is a meaningless concession.

Section 211 also allows the Secretary of Commerce to take an item off the list after consulting with the Secretary of Defense, but does not allow the Secretary of Defense to prevent an item from being deleted.

The effect of these provisions is to give the Commerce Department sole power to decide what is controlled for export and what is not. The Secretary of Commerce could – and no doubt would – rewrite the entire National Security Control List without any real restraint by the national security agencies. This is the exact reverse of what the process should be.

The Defense, Energy and State Departments house the experts who understand how dual-use equipment operates and what the risks are if such equipment is diverted for military purposes. They also know which countries and companies in the world are most likely to divert it. These experts are not at the Commerce Department. In order to bring the maximum amount of government expertise to bear upon export control decisions, the qualified personnel at the national security agencies must be able to decide what is controlled and who is allowed to buy it.

But this bill gives the Commerce Department more influence than any other agency. In addition to deciding what will be controlled, Commerce will chair the most important export control committees and will use its administrative preeminence to influence the outcome of licensing decisions.

I hope that this Committee will recall the testimony it received last June from Dr. Peter Leitner, who is a Senior Strategic Trade Advisor at the Department of Defense. Dr. Leitner explained how the influence of technical experts from the national security agencies has been diluted by making them subordinate to a committee of non-specialists chaired by the Department of Commerce.

Congress should ensure that no license application is approved unless all the national security agencies concur. It makes no sense to allow cases to be escalated to the political level where the judgments of national security experts can be reversed by political considerations. If a national security agency takes a stand in opposition to an export application at the expert level, the case should end there.

Instead of being like poor relatives invited to dinner, the national security agencies should be put at the head of the table. Each interagency committee should be chaired by a national security agency. There is no reason to give this function to the Commerce Department, which has the least expertise in the subject matter. And the power to decide what to put on the control list should also be given to the national security agencies. Either the State or the Defense Department should be given the lead in formulating the export control list, with help from the Department of Energy for nuclear items. If export control is going to be a strategic question, instead of a trade question, then the strategic experts should be put in charge of it. That is the only division of labor that makes sense.

**The power of the President**

S. 1712 effectively takes away the President's ability to keep controls in place. The bill provides that the Secretary of Commerce shall determine that an item has mass market or foreign availability status if the item meets the criteria in Section 211. The Secretary must then decontrol the item.

The only way to retain control is for the President to make a special finding within 30 days that exporting the item "would prove detrimental to the national security of the United States." That finding would be impossible to make unless the President could foresee which country would buy the decontrolled item and how the country would use it against the United States. No President can foresee that. And even if the President could foresee it, he could still not stop the export unless there were a "high probability" that foreign supply of the item could be cut off. Is there a "high probability" that North Korea can be persuaded to stop exporting rocket motors?

When one combines the "foreign availability" and "mass market" criteria in this bill, it is hard to see what would be left on the export control list.

These defects are not cured by Section 201(c), which allows controls on items that could "materially" contribute to the proliferation of weapons of mass destruction. This section, in fact, would appear to put the United States in violation of the Nuclear Nonproliferation Treaty. Article one of the treaty obliges the United States "not in any way" to assist a non-nuclear-weapon state in acquiring nuclear weapons. There is no "materiality" exception in the treaty. A series of U.S. exports, each of which standing alone would not be "material," would violate the treaty if the exports "in any way" assisted a nuclear weapon effort. The term "material" is so vague that the Commerce Department could interpret it quite broadly.

**Dangerous buyers**

This past January, President Clinton lowered export controls on high-performance computers. He plans to lower them again later this year. These actions are certain to allow foreign nuclear and missile makers access to American machines. To reduce the risk that American computers will help fuel nuclear and missile proliferation, the United States should publish a comprehensive list of dangerous buyers – in addition to the present list of risky countries. The list would consist of foreign firms known to be linked to nuclear weapon and missile development. The list would not function as a blacklist. It would only be a warning list. Before selling any such company a product that could contribute to the spread of weapons of mass destruction, an exporter would be required to obtain an export license. This would allow the government to turn down dangerous sales without impeding innocent ones, and enable American industry to keep its competitive edge without arming the world. There will always be

the buyer who smuggles, or uses a front company, but that buyer won't get the parts and service needed to keep a high-tech enterprise going.

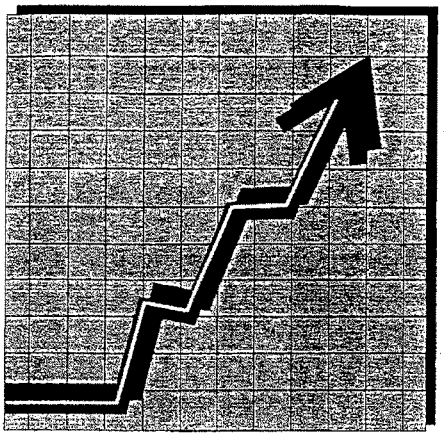
The United States did publish a list of 150 dangerous buyers in India and Pakistan after the two countries tested nuclear weapons in 1998. But so far, our government has not published a comprehensive, worldwide list of such buyers. The U.S. warning list for China, for example, contains only six names. The government has claimed that a more extensive list would reveal intelligence sources and set off diplomatic conflicts. But it is well-known that hundreds of firms in China and Russia are active in nuclear, missile and military production. Their names are not secret. It is silly to pretend we don't know they exist. The computer industry, in fact, would welcome a list of dangerous buyers. Industry would prefer to spend its scarce marketing dollars on buyers that don't present problems.

As a first step in building a list, I have attached to my testimony the names of 50 firms that are well-known parts of China's nuclear, missile and military complex. They have been selected on the basis of reliable, unclassified information. I recommend that the Committee submit these names to the Department of State, and ask for an opinion on whether the names should be included on the published U.S. export warning list. If the State Department judges that these firms should be included, then the Committee should ask the Commerce Department to add the names to the "entity" list in Part 744 of the Export Administration Regulations. American firms should not unwittingly make sales that undermine American security.

**Appendix A to Testimony of Gary Milhollin before the Senate Committee on Governmental Affairs, May 26, 2000**

22nd Construction and Installation Corporation (Yichang)
23rd Construction Corporation (Beijing)
Aviation Industries of China I and II (AVIC) (Beijing)
Beijing Institute of Aerodynamics (BIA) (Beijing)
Beijing Institute of Electromechanical Engineering (Beijing)
Beijing Institute of Electronic Systems Engineering (Beijing)
Beijing Institute of Nuclear Engineering (BINE) (Beijing)
Beijing Institute of Technology (BIT) (Beijing)
Beijing Research Institute of Uranium Geology (BRIUG) (Beijing)
Beijing University of Aeronautics and Astronautics (BUAA) (Beijing)
Beijing Wan Yuan Industry Corporation (BWYIC) (also known as the China Academy of Launch Vehicle Technology [CALT]) (Beijing)
Chengdu Aircraft Industrial Corporation (CAIC) (Chengdu)
China Aerospace International Holdings Ltd. (CASIL) (Hong Kong)
China Aerospace Machinery and Electronics Corporation (CAMEC) (Beijing)
China Aerospace Science and Technology Corporation (CASC) (Beijing)
China Chang Feng Mechanics and Electronics Technology Academy (Beijing)
China Great Wall Industries Corporation (CGWIC) (Beijing)
China Haiying Electro-Mechanical Technology Academy (Beijing)
China Hexi Chemistry and Machinery Company (Beijing)
China Nanchang Aircraft Manufacturing Company (Nanchang)
China National Aero-Technology Import-Export Corporation (CATIC) (Beijing)
China National Aero-Technology International Supply Corporation (CATIC Supply) (Nanchang)
China National Nuclear Corporation (CNNC) (Beijing)
China North Chemical Industries Corporation (NOCINCO) (Beijing)
China North Industries Corporation (NORINCO) (Beijing)
China North Opto-electro Industries Corporation (OEC) (Beijing)
China Nuclear Energy Industry Corporation (CNEIC) (Beijing)
China Precision Machinery Import-Export Corporation (CPMIEC) (Beijing)
China Sanjiang Space Group (Wuhan)
Chinese Academy of Sciences (CAS) (Beijing)
Commission on Science, Technology and Industry for National Defense (COSTIND)
East China Research Institute of Electronic Engineering (ECRIEE) (Hefei)
Harbin Engineering University (Harbin)
Harbin Institute of Technology (HIT) (Harbin)
Hua Xing Construction Company (HXCC) (Yizheng)
Hubei Red Star Chemical Institute (also known as Research Institute 42) (Xiangfan)
Nanjing University of Science and Technology (Nanjing)
National University of Defense Technology (NUDT) (Changsha)
Northwestern Polytechnical University (NPU) (Xian)
Nuclear Power Institute of China (NPIC) (Chengdu)
Research Institute 31 (Beijing)

Shaanxi Institute of Power Machinery (also known as Research Institute 41) (Shaanxi)
Shanghai Institute of Electromechanical Engineering (Shanghai)
Shanghai Power Equipment Research Institute (SPERI) (Shanghai)
Shanghai Xinfeng Chemical Engineering Research Institute (Shanghai)
Shanghai Xinli Research Institute of Power Equipment (Shanghai)
Shanxi Xingan Chemical Material Plant (Taiyuan)
Shenyang Aircraft Corporation (SAC) (Shenyang)
Shenyang Aircraft Research Institute (SARI) (Shenyang)
Xidian University (also known as the Xian University of Electronic Science and Technology) (Xian)



# 25 MYTHS ABOUT EXPORT CONTROL

March 1994

Wisconsin Project on Nuclear Arms Control
1701 K Street, N.W.
Suite 805
Washington, D.C. 20006

In 1941, it took an entire Japanese carrier task force with some 300 planes to inflict 3,000 deaths at Pearl Harbor. Less than four years later, a single American plane dropped a single bomb that killed 100,000 at Hiroshima. A few days after that, a second bomb killed more than 75,000 at Nagasaki, although it missed its target by more than two miles. Since the days when this awesome power was first unleashed, the United States has tried to limit its spread.

It has been axiomatic that the United States would not sell atomic bombs to other countries. And as a corollary, it would not sell the means to make such weapons. Since the 1940s, these two principles have been central to American foreign policy.

First through Cocom, an agreement that successfully denied Western technology to the Warsaw Pact, and then through other agreements not to sell nuclear, chemical and missile technology, the United States and its allies have limited the spread of this technology around the globe. Although controlling exports has never been the sole means of limiting the spread of the bomb, it has been an indispensable part of the effort.

But export control laws are now under siege. The end of the Cold War has triggered pressure from industry to dismantle Cocom, and there is mounting pressure to scale back other export controls as well. But is the world safer after the Cold War? Should less be done to combat nuclear proliferation?

The Export Administration Act is now before Congress and a group of American exporters has mounted an unprecedented campaign to weaken this vital law. If they succeed, developing countries will find it easier to build atomic bombs and long-range missiles under the Clinton administration than they did under either presidents Bush or Reagan.

These exporters hope that Congress and the public have already forgotten the Gulf War. U.N. teams inspecting Iraq found factories full of Western equipment--machines that U.S. pilots died trying to bomb, and that almost gave Saddam Hussein a nuclear weapon. The inspectors wrote in their reports that to stop Saddam from reviving his bomb program, there must be "strict maintenance of export controls by the industrial nations." And

by 1992, the Bush administration had concluded that Iran was following the same purchasing strategy as Iraq--buying Western "dual-use" equipment to make nuclear weapons.

The lesson is therefore clear: the export of American high technology must not come at the expense of American security. Yet, if the claims now being made by some exporters are believed, that is precisely what will happen. Congress and the administration are being bombarded with so much misinformation that exporters' claims have risen to the level of myths. The purpose of this report is to reintroduce some balance into the debate, by pairing some of the myths with statements of reality.

## THE TWENTY-FIVE MYTHS

**Myth #1:** Export controls do not work. They will never stop the spread of weapons of mass destruction.

**Reality:** Export controls do work. They buy the time needed to turn a country off the nuclear weapon path. Argentina and Brazil agreed to give up nuclear weapons mainly because of the costs that export controls imposed upon them. And in Iraq, secret documents showed that export controls on dual-use equipment seriously hampered the Iraqi nuclear weapon design team. The Iraqis spent time and money making crucial items that they could not import. The same controls also stopped Iraq's drive to make a medium-range missile--one that would have been invulnerable to U.S. Patriot defenses. In addition, these controls are now hampering India's effort to build an ICBM.

**Myth #2:** Dropping export controls will create jobs, the Clinton administration's main priority.

**Reality:** Export controls have only a microscopic effect on employment. The total American economy was about six trillion dollars in 1992. Of that, only <u>four tenths of one percent</u> ($23.7 billion) even went through Commerce Department licensing. And only $790 million in applications were denied--which is <u>one hundredth of one percent of the U.S. economy</u> and less than half the cost of one B-2 bomber. If the American economy were equivalent to a dollar, only four tenths of a penny's worth would go through export control and only one hundredth of a penny's worth would be denied a license. Gutting export controls stimulates proliferation, not the U.S. economy.

**Myth #3:** Export controls are less important after the Cold War.

**Reality:** In fact, they are more important. With bipolar stability gone, regional tensions are growing. These tensions stimulate the appetite for weapons of mass destruction. The nuclear and missile arms race is still on between India and Pakistan, and still on in the Middle East. As CIA director Woolsey said in his confirmation hearings, "we have slain a large dragon, but we live now in a jungle filled with a bewildering variety of poisonous snakes." It is illogical to say that because the Cold War is over, proliferation is the main international threat, and then to say that export controls, which are one of the best ways of containing that threat, should be reduced.

**Myth #4:** The end of the Cold War has made East-West controls irrelevant.

**Reality:** These controls are still important. Cocom, the Coordinating Committee on Multilateral Export Controls, was built up after World War II to keep Western technology away from the Warsaw Pact. But Cocom is due to end on March 31 with nothing effective to replace it. Western goods will flow into the former East Bloc before those countries can control their own exports. Thus, Western goods run the risk of being reexported through the former East Bloc to Iran, Iraq, Libya or Syria. The East Bloc is now part of the proliferation problem.

**Myth #5:** Export controls are still locked into the Cold War mode; they must be reduced to reflect new conditions.

**Reality:** Export controls have already been cut drastically since the Cold War. Since 1988 applications to the Commerce Department have dropped by 75%. Cases have fallen from nearly 100,000 in 1989 to about 25,000 in 1993. The value of goods individually licensed has dropped from over $100 billion a few years ago to just over $20 billion last year, and is expected to fall to only $10 billion in 1994. The reason is simple: fewer items are controlled, and so fewer applications are required. Further cuts will only help nuclear and missile aspirants like Iran and Libya, whom former CIA director Gates accused in 1992 of trying to procure high-technology items for rocket motors.

**Myth #6:** Export controls put U.S. business at a competitive disadvantage.

**Reality:** Licensing has little impact on sales. Over 98% of export applications are approved. Over the past four years, the Commerce Department has denied an average of only 323 cases annually, an insignificant number of transactions. Moreover, virtually all advanced countries now control their exports in the same way the United States does. Thus, in over 98% of the cases covered by export controls--which in turn are only a tiny fraction of overall American exports--business suffers no greater burden than filling out a form. U.S. foreign military sales have grown steadily despite control by the State Department's munitions list. And American firms have already regained the market share they lost in the early 1980s, making the United States again the world's leading exporter.

**Myth #7:** U.S. exporters lose sales because approvals take too long.

**Reality:** The Commerce Department is now meeting its licensing deadlines in 97% of its applications. The average time for approval is only nine days--unless the Commerce Department refers the case for interagency review. The Department of Energy, to which Commerce refers nuclear cases, turns them out so rapidly that Energy spends an average of less than 40 minutes on each.

**Myth #8:** Export controls cost U.S. businesses over $20 billion per year in lost sales.

**Reality:** This claim is purely speculative, and it defies common sense. The amount claimed to be lost is nearly equal to the total value of goods licensed yearly by the Commerce Department. Yet over 98% of applications are approved. But even if $20 billion were lost, it would amount to only three tenths of one percent of the American economy. This amount is insignificant compared to the cost of fighting a nuclear Desert Storm, or to the cost of fighting a nuclear war on the Korean peninsula.

**Myth #9:** Export controls must be multilateral to work.

**Reality:** Unilateral controls are also essential. Since World War II, multilateral controls have been set up by U.S. example--America adopted unilateral controls <u>first</u> and

then asked other countries to follow suit. U.S. diplomats are using this strategy today to help create export controls in the former East Bloc. International leadership is always unilateral. If the United States had waited for Europe, Japan and the Arab countries to agree on what to do when Iraq invaded Kuwait, Iraq might still possess Kuwait today. Instead, America acted unilaterally and asked others to join--using the same strategy it has adopted for export control. Unilateral controls also reflect moral values. The United States did not sell poison gas plants to Libya and Iraq because Germany did, or agree to sell nuclear reactors to Iran and Pakistan because China did, or sell large rockets to India because Russia did. Would a U.S. firm enjoy seeing its logo on the Russian and German-supplied Scuds that hit Tel Aviv?

**Myth #10:** There should be a short time limit on all unilateral controls.

**Reality:** It can take years for the United States to convince its allies to adopt multilateral controls. In 1992 the Nuclear Suppliers Group agreed to control more than 60 items that the United States had controlled unilaterally for nonproliferation reasons for over a decade. Premature decontrol of these items by the United States would have prevented this important victory.

**Myth #11:** U.S. export controls limit the sale of items that are readily available abroad.

**Reality:** Such items are rarely available. Only a few companies can supply the items now left on export control lists. These lists have been cut drastically in the 1990s, so that only the highest-technology items remain. Almost all of the makers of such items are in advanced countries--countries that use controls similar to those of the United States.

**Myth #12:** If a foreign competitor is willing to sell an item, showing "foreign availability," American firms should be able to do the same.

**Reality:** This pushes export control down to the level of the worst abuser. Germany sold Iraq more pieces of dangerous equipment before the Gulf War than all other countries combined. If American policy had been as lax as Germany's, Saddam's bomb program would have advanced

much faster. And for exports to Iran, U.S. policy would now have to be relaxed because of sales by Germany, Japan and Switzerland. Moreover, U.S. officials acknowledge that estimates of foreign availability are too imprecise to dictate export policy. Instead of indexing U.S. law to foreign availability, which only benefits proliferators, the United States should pressure new supplier nations to join multilateral control efforts.

**Myth #13:** Export controls should be dropped when an item is superseded by advances in technology.

**Reality:** The bombs dropped on Hiroshima and Nagasaki are "obsolete" by modern standards. Should they be exported? Should the means to make them be exported? The first U.S. intercontinental ballistic missiles are also obsolete and after the Gulf War, U.N. inspectors discovered that Iraq nearly made an atomic bomb with the inefficient "calutrons" that the United States abandoned in the 1940s. It is no consolation to be killed by a bomb made with obsolete equipment.

**Myth #14:** The biggest emerging markets for American goods are in "sensitive" countries.

**Reality:** This is <u>not</u> true of items controlled for export. Only the highest-performing equipment is now left on control lists. In most of the sensitive countries, only the military is advanced enough to make use of such equipment, or has the money to buy it. The main civilian markets for these items are, and will be, in the developed world. If an exporter cannot survive by selling to its main market, it will not survive through risky sales to a marginal market.

**Myth #15:** License applications only create a mountain of paperwork, costing U.S. exporters time and money.

**Reality:** The benefit of licensing outweighs its burden. In addition to preventing dangerous sales, licensing provides an essential tracking function. It allows U.S. and foreign officials to identify buying patterns that can unmask a country's true intentions. Most exporting firms are accustomed to licensing and go through it with ease. Rather than eliminate this valuable process, it should be made more efficient.

**Myth #16:** U.S. exports are controlled by a maze of regulations, agencies and special committees that impede rather than help exporters.

**Reality:** The present system brings the maximum expertise to bear in the shortest possible time. To judge an export application, one must understand how the item could be used to make a weapon of mass destruction, whether the importer is reliable, and whether the claimed use is technically credible. No single government agency has the expertise to do this. The present system relies on experts from the Departments of Defense, Energy and State, and from the CIA and the Arms Control and Disarmament Agency. An interagency process is therefore indispensable. Leading U.S. allies have adopted a similar interagency process. The reason is simple: without referrals there is no expertise, and without expertise one cannot make a competent export decision.

**Myth #17:** The way to "streamline" licensing is to reduce interagency review and give more power to the Commerce Department.

**Reality:** The Commerce Department has no substantive competence in strategic technology. Its current function is to manage the flow of cases, referring them to the proper experts in other agencies. It would be a mistake to give Commerce a substantive role for which it is not equipped. Commerce also has a conflict of interests--it must promote exports as well as regulate them. This promotion function is the dominant one; it causes Commerce invariably to champion the exporter's cause. In 1991, Commerce officials even altered export records on Iraq before submitting them to Congress, doing so in order to conceal embarrassing approvals. In light of its record in Iraq, the role of Commerce in export licensing should be reduced and the roles of the national security agencies should be increased.

**Myth #18:** We need "higher fences around fewer goods." Only "chokepoint" technologies should be controlled--items specially designed to make weapons of mass destruction.

**Reality:** This ignores the lesson of Iraq. Saddam Hussein's scientists were masters at upgrading medium-tech items to "chokepoint" level. The Iraqis imported equipment that was "dual-use"--capable of making nuclear weapons or long-range missiles but also having civilian applications. The Iraqis bought dual-use isostatic

presses to shape A-bomb parts, dual-use mass spectrometers to sample A-bomb fuel, and dual-use electron beam welders to increase the range of Scud missiles. One of those increased-range Scuds killed U.S. troops sleeping in Saudi Arabia. Iran is now following the same purchasing strategy as Iraq. There is no hope of stopping proliferation without controlling dual-use equipment; current U.S. export laws reflect that fact. If "higher fences around fewer goods" is carried to its conclusion, there will be a very high fence around assembled hydrogen bombs, and no controls on the means to make them.

**Myth #19:** The United States should agree to a license-free zone with other nations that join nonproliferation control regimes.

**Reality:** This step would destroy the regimes. Iran, Iraq, Libya, North Korea and Syria all joined the Nuclear Nonproliferation Treaty, but it would be folly to sell them nuclear technology. The United States is not about to do so. Nor is it ready to sell them dual-use technology. Likewise, Spain and Italy adhere to the missile technology control regime and want to buy large space rockets. But Spain is reported to be developing a multi-stage missile that will reach North Africa and neither Spain nor Italy can adequately control its own exports. Thus, U.S. rocket technology sold to these countries could be reexported to the very countries against which the regimes are targeted. If an item that only the United States makes is freely sold to the other 25 members of the missile control regime, there would then be 25 potential suppliers to proliferators instead of only one.

**Myth #20:** Export controls should be based on destination, not on the item sold, which would isolate rogue countries without hurting sales to other markets.

**Reality:** This would simplify the process by gutting it. Unscrupulous buyers would set up front companies in non-prohibited countries with weak controls and then transship the item to prohibited countries. The Iraqis were masters at this. End-use or end-user checks only catch a small number of violations, because the checking process is costly and because front companies can disappear overnight. An export system based on destination alone leaves honest U.S. exporters more vulnerable to having their equipment turn up in the next Iraq. Moreover, it is diplomatically difficult to

name a risky buyer like Syria, which is participating in the Mideast peace process, as a rogue nation. Germany, for example, will not even agree that Iran is a rogue nation.

**Myth #21:** Export controls are easily defeated by smuggling.

**Reality:** After the Cold War, Cocom officials toured the former East Bloc to measure the impact of Cocom controls. East Bloc officials said that smuggling was sometimes successful, but spare parts and service were difficult or impossible to obtain. Thus, smuggled equipment often became inoperable, making it risky to build manufacturing operations around it. The way to deal with smuggling, like street crime, is not to abolish laws, but to improve enforcement.

**Myth #22:** It is unfair to require a license for low-tech goods simply because the exporter "knows" the goods will be used to produce weapons of mass destruction.

**Reality:** This rule does not bar exports; it only requires a license; and 98% of license applications are approved. Germany and the United Kingdom also have this rule. U.S. exporters have lived for years with the rule for nuclear goods; during the Bush administration it was merely expanded to cover missile and chemical weapon development. The rule encourages the exporter to know his customer and it allows the government to track dangerous programs and slow them down.

**Myth #23:** High-speed computers are not important for nuclear weapon or missile development.

**Reality:** The U.S. National Laboratories invented high-speed computers expressly to design nuclear weapons. They are also used to design missile components. They drastically cut the time and money needed for weapon development and they reduce or eliminate the need for tests. The absence of tests can mask a program from detection. In many developing countries, the only institutions that can absorb supercomputer-level technology are run by the military. Decontrolling these computers will allow many Third World countries to build more powerful bombs and missiles, and to build them faster.

**Myth #24:** High-speed computers are widely available on the world market.

**Reality:** Only a few countries manufacture such computers, and these countries coordinate their exports with the United States. Moreover, this claim is refuted by publicly-available Commerce Department data. In December 1993, Commerce found that computers were available from foreign sellers only at a speed of 67 Mtops (millions of theoretical operations per second). Only a few years ago, a level of 100 was deemed a supercomputer, powerful enough to deny to proliferant countries. Under industry pressure, however, U.S. computers are now being decontrolled up to a level of 500 Mtops, a dangerous and unnecessary action that will undermine U.S. security.

**Myth #25:** The 1993 report to Congress by the administration's Trade Promotion Coordinating Committee (TPCC) is a reliable guide to export policy.

**Reality:** The TPCC was created to promote exports. It had no mandate to balance trade against security. Its report relied on the advice of more than 2,000 representatives of export interests, and presents the exporters' point of view. It advocates the most radical reduction in U.S. export controls ever made. Because export control has only a microscopic effect on jobs, the report promotes proliferation but not the U.S. economy.

THE NEW YORKER



# THE TALK OF THE TOWN

THE NEW YORKER, DECEMBER 13, 1999

## DEPT. OF MASS DESTRUCTION

*Saddam's nuclear shopping spree.*

EVER since the United Nations weapons inspectors were shut out of Iraq, a year ago, the world has been left to wonder what Saddam Hussein is up to. Well, now it can be told: he has been secretly trying to transform his desert dictatorship into a world-class center for the treatment of kidney stones.

Or so it would seem, to judge from his latest purchases on the international medical-equipment market. Although Iraq remains under a strict United Nations embargo, the embargo does not cover medical supplies. Last year, the Iraqi government ordered half a dozen lithotripters, which are state-of-the-art machines for getting rid of kidney stones. (The word "lithotripter" comes from the Greek for "stone breaker.") A lithotripter uses a shock wave to pulverize these painful objects without surgery. Machines like the ones Iraq bought require a high-precision electronic switch that triggers a powerful burst of electricity. In addition to the lithotripters, Iraq wanted to buy a hundred and twenty extra switches. That is at least a hundred more than the machines would ever need.

Iraq's strange hankering for this particular "spare part" becomes less mysterious when one reflects that the switch in question has another use: it can trigger an atomic bomb. According to a knowledgeable U.N. inspector, each bomb of the type that Iraq is trying to build requires thirty-two switches. Thus, a hundred of them would outfit three bombs. It is hardly a coincidence that, as the former U.N. inspector Scott Ritter testified at a Senate hearing last year, the inspectors had "intelligence information which indicates that components necessary for three nuclear weapons exist" in Iraq. Saddam Hussein has been shopping for what he needs to make sure they work.

Iraq went to Siemens, the German electronics giant, to place the order. Before the Gulf War, Iraq acquired Siemens computers and other equipment useful for processing uranium to nuclear-weapons grade, and the company provided electrical equipment for one of Iraq's main missile sites. (Siemens has denied helping Iraq advance its nuclear program.) In this instance, Siemens forwarded the switches order to its supplier, Thomson-C.S.F., a French military-electronics company. The French government promptly barred the sale. Stephen Cooney, a Siemens spokesman, refuses to say whether Siemens nevertheless filled the switch order, or even whether the order was placed. If Siemens made the deal, Iraq got a powerful nuclear boost.

The Clinton Administration has been relatively quiet on Iraq lately. Although it maintains that it remains suspicious of Saddam, it claims to have no specific evidence that he has resumed his efforts to build weapons of mass destruction. The kidney-stone affair suggests otherwise.

The U.N. inspectors have learned that Iraq's first bomb design, which weighed a ton and was just over a yard in diameter, has been replaced by a smaller, more efficient model. The inspectors have deduced that the new design weighs only about one thousand three hundred pounds and measures about twenty-five inches in diameter. That makes it small enough to fit on a Scud-type missile. The inspectors believe that Iraq may still have nine such missiles hidden somewhere.

The inspectors have also concluded that Iraq's bomb design will work. Iraq, they believe, has mastered the key technique of creating an implosive shock wave, which squeezes a bomb's nuclear material enough to trigger a chain reaction. The new design also uses a "flying tamper," a refinement that "hammers" the nuclear material to squeeze it even harder, so bombs can be made smaller without diminishing their explosive force.

How did Iraq progress so far so quickly? The inspectors found an Iraqi document describing an offer of design help—in exchange for money—from an agent of Pakistan. Iraq says it didn't accept the offer, but the inspectors think it did. Pakistan's latest design also uses a flying tamper. Regardless of how the Iraqis managed to do it, Saddam Hussein now possesses an efficient nuclear-bomb design. And, if he did succeed in getting hold of the necessary switches, then the only thing he lacks is enough weapons-grade uranium to fuel the warheads.

The fuel, unfortunately, is getting easier to find. United States officials report that on May 29th Bulgaria seized approximately a third of an ounce of weapons grade uranium at its border. The not cargo, accompanied by documents in Russian, was concealed in a lead container in a pump stowed in a car. A third of an ounce is not enough for a bomb (Iraq's design, for example, needs thirty five pounds), but this seizure and others like it show that weapons-grade fuel is beginning to circulate in the black market. Unless the U.N. Security Council can agree on a plan to reinstate meaningful inspections, Saddam may be able to complete his nuclear shopping sooner rather than later. —GARY MILHOLLIN

The Washington Post

OUTLOOK

A LOOK AT . . .
Exporting Trouble

SUNDAY, MARCH 12, 2000

**HIGH-PERFORMANCE COMPUTERS** *aren't like most other products that U.S. companies sell abroad. They're more like weapons, the author argues.*

# With Looser Computer Controls, We're Selling Our Safety Short

By GARY MILHOLLIN

Israel has begun to outfit Chinese planes with a powerful new radar, one reportedly able to see targets and help direct air battles as far as 250 miles away. The Clinton administration has been trying to stop this deal, but it is facing a formidable barrier: its own desire to promote U.S. exports.

In fact, the deal is getting a boost from Uncle Sam. The Commerce Department has allowed Israel's premier maker of military radar, Elta Electronics Industries, to buy two high-performance computers from Sun Microsystems Inc. of Palo Alto, Calif. Elta will be able to use them to outfit the Chinese planes cheaper, faster and better.

This means that if the United States ever has to defend Taiwan, American pilots could be targeted by radar built with American equipment.

Unfortunately, this alarming sale is just a drop in the flood of computers the administration has decided to let American companies sell abroad. On Jan. 23, President Clinton lowered export controls that had blocked scores of American high-performance computers from being shipped to nuclear and missile programs in countries including China, India and Russia.

The truth is, high-performance computers aren't like most other exports—they're more like weapons. They are essential to develop the software and hardware that make things like advanced military radar work. And one of the driving forces behind the development of "supercomputers" has always been the desire to design better nuclear weapons and the missiles that deliver them.

That is why Congress has required a control process for international sales. A U.S. manufacturer must notify the government if it wants to sell a high-performance computer to a buyer in a "proliferant" country like China or Israel; then it must wait 10 days. If any federal agency is suspicious of the buyer, the exporter must request a formal license. In practice, roughly 90 percent of the sales meet with no objection. The process, therefore, does not seriously impede exports.

Before Jan. 23, any computer capable of more than 2 billion operations per second fell under those rules. After that date, the bar rose to 6.5 billion operations per second. The administration also plans to decontrol computers performing up to 12.5 billion operations per second later this year. (By comparison, the most popular new desktop PCs perform 1.2 billion to 1.5 billion operations per second.)

These new rules will, for the first time, allow a string of foreign weapons makers to buy powerful American computers that had been specifically denied to them.

Consider some of the buyers who were blocked by the old rules from purchasing high-performance computers from Digital Equipment Corp.: China's Harbin Institute of Technology, which makes rocket casings and other components for China's long-range nuclear missiles; the Weizman Institute in Israel, which researches high-energy physics and was the birthplace of Israel's nuclear weapons effort; the Nanjing (China) Public Security Bureau, whose mandate includes tracking political dissidents.

All those proposed sales involved computers operating between 2 billion and 6.5 billion operations per second. Under the loosened rules, the sales will be able to take place without government interference. Whether they happen or not is up to Compaq Computer Corp., which owns Digital.

And Compaq is not the only company that could profit from the looser rules. IBM was turned down when it tried to supply three computers to China's Northwest Polytechnical University, which develops engines and guidance systems for large rockets and trains China's missile forces.

And, of course, there is Sun Microsystems: The two computers it is selling to the Israeli radar maker, Elta Electronics, slip beneath the new control level. So does the computer Sun had previously tried to sell to the Rafael Armament Development Authority, which played a major role in developing Israel's largest nuclear-tipped missile.

What will these countries do with such computers? Could China use them to make better atomic bombs? Yes. In a study released in 1998, the Department of Energy found that for countries such as China or India to improve their nuclear weapon designs, they will need computers able to perform about 4 billion operations per second. That performance level is right in the middle of the range that Clinton just decontrolled.

How many computers will be exported? According to the General Accounting Office, the old rules have blocked at least 85 high-speed computers from going to potentially dangerous buyers since 1998. These buyers included Chinese organizations "reportedly engaged in military or proliferation activities" and Indian companies "engaged in missile proliferation. . . ."

Astonishingly little money is at stake in these transactions. According to the export license applications, the sale to China's Harbin Institute was valued at $348,000; the sale to Weizmann at $41,000; and Sun's sale to Rafael at $25,000. Put this in context: Compaq, for example, has an annual revenue of roughly $31 billion. Why would such a wealthy company want to outfit nuclear plants in sensitive regions of the world for a few hundred thousand dollars? With so much risk to reputation, what is the motivation?

The companies don't have a convincing answer. Dan Hoydysh of the Unisys Corp., who acts as spokesman for the big computer exporters, comes closest to providing one. "These computers are going to be available from any number of foreign manufacturers, so it makes no sense to control them," Hoydysh told me. He argues that if U.S. controls weren't loosened, foreign competitors would step in and make the sales that American companies can't. The White House accepts this argument. It is contradicted, however, by the independent evidence.

American makers of high-speed computers have almost no foreign competition. Virtually all the computer chips in the world are made by American companies. In 1998, the GAO found that "U.S. companies and their international business partners overwhelmingly dominate the international market for supercomputers." Only three firms in Japan provided competition, the GAO said, and Japanese export controls are at least as stringent as those in the United States. The GAO reiterated its findings as recently as last November. Another 1998 study, by the Commerce and Defense departments, reached the same conclusions.

Perhaps the most understandable argument against export controls is the astonishing proliferation of increasingly powerful computer chips. Yesterday's supercomputer is today's student laptop. Just as it is impossible to stem the spread of information in the age of the Internet, the companies say, the number of powerful computer chips is outstripping the government's ability to regulate them. "Controlling these machines is simply not feasible," Hoydysh contends.

He cites IBM's Aptiva line of personal computers, sold with a chip rated at 2.1 billion operations per second, and Apple's G4 personal computer, which can perform 2.7 billion. Both exceed the previous control level of 2 billion. Apple, in fact, began a TV ad for the G4 with the words, "For the first time in history, a personal computer has been classified as a weapon by the U.S. government. . . ."

Hoydysh is right that things are changing, and that computers once considered dangerous have become commonplace. That doesn't mean we should put them into unreliable hands. A machine performing 2, 4 or 6 billion operations per second is still a threat in the hands of an arms maker, however many such machines already exist—just as the prevalence of handguns doesn't make the one pointed at you any less lethal. The real question is whether it is still feasible to prevent fast computers from going to foreign weapon sites, where they will clearly do harm.

It is feasible, to a great extent, if the government has the will. It would be simple for the United States to publish a comprehensive list of dangerous buyers—in addition to the present list of risky countries. Before selling any computer to an entity on the buyers list, an exporter would have to get a license. This would allow the government to turn down dangerous sales without impeding innocent ones, and enable American industry to keep its competitive edge without arming the world. There will always be the buyer who smuggles, or uses a front company, but it won't get the parts and service needed to keep a high-tech enterprise going.

The administration did come out with a list of 150 dangerous buyers in India and Pakistan after the two countries tested nuclear weapons in 1998. But so far, it has refused to publish such a worldwide list, saying it would reveal intelligence sources and set off diplomatic conflicts. That is ridiculous: Hundreds of firms in China and Russia are active in nuclear, missile and military production. Their names are well-known. It is fatuous to pretend we don't know they exist.

The computer industry, indeed, would welcome such a list. "We would support any government effort to identify entities engaged in dangerous activities," Hoydysh says. "If the government tells us who the bad guys are, we won't sell to them." This makes perfect economic sense. Industry wants to concentrate on buyers that don't present problems.

The industry's true motive seems to be a desire to be forever first—first in the buyer's door with the highest processing speed. "Market access" is the term Hoydysh uses. By maintaining that advantage, American firms hope to prevent foreign firms from ever gaining a foothold. Any restriction on the freedom to sell—such as export controls—is seen as a risk. The price of the strategy, of course, is that bomb and missile makers around the world will achieve their goals faster and more efficiently with American equipment.

It is time for the administration to understand that there is more to foreign policy than promoting trade. It is easier, safer and more economical to stop dangerous exports than to defend against the weapons they produce. The revenue isn't worth the risk. And it is time for the computer industry, which sees itself as forever young, to grow up and accept responsibility for the nation's security.

**STATEMENT OF DAN HOYDYSH**

**CO-CHAIR OF THE COMPUTER COALITION FOR RESPONSIBLE EXPORTS**

**BEFORE THE SENATE GOVERNMENTAL AFFAIRS COMMITTEE**
**UNITED STATES SENATE**

**MAY 26, 2000**

Mr. Chairman, Members of the Committee.

Good Morning. My name is Dan Hoydysh. I am Director, Trade, Public Policy & Government Affairs of the Unisys Corporation. I also have the privilege of serving as Co-Chair of the Computer Coalition for Responsible Exports (CCRE) and am testifying today on CCRE's behalf (a curriculum vitae and required disclosures are attached). I want to thank you for providing me and the CCRE with the opportunity to share our views on U.S. computer export controls.

The CCRE is an alliance of American computer companies and allied associations established to inform policy makers and the public about the nature of the computer industry -- its products, market trends, and technological advances.

CCRE Members include Apple Computer, Inc., Compaq Computer Corporation, Dell Computer Corporation, Hewlett-Packard Company, IBM Corporation, Intel Corporation, NCR Corporation, SGI, Sun Microsystems, Inc., Unisys Corporation, the American Electronics Association (AEA), the Computer and Communications Industry Association (CCIA), the Computer Systems Policy Project (CSPP), Electronic Industries Alliance (EIA), and the Information Technology Industry Council (ITI).

The CCRE is committed to promoting and protecting U.S. national security interests, and seeks to work in close partnership with the Congress and the Executive Branch to ensure that America's economic, national security, and foreign policy goals are realized. CCRE also believes that a strong, internationally competitive computer industry is critical to ensuring that U.S. national and economic security objectives are achieved and that U.S. economic and technological leadership is maintained.

The U.S. computer industry has a long history of cooperation with the U.S. government on security-related high technology issues. They take their responsibilities in the area very seriously. CCRE members strongly believe that U.S. national security is tied to U.S. technological leadership. U.S. computer companies also devote hundreds of employees and millions of dollars annually to complying with export control regulations. It is not our role, however, to define U.S. national security needs - - that is for the Congress and the Executive Branch. Rather, we do and will continue to provide the Congress and Executive Branch with information concerning the rapidly changing technology and international market conditions that we believe they will need to take into consideration in shaping up-to-date and effective U.S. export control policies for computers.

In our testimony today we want to make the following key points given the trends in computer performance over the foreseeable future: (1) a responsive and efficient export control regime is essential to maintain U.S. leadership in the information technology industry; (2) a 6-month delay in implementing adjustments to the computer export controls is too long and a considerably shorter period should be adopted by this Congress; and (3) technological and market realities both support the Administration's February announcement to update the Tier III export control thresholds and confirm the need for a further update.

## I. The Export Control System Needs to be Changed

As you know, the U.S. computer industry continues to be a driving force behind our continued economic growth and job creation and is responsible for one-third of real economic growth. U.S. computer companies need to innovate, grow, and compete in new markets. the industry's strength and vitality have been important factors in maintaining our national security. Export controls can have profound effects on the health of such industries and on their contributions to the national security. The Defense Science Board's Task Force on Globalization and Security, an independent Federal Advisory Committee to the Department of

Defense, comprising many distinguished experts in national security, specifically points out the role between export controls and the health of the U.S. computer industry:

> Exports are now the key to growth and good health. In the computer and communications satellite industries, for example, between 50% and 60% of all revenues come from foreign sales. Any significant restriction on exports would likely slow corporate growth and limit the extent to which profits can be put back into research and development on next-generation technology. . . . If U.S. high-tech exports are restricted in any significant manner, it could well have a stifling effect on the U.S. military's rate of technological advancement.

DSB Report at 27.

CCRE believes that in the long term fundamental reform of the computer export controls is necessary. As the computer industry's experience with the present export control regime clearly shows, there is a need for a more efficient and responsive new computer export control system. A performance based computer export control system is proving difficult to administer given the rapid advances in computer performance levels and the global availability of components and know-how. In light of this reality, we urge that the Congress and the Executive Branch, with the support and assistance of the computer and other high-tech industries, continue their bipartisan consideration of new methods of achieving the national security goals presently associated with computer export controls.

In the short term, however, the CCRE supports the ongoing effort to modernize and reauthorize the Export Administration Act (EAA), but believes that the EAA should adequately reflect current foreign policy, national security and market realities. The result of past efforts failing to reauthorize the EAA has been an increasingly outdated U.S. export control regime built on the remains of a Cold War-era statute. S. 1712, the Export Administration Act of 1999, presents a valuable first step to clear away conflicting export control systems and modernize the U.S. export control regime to reflect market realities.

## II. The Process for Updating Export Controls on Computers Should be Streamlined

In 1997, the House Armed Services Committee correctly predicted that export controls on computers would need to be updated periodically. Consequently, the Congress provided a means for adjusting those controls in the FY 1998 NDAA. That process, however, includes a waiting period of 6 months before new export control thresholds become effective. The 6 month waiting period has, however, proved to be too long for the rapid changes that take place in our industry.

Just last week the U.S. House of Representatives overwhelmingly approved an amendment to the National Defense Authorization Act for FY 2001 that would shorten the waiting period from 180 days to 60 days before new rules governing computer export controls can take effect. The House approved the amendment by a 415-8 vote. The amendment was offered by House Rules Committee Chairman David Dreier (R-CA), Armed Services Committee Ranking Member Ike Skelton (D-MO), International Relations Committee Chairman Ben Gilman (R-NY), and Ellen Tauscher (D-CA). The amendment was also supported by Armed Services Chairman Floyd Spence (R-SC). The House vote is a clear recognition that the six-month waiting period is not consistent with technological and competitive reality. The support for the amendment by those members concerned about U.S. national security supports the notion that the reduction will actually help strengthen national security by ensuring that U.S. companies maintain their technological preeminence, upon which the U.S. military superiority ultimately depends.

In addition, when the Senate Banking Committee reauthorized the Export Administration Act last year, it also recognized (i) that a 6-month waiting period is too long for an industry, like the computer industry, that needs to get its latest products to market before foreign competitors

capture those markets, and (ii) that a considerably shorter waiting period would still protect the national security. Since then, Senators Harry Reid (D-NV) and Robert Bennett (R-UT) have also offered seperate legislation in the Senate, S. 2539, that would reduce the waiting period.

The House of Representatives, the Senate Banking Committee, and Senators Reid and Bennet are correct. A shorter waiting period will still give the Congress adequate time to review the national security ramifications of any changes in the U.S. computer export control laws and allow the U.S. computer industry a chance to compete in some of the most important emerging markets in the world.

The House NDAA Amendment and the other initiatives would make the waiting period more reasonable and bring it into line with other waiting periods for changing national security export controls. For example, 6 months is considerably longer that the 30-day waiting period established by Congress to remove defense articles from the Munitions List (a list of defense articles and services that are subject to export controls, including such items as artillery, launch vehicles, missiles, rockets, torpedoes, warships, aircraft and tanks).

Indeed, recent events have demonstrated clearly that the 6-month waiting period is so long that it is impossible for the computer export controls to keep pace with current technological and market realities. Last fall Apple Computer began marketing its new single-processor personal computer whose power exceeded the then current computer export control threshold. Apple was unable to sell those new G4 computer systems in over 50 countries because the export control adjustments made in July did not become effective until January. IBM was in a similar predicament with its new Aptiva personal computer line. We believe that this recent experience in the harm caused by a 6-month delay in adjusting the export control threshold demonstrates clearly the urgent need to reduce the waiting period from 6 months.

Furthermore, it is quite clear that foreign computer companies are positioned to take advantage of markets closed to U.S. computer companies while the U.S. companies are waiting for the 6-month waiting period to run its course. If U.S. companies have to wait until the export controls are updated as much as six months later, foreign computer companies selling comparable computers will reap the significant benefit of being "first to market." As you know, for high technology products being "first to market" is a critical commercial fact of life. The U.S. computer industry will soon be facing a crisis when computer systems with the new Intel Itanium™ come on the market, but are still controlled by outdated export control thresholds. At present, at least five foreign firms (NEC, Siemens, Hitachi, Fujitsu, and Bull) have already indicated that they intend to market computer systems with the Itanium. Those foreign computer companies will reap all the advantages of "first to market" in some of the most important growing markets in the world, while our computer companies face the barriers of the pre-export notification and licensing process. Once lost, foreign markets will be very hard to recover.

According to the DSB, export controls under these circumstances could very well harm the national security:

> DoD should attempt to protect for the purposes of maintaining military advantage only those capabilities and technologies of which the U.S. is the sole possessor and whose protection is deemed necessary to preserve an essential military capability. Protection of capabilities and technologies readily available on the world market is, at best, unhelpful to the maintenance of military dominance, and, at worst, counterproductive (e.g., by undermining the industry upon which U.S. military-technological supremacy depends).

DSB Report at vii.

This change is critically important to the U.S. computer industry. We urge you to support these initiatives to reduce the NDAA waiting period.

## III. The Technological and Market Realities of the Global Computer Industry Support the February Announced Update and Confirm the Need for Another Update this Year

In February, the President announced that the computer export control threshold for Tier III countries would be increased from 6,500 MTOPS to 12,500 MTOPS in light of the widely available computers that would be performing in that range. The update will take effect six months later, following the 6-month waiting period. Unfortunately, because of the 6-month waiting period, this recent update to 12,500 MTOPS will quickly be out of date because Intel's new microprocessor, the Itanium, will soon be available - domestically and overseas. The Itanium will be used primarily in widely available multiprocessor business computer systems. The business computers at issue are used in such businesses as banks, telephone companies, productions and engineering facilities, offices, as well as in providing the backbone of the Internet and e-commerce. Four-way multiprocessor Itanium systems are presently projected to perform above 23,700 MTOPS. Another update of the Tier III computer export controls is therefore necessary as soon as possible to take into account these new widely available products.

The business computers at issue are widely available because (A) of the increasing power of widely available microprocessors, that (B) are employed in increasingly common multiprocessor systems (with correspondingly higher performance levels) that are widely used in business applications, and (C) global computer market trends mean that multi-processor computers are so widely available that many are now commodities.

### A. Increasing Processing Performance Trends Support the February Proposal to Adjust the Computer Export Controls

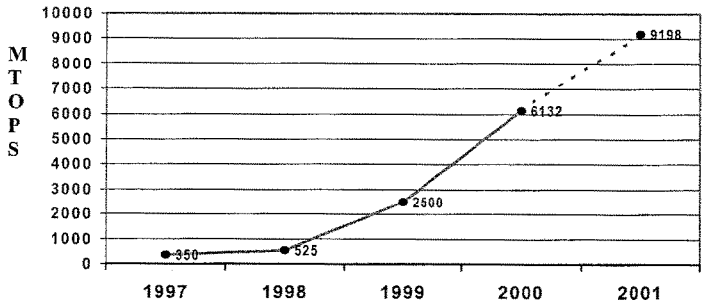
The recent increases in microprocessor performance are one of the main factors supporting the proposed adjustment and the need for another adjustment. The performance of

microprocessors (chips) -- the brains of the computer -- continues to improve dramatically. Gordon Moore, the former CEO of Intel once observed "that the power of semiconductor technology doubles every 18 months." However, the pace of technological advance is accelerating even faster.

In March of 1999 the Pentium® III Xeon™ microprocessor, then the state-of-the-art mass market processor used in multiprocessor systems, performed at 1167 MTOPS (500 MHZ). Eighteen months later the state-of-the-art mass market microprocessor is forecast to be Intel's Itanium, with performance of 5622 MTOPS. *Thus in 18 months, instead of doubling, the performance of mass market microprocessors will have quintupled - increased by almost 500%.*

The following table demonstrates the performance level of widely available single microprocessors made by Intel and other companies: The impact of the Itanium is readily apparent in the sudden increase this year.

**Performance of Widely Available Single Microprocessors**



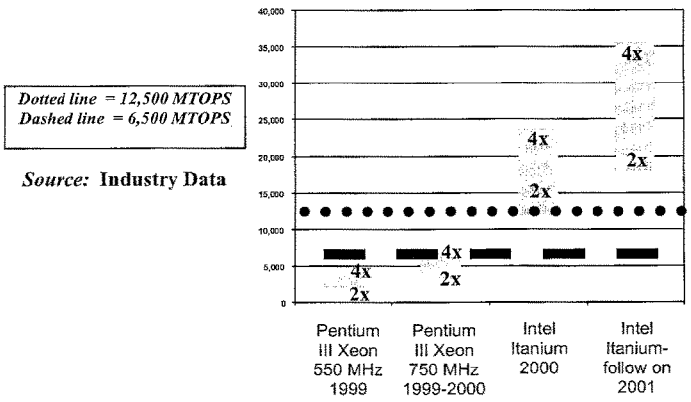

***Source:*** **Industry data based on Intel & other microprocessors**

**B. The Trend of Increasing Performance Through the Use of Multiprocessor Systems Supports the February Announcement and the Need for Further Adjustments this Year.**

Another major factor supporting the February announcement and confirming the need for another update is the increasing usage of multiprocessor computer systems. Multiprocessor systems using the latest microprocessors are now widely available on the world market. According to projections in the Gartner Group Report, this year over 4.3 million computers that can accommodate two processors, over 500,000 computers that can accommodate 4 processors, and over 125,000 computers that can accommodate 8 processors will be sold world-wide. The Gartner Group Report projects that by the end of this year, the installed worldwide base of computer systems that can accommodate 2, 4, 6, and 8 processors should be approximately 14 million, while by the end of 2001 there will be over 20 million such computers installed worldwide.

The following chart and examples using Intel technology illustrate the dramatic increases in widely available multi-processor power that is resulting in an ever increasing number of computers performing in the range covered by the President's proposal and forecast to perform above the recent update.

**Power of Widely Available US and foreign computer systems**




A review of the present widely available microprocessors available domestically and overseas clearly shows that the February announced update was necessary. Today the 550 MHZ Intel Pentium III Xeon, which performs at about 1300 MTOPS, is the basic building block of multiprocessor servers using Intel architecture. A computer system using two 550 MHZ Intel Pentium III Xeon microprocessors performs at about 2400 MTOPS, while one using four microprocessors performs at about 4600 MTOPS, and one using eight microprocessors performs at about 9000 MTOPS. It is projected that the 550 MHZ Intel Pentium III Xeon will very soon be replaced by the 750 MHZ Intel Pentium III Xeon (1750 MTOPS), with computer systems using two of those microprocessors performing at 3250 MTOPS, while one using four microprocessors will perform at 6250 MTOPS, and one using eight microprocessors will perform at 12,250 MTOPS.

However, this year it is also expected that the Intel Itanium microprocessor will soon be available for use in multiprocessor servers using Intel architecture. By the end of this year, systems with two Itanium microprocessors are projected to perform at just under 12,000 MTOPS, while one with four microprocessors is projected to perform just under 24,000 MTOPS. Furthermore, in the second half of next year the follow-on to the Itanium is projected to have a 2-way performance of just under 18,000 MTOPS, and a 4-way performance of just under 36,000 MTOPS. In addition, the follow-on to the Pentium, the Foster, will also soon be widely available. In the first half of next year an 8-way Foster is projected to perform just under 27,000 MTOPS. The February announced update to 12,500 MTOPS will clearly fail to cover these widely available systems. Unless we are prepared to concede some of the most important growing markets in the world to foreign manufacturers providing these systems, the computer export controls will need another update as soon as possible to cover the expected sales of these systems.

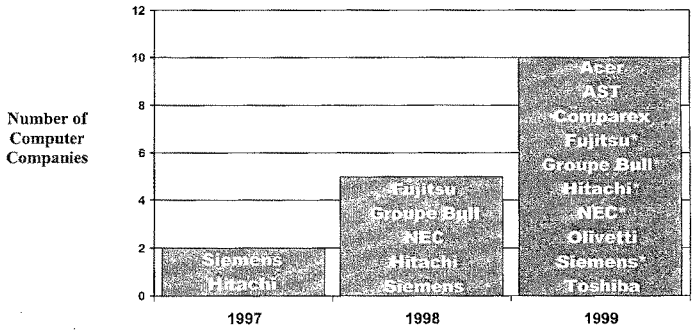
### C. Global Computer Market Trends of Increasing Use of Multiprocessor Systems Support the February Announcement and the Need for Another Adjustment

Any review of proposals to adjust computer export controls should take into account global computer market trends - - both the foreign availability of multiprocessor computers, as well as the foreign capability to manufacture computers that would be subject to export controls. In addition, the overseas installed base of computers that would be subject to export controls is also relevant to the effectiveness of any export control regime.

#### (1) Foreign Availability and Capability

The number of foreign computer companies and the number of products they offer that compete at higher performance levels is increasing all the time as computer technology continues to advance and is available overseas and at relatively low cost. The chart on the next page shows

the increasing number of foreign computer companies that are marketing servers and workstations that can perform in the range covered by the proposed adjustment to the computer export control laws.




***Source*: GartnerGroup for 1997-1999.**
***Companies that have announced they will market Intel Itanium computers in multiprocessor configurations pending Itanium release in July 2000.**

Computer companies in France (Bull), Japan (Hitachi, NEC, Fujitsu, Mitsubishi and Toshiba), Taiwan (Acer and AST), Germany (Siemens and Comparex), and Italy (Olivetti) are all making 2 and 4-way multiprocessor computers. Many of these companies are already marketing or have announced that they will be selling 8-way computers (e.g. Bull, Comparex, NEC, Hitachi, Fujitsu, and Siemens). (See Attachment 1 for specific details on these foreign computers.)

Most significantly, it should also be noted that NEC, Siemens, Hitachi, Fujitsu, and Bull have already indicated that they will be employing the Intel Itanium in multi-chip computers. Thus, even before its release, it is clear that this new powerful microprocessor will be available in multiprocessor systems worldwide.

Indeed, the Gartner Group Report forecasts that this year foreign computer manufacturers will sell over 20,000 eight-way configurable computers, almost 140,000 four-way configurable computers, and almost 950,000 two-way configurable computers. In 2001, the Gartner report projects that over 1,300,000 two-way computers and over 150,000 four-way computers will be manufactured by foreign computer companies. Many of these foreign computer systems will be using widely available microprocessors that will have performances for 4-way configurations above 20,000 MTOPS.

The DSB Report explicitly discusses foreign capability based on uncontrollable commodity microprocessors:

> Microprocessors, which are the essential ingredient for high-performance computers (HPCs), have long been a commodity product widely available on the world market from a vast range of sources. Chip-maker Intel alone has over 50,000 authorized dealers worldwide.

DSB Report at 26-27.

In addition, foreign end-users can also achieve high performance levels, in excess of the thresholds in the February announcement, through networking commercial off-the-shelf inexpensive computers. Indeed, this view is supported by a statement from the Cox Committee Report:

> According to officials at the Lawrence Livermore National Laboratory, networking represents only a ten percent additional cost over the cost of computing hardware for large systems. Thus, up to approximately 50,000 MTOPS, the computing capability available to any country today is limited only by the amount of money that is available to be spent on commercial-off-the-shelf networking.

(Cox Committee Report, Volume 1, Chapter 3/Technical Afterword, at 158). Furthermore, the Cox Committee Report notes that there are networking technology installations in 17 foreign

countries, including India, Israel, and the PRC. (Id.) The DSB Report also considered the impact of clustering:

> The technology to "cluster" these computers (i.e. link then together to multiply their computing power) is also available online. Through clustering, it is possible to create computer systems ranging in computing power from 4,000-100,000 MTOPS (millions of theoretical operations per second)-equivalent to the supercomputers currently under strict export controls.

DSB Report at 26-27.

Finally, it should be noted that our foreign competition are not constrained by export controls to the same extent as is the U.S. computer industry. The end of the Cold War and the demise of effective multilateral export controls has essentially freed our foreign competition from such constraints. Indeed, the DSB remarked on just this point when it examined the effectiveness of U.S. export controls:

> In the wake of CoCom's dissolution, a chasm has developed between the U.S. and many of its Western allies, who no longer view China as a threat and have relaxed or lifted dual-use export restrictions to China accordingly.

DSB Report at 26. The DSB also commented on the effectiveness of today's multilateral controls.

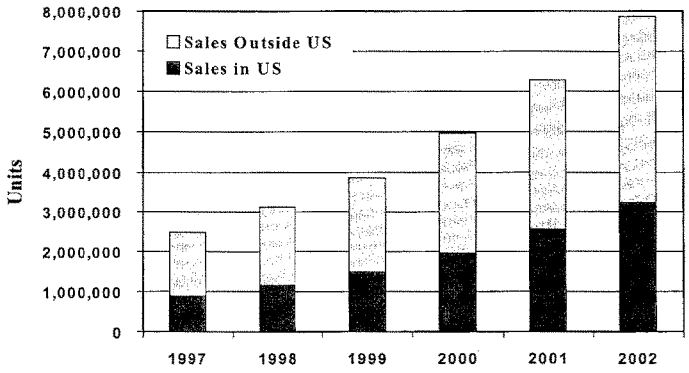
> [M]ultilateral controls today are for all practical purposes ineffective at manipulating global access to dual-use technologies

Id.

(2) Foreign Installed Base

As computer technology advances and is spread around the world, the installed base of computers that can perform above current export control thresholds will continue to grow. In

**Worldwide Unit Sales of Multiprocessor Systems (2x-8x)**




*Source*: GartnerGroup
Figures for 1998 - 2002 are projected

addition to providing data on technology advances, the Gartner Group Report also provided data on international market trends. The Report shows that there is presently a large overseas installed base of servers and workstations, many of which perform in the range covered by the proposal. The following chart shows the increasing foreign installed base.

The Gartner Group Report forecasts that by the end of this year, over eight million multiprocessor servers and workstations will have been sold overseas by U.S. and foreign computer manufacturers. The Report also forecasts that by the end of this year over one million computers that can be configured with up to four microprocessors will have been sold overseas.

Accordingly, the large installed base of computers outside the United States cannot be ignored when considering changes to the computer export controls. The larger the installed base -- the more difficult it is to implement an effective export control system.

## V. Conclusion

The discussion above concerning the changing performance levels of business computers and the intense global competition confronting the U.S. computer industry clearly shows that there is a present and clear need for long-term changes as well as immediate updates in the export control regime for computers and that such changes are consistent with the national security. CCRE is committed to working with the Congress and the Executive Branch in determining the adjustments that will be necessary in light of the technological and market realities.

STATEMENT OF DAN HOYDYSH

CO-CHAIR OF THE COMPUTER COALITION FOR RESPONSIBLE EXPORTS

BEFORE THE SENATE GOVERNMENTAL AFFAIRS COMMITTEE
UNITED STATES SENATE

MAY 26, 2000

**Attachment 1**

FOREIGN COMPETITION

There is substantial foreign commercial availability of multiprocessor systems comparable to U.S. multiprocessor systems. For example, the following systems are on the market this year:

**Acer (Taiwan)** Altos 21000 with up to four Intel Pentium III Xeon processors at 550 MHz. Forthcoming Altos servers will run at over 600 MHz.

**AST (Taiwan)** Premium 2000H with up to two Pentium III processors at up to 700 MHz.

**ATEC (Thailand)** NexusTM 700 with dual Pentium III 450 MHz processors.

**Comparex (Germany)** S1000-890 with up to 8 Pentium III Xeon processors.

**Fujitsu (Japan)** Teamserver T890ie with up to 8 Pentium III Xeon 550 MHz processors.

**Fujitsu Siemens (Germany)** GP7000f Model 2000 with up to 64 SPARC64 processors. Primergy N800 & K800 with up to 8 Pentium III Xeon 550 MHz processors. Celsius 630 workstation with up to 2 Pentium III Xeon 550 MHz processors.

**Groupe Bull (France)** EPC2400 with up to 32 nodes and 24 Power PC RS64 III processors per node. HV8600 with up to 8 Pentium III Xeon processors.

**Hitachi (Japan)** MP6000 with up to 8 ACE2 processors.

**Legend (China)** WanQuan 4000 server with 4 processors.

**NEC (Japan)** Supercomputer SX4 with up to 512 processors.

**Tatung (Taiwan)** TNS-3000PS & 3000 PW with up to 2 Pentium III 800 MHz processors. TNS 3000XW & XS workstations with up to 2 Pentium III Xeon 800 MHz processors.

INSERT FOR THE RECORD

RESPONSE FROM MR. JOHNSON FOR SENATOR LIEBERMAN'S QUESTION

Question: Is it clear that the United States has the legal authority to undertake extensive post-shipment verifications to see exactly how exported high performance computers are being used?

Answer: Two United States laws specifically authorize the Secretary of Commerce to conduct post shipment verifications. Section 12(a) of the Export Administration Act of 1979, as amended,[1] authorizes the Secretary of Commerce to conduct post-shipment verifications of items licensed for export. This would include licensed export of high performance computers. Commerce Department regulations also authorize the Bureau of Export Administration to impose certain safeguard conditions as part of a license for export of these computers. The specific conditions that may be imposed depend on the country of destination and the end-use or end-user.[2] Conditions 32 and 33 require end-users to cooperate with the United States Government or exporting company officials in conducting comprehensive post-shipment verifications.[3] Nevertheless, since these safeguard conditions are included as license conditions, they would not cover high performance computers that are exported without a license.

Another law, section 1213 of the National Defense Authorization Act for fiscal year 1998,[4] requires the Secretary of Commerce to conduct a post-shipment verification of each high performance computer of more than 2,000 MTOPS that is exported from the United States, with or without a license, to a tier 3 country. Although Commerce Department

[1] 50 U.S.C. § 2411(a)(1).
[2] 15 C.F.R. § 742.12(b).
[3] 15 C.F.R. § pt. 742, Supplement 3.
[4] Public Law No. 105-85, 111 Stat. 1934.

regulations require exporters to submit post-shipment verification reports to BXA regarding export of these high performance computers, there is no requirement for the exporter to provide information about how the computer is being used.

Even in the absence of the specific safeguard conditions described above, Commerce maintains that section 12(a) of the Export Administration Act and section 1213 of the National Defense Authorization Act are sufficiently broad so as to allow it to undertake post-shipment verifications that determine how an exported computer is being used. This would include checks by highly trained technicians who could go in and look at data in the computer, the computer codes and the computer's programming. As the authorities described are quite broad and without restriction, we generally agree with Commerce's position. Nevertheless, it is doubtful that these United States domestic laws would bind foreign countries or foreign importers. Thus, absent inclusion of the described safeguard conditions in a licensed export, the extent to which the Commerce Department or an exporter could conduct a post-shipment verification would depend on the foreign country or importer's consent. Of course, if a foreign country or importer refused to allow a comprehensive post-shipment verification, Commerce could take that into consideration in granting future licenses.

Even in situations where foreign countries or importers permit comprehensive post-shipment verifications, there may be funding restraints on Commerce's ability to conduct them. As we mentioned in our testimony, conducting comprehensive post-shipment verifications are very expensive and thus it is not clear that Commerce has the necessary resources available to conduct them on any broad scale.

RESPONSES TO QUESTIONS FOR THE RECORD FROM MR. JOHNSON

GAO

United States
General Accounting Office
Washington, D.C. 20548

Office of Congressional Relations

**ANSWERS TO QUESTIONS**
**FOR THE RECORD**
**SENATE GOVERNMENTAL AFFAIRS COMMITTEE**
**HEARING ON EXPORT CONTROLS**
**MAY 26, 2000**

(1) Does the GAO have any idea of the cost incurred to the government of reviewing computer export licenses and then the cost of inspection visits to end-users?

No. GAO has not developed data on either the cost of reviewing computer export licenses nor the cost of inspection visits to end users. General information that we have for aggregate inspection visits indicates that the Office of Export Enforcement assessed the results of 497 post-shipment verifications (PSVs) completed during fiscal year 1999. Of these PSVs, 330 were conducted by Export Enforcement special agents as part of the Safeguards program, while the other 167 were conducted by Foreign Commercial Service or other personnel assigned by American Embassies. Twenty-six PSVs produced information that required further enforcement action.

(2) Has the General Accounting Office ever examined the cost of our export licensing process, including all the various agencies involved, and, if so, what were GAO's recommendations for more cost efficient procedures?

No. GAO has not examined the cost of the export licensing process.

(3) One of the issues relating to the time provided to the Congress to review licenses has been GAO's turn around time to examine controversial cases. On average, could you estimate for me how long it would take GAO to investigate a license application if the Congress asked GAO to do so? I know this is to some degree a subjective question but I would appreciate your best response because, as you know, there is legislation pending before this Congress which would shorten our review time.

GAO does not investigate license applications. It twice has been asked to review a mandated report from the President justifying changes in control levels for computer exports. Our reviews have been done to assist Congress in its review of executive branch changes in the export controls for computers. Current law requires a 180-day notification period to Congress before certain changes in controls can become effective.[i] Language in the current version of S. 1712 and in amendments introduced in the House would reduce this interval to either 30 or 60 days. The most recent assessments performed by GAO were completed 4 to 5 months after the executive branch decision. These assessments could be completed sooner if we were to receive information from Commerce more expeditiously.

---

[i] Under the National Defense Authorization Act (NDAA) of1998, Congress has 180 days to review NDAA notification level changes and 120 days to review changes to the Tier 3 country list starting the day the President notifies Congress in writing of said changes. (Source: http://www.bxa.doc.gov/HPCs/Default.htm)

RESPONSE TO QUESTION FOR THE RECORD FROM MR. MILHOLLIN

WISCONSIN PROJECT ON NUCLEAR ARMS CONTROL

July 11, 2000

Ms. Hannah Sistare
Staff Director and Counsel
Committee on Governmental Affairs
United States Senate
Washington, D.C. 20510-6250

Dear Ms. Sistare:

I am pleased to respond to the question for the record submitted by Senator Akaka. Senator Akaka's question is directed to my testimony of May 26, 2000 on the control of high-performance computers exported from the United States.

My response to Senator Akaka's question is as follows:

"Maintenance of high-performance computers can be required, for example, because of problems with memory units and problems with interfaces between busses and boards. For massively parallel systems, writing operating software can be difficult because of the need to integrate multiple independent data streams. If the software application does not function properly, maintenance of the software is required and the software may be written specifically for the high-performance computer in question."

Thank you for the opportunity to respond to Senator Akaka's question.

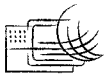
Sincerely yours,

Gary Milhollin

Gary Milhollin

1701 K STREET, NW SUITE 805
WASHINGTON, DC 20006
PHONE 202-223-8299 FAX 202-223-8298

RESPONSES TO QUESTIONS FOR THE RECORD FROM MR. HOYDYSH



**Computer Coalition**
**for Responsible Exports**

June 29, 2000

Hannah Sistare
Staff Director and Counsel
Committee on Governmental Affairs
United States Senate
Washington DC 20510-6250

Dear Ms. Sistare:

Following our testimony before the Committee last month, Senator Akaka asked us to respond to a few specific question related to U.S. export controls on computers. Below are the questions and our responses.

**Question 1.**

**Q:** Which countries that export high-speed computers require their Defense Ministries to review computer License?

**A:** It is our general impression that Defense Ministries are normally not involved in reviewing export license applications for commercial items such as computers.

CCRE suggests that you consult the U.S. Commerce Department or State Department for a more detailed response.

**Question 2.**

**Q:** What other countries require end user certificates and inspections of end-users of HPCs in China?

**A:** Again, this question could better be answered by the Commerce Department or State Department. However, to the best of our knowledge, the United States is the only country that requires end-user certificates for, and inspections of, HPCs exported to China.

**Question 3.**

**Q:** You have considerable experience in government, could you tell me why every Administration since President Reagan has eased export controls on computers?



1341 G Street, NW Suite 1100
Washington, DC 20005
(202) 585-0217 *fax* (202) 393-0712
Website: www.ccre.net

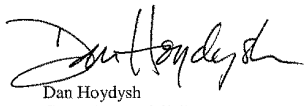
**A:** Every Administration has eased export controls on computers to reflect advances in technology and changing market realities. For example, the first major computer decontrol occurred in 1985 under the Reagan Administration when microprocessor-based PCs were decontrolled. These systems were decontrolled because they were being produced in large volumes by domestic and foreign producers. During the Bush Administration the threshold for controlling "supercomputers" was raised from 100 MFLOPS to 160 MFLOPS and then to 195 MTOPS (MFLOPS and MTOPS are roughly equivalent measures).

Each Administration raised computer control thresholds because they realized that attempting to control the uncontrollable is ineffective and counterproductive. It is ineffective because it does not prevent the target from acquiring HPCs and it is counter productive because it dilutes government resources that would otherwise be available for policing truly sensitive exports.

* * *

If there is anything else we can help with, please do not hesitate to let us know. We remain committed to working with you to help develop effective and meaningful export control policies which both protect U.S. national security and ensure continued U.S. technological leadership and global competitiveness.

Sincerely,



Dan Hoydysh
Co-chairman, CCRE
Director of Trade Policy
Unisys, Corporation