

WITHDRAWAL SHEET

Clinton Library

Collection: Clinton Administration History Project

Archivist: JGP

OA/Box: [24116] [3]

File Folder: Dept. of Commerce – Bureau of Export Administration

Date: 8/2/04

DOCUMENT NO. & TYPE	SUBJECT/TITLE	DATE	RESTRICTION
1. Memo to File	From John Sopko; re: China Spy Timeline, 1p. (partial)	3/17/99	P1/BI Unclass.

RESTRICTIONS

- P1 National security classified information [(a)(1) of the PRA].
- P2 Relating to appointment to Federal office [(a)(2) of the PRA].
- P3 Release would violate a Federal statute [(a)(3) of the PRA].
- P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA].
- P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [(a)(5) of the PRA].
- P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA].

C. Closed in accordance with restrictions contained in donor's deed of gift.

- B1 National security classified information [(b)(1) of the FOIA].
- B2 Release could disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA].
- B3 Release would violate a Federal statute [(b)(3) of the FOIA].
- B4 Release would disclose trade secrets or confidential commercial financial information [(b)(4) of the FOIA].
- B6 Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA].
- B7 Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA].
- B8 Release would disclose information concerning the regulation of financial institutions [(b)(9) of the FOIA].
- B9 Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA].

**KEYNOTE ADDRESS
UNDER SECRETARY WILLIAM A. REINSCH
BUREAU OF EXPORT ADMINISTRATION
U.S. DEPARTMENT OF COMMERCE**

**UPDATE 2000
WASHINGTON, DC**

JUNE 10, 2000

INTRODUCTION

Welcome to BXA's thirteenth Update conference. It is a pleasure to be here and to again have the opportunity to discuss our Nation's export control policies. But this year the opportunity is bittersweet, as this is the final Update of this Administration, and the last time I expect to appear before you.

It is with this in mind that I want to indulge in a bit of history of what we have done over the past seven and half years as well as some of the challenges we and our successors will face in the days ahead.

When this Administration began its work, we were at a crossroads in U.S. strategic trade policy. The design of our export control system was antiquated and its process creaky, having been designed for the Cold War, when political relationships were less ambiguous.

Our goal was to build a strong Western alliance as a bulwark against Communism. Our security was tied to keeping advanced capabilities out of our adversaries' hands. This meant keeping our best technology from reaching beyond our borders.

Then the world changed dramatically. The familiar framework we had followed for nearly a half-century required new flexibility to deal with more ambiguous, but equally real emerging threats. Instead of bipolar simplicity, we face a number of rogue states -- or should I say "states of concern?" -- bent on acquiring weapons of mass destruction and destabilizing their regions through acts of terrorism.

The Administration realized early on that rapid technological change and economic globalization compelled comprehensive reform of our export control system which balances the need to keep sensitive goods and technologies out of the hands of countries and projects of concern without imposing unnecessary or ineffective constraints on business. That is why we liberalized outdated controls, streamlined our existing export control system, enhanced our enforcement programs, and helped to strengthen multilateral regimes.

Among other things, we:

- updated and liberalized controls on high performance computers, semiconductors and semiconductor equipment, Beta-test software, telecommunications equipment, and chemical mixtures and samples, among others.
- streamlined controls on encryption products to support the growth of electronic commerce and help industry maintain its leadership in research, market share, and competitiveness while protecting our national security and law enforcement priorities.
- completed the transfer of jurisdiction of commercial communication satellites and commercial jet engine hot section technology from the State Department 's Munitions List to the Commerce Control List, although the Congress subsequently moved satellites back -- an action they are already regretting.
- amended our control list of nuclear items to conform more closely with that of our allies, and expanded the number of countries to which exporters can ship nuclear-controlled items via license exception.
- eased sanctions to open markets in Cuba and North Korea for U.S. industry to provide needed food and medical supplies to distressed populations there.
- clarified and simplified the Export Administration Regulations through the first comprehensive revision and reorganization in 40 years, making them clearer and more user-friendly.
- simplified our regulations for the export clearance process to provide flexibility so that exporters can structure their transactions as they wish. We also reduced the size of the regulations as well, slashing the "Exporter of Record" regulation, for example, from 19,000 words to 6,000.
- improved the license process by broadening agency review opportunities while limiting the time for those reviews, providing an orderly procedure to resolve Interagency disputes, and establishing more accountability throughout the interagency process. While average times are a bit longer, we have effectively eliminated the black hole into which licenses were frequently falling.
- developed the Special Comprehensive License, which allows experienced, high volume exporters to export a broad range of items under a single license.
- supported the Automated Export System to better facilitate exports by allowing data to be submitted directly through electronic submissions.
- created the Simplified Network Application Process to allow exporters to submit license applications quickly and easily on-line. Since its inception in February 1999, SNAP has received 8,973 license applications from 2,033 registered users representing 1,044 companies. This is 54% of all license applications received.

- helped create the Wassenaar Arrangement, which established multilateral controls on exports of conventional arms and sensitive dual use equipment.
- worked to strengthen other multilateral nonproliferation regimes, which, in turn, enhances U.S. exporters' ability to compete on a level playing field.
- instituted the License and Enforcement Action Program or LEAP to increase industry understanding of its rights and obligations. While this is a work in progress, LEAP is already redoubling our efforts to enhance compliance, standardize the conditions applied to licenses, expand end use visits, increase reviews and spot checks of license exceptions, institute broader information sharing with the intelligence community, and expand outreach efforts.

LIBERALIZING CONTROLS

In liberalizing controls, we have focused on narrowing the range of these controls to cover only the most critical products and technology. Our rationale is clear. We do not protect national security by unnecessarily controlling widely available, older generation products.

This is perhaps the most fundamental change in philosophy this Administration has made, and a considerable part of my job has been to explain and defend it. You have heard me articulate our basic equation before: strong exports = strong high tech companies = a strong defense = improved national security.

This equation is based on our realization that the new era we live in is one where the military prime contractor is no longer king; the technology driver in the economy is the civilian sector; and success measured in terms of profits that can be put back into R&D on next-generation products depends on exports.

That means, particularly in microprocessor based sectors, accepting, if not encouraging expanded exports ultimately promotes our security rather than our vulnerability.

At our Update Conference in San Diego last February, I announced President Clinton's decision to substantially raise the performance levels allowed for HPC exports. Coupled with the six month waiting period mandated by Congress, the Tier 3 military level of 12,500 MTOPS will go into effect on August 14th. We expect the President to make a new announcement shortly, which will be effective in January.

The new announcement, like the previous ones, will no doubt be attacked by those in the Congress and the nonproliferation community who have not yet reconciled themselves to technological reality and wish for the good old days when security could be defined by export denials. Fortunately for you --and for our security --we are winning this debate and are increasingly dealing with ankle biters rather than frontal assaults.

Even so, this battle of philosophies has too often been one of two steps forward, one backward, or occasionally the other way around. I have testified before Congress fifty times during my tenure. Forty-one of these appearances were during the 105th and 106th Congresses alone, and usually involved defending the Administration's policy. Along with that testimony, we provided 320,000 pages of documents to the Congress while the Cox Committee was doing its work, and were subjected to 16 GAO and 9 Inspector General investigations.

Out of all that labor came one significant step backward --the transfer of commercial communications satellite jurisdiction back to the State Department. The jurisdictional change affected our foreign relations, our national security and a broad range of U.S. industry, from small, high tech firms to industrial giants, even for sales to allies. Since the transfer, which this Administration opposed, satellite exports have declined forty percent, from \$1.06 billion in 1998 to \$637 million in 1999 according to Census Bureau export statistics, and the satellite industry has told us that the U.S. share of the world market has dropped from 73% in 1998 to 62% in 1999 and to 52% by the end of the first quarter of 2000. The changed controls on satellites bear much of the responsibility for this, and we can only conclude that a system that works well for arms exports is, even with the best intentions in the world, not appropriate for commercial exports. This is a fundamental point --treating exports of commercial items, like communications satellites, as arms sales does more harm than good to our national security and to the high tech industries upon which our military and intelligence agencies depend.

Ultimately, I am confident we will prevail on this matter as well, although the cost to the satellite industry and its world leadership in this critical sector will be enormous.

PROCESS REFORM

The goal of any government agency, especially those with regulatory responsibilities, is to be responsive and fair. I believe our achievements in liberalizing controls and streamlining the process show that we have done just that.

During the Clinton Administration, we have processed nearly 100,000 license applications for almost \$100 billion in U.S. exports abroad. Although this is a big reduction from the days when the Reagan Administration did that many every year, it has been no easy task. The cases are more complex and the interagency review process rigorous. We believe nonetheless that the President's approach of allowing the relevant agencies to be fully represented in the process is an overall improvement that has produced more effective analyses and better policy development, albeit at some cost in time, which we continue to try to reduce. Roger will report on our results in that regard shortly.

We have also made things better by expanding efforts to assist exporters. Our Exporter Services Division, which is doing a wonderful job of putting on this conference, has completed over 1.2 million phone consultations in the past seven years, an average of 175,000 per year. In addition, they have held nearly 10,000 one-on-one counseling sessions to assist small and large exporters alike.

We have also gone out into the field with over 1,700 conferences with nearly 115,000 business people. These include seminars to answer licensing questions and explain changes in export controls, and training sessions for business executives on enforcement and compliance programs.

Our outreach to industry has not been confined to export controls alone. We have also worked to address the way changes in the world have impacted industry, particularly the defense sector. The Administration, through BXA's DPAS program, helps defense firms diversify their activities into civilian areas by developing and providing detailed economic and statistical information. This helps us develop policies that ensure our industry and technology base are able to support changing security requirements, as well as develop next generation weapon systems.

You will also see on our website, under Defense Programs, that we provide a wide range of international market and competitiveness information of value to both defense and commercial high technology companies. We provide information that firms can use to develop new product lines and market existing products both here and abroad. Much of our work is one-on-one with individual companies, and we have a growing stack of success stories as testimony to our efforts.

We also continue to work with the Newly Independent States to help them develop effective export control programs. We have an extensive effort to focus on export control licensing processes and procedures, preventive enforcement mechanisms, industry-to-government relations and electronic automation of the licensing system. Since 1993, we have delivered 140 bilateral and multilateral workshops in 25 countries.

BXA's enforcement programs play a critical role in protecting our national security and foreign policy interests, particularly as we focus more on specific end-users and end-uses. We have conducted hundreds of investigations over the last four years that have led to the criminal prosecution of persons who illegally exported zirconium for Iraqi munitions, unlicensed equipment for India's missile program, brokerage services for Iraqi rocket fuel, and gas masks to suspected Aum Shinrikyo terrorists in Japan, just to name a few. These investigations also included the first civil charges and penalties for alleged unlicensed exports of controlled biotoxins.

Enforcement is a critical partner for exporters. I cannot stress enough how important it is for companies to "know their customers," and to exercise due diligence in transactions to destinations of proliferation concern. I urge you to work with our enforcement people when you uncover a suspect transaction. Our enforcement organization has developed special programs to help with such "preventive enforcement" activities, which I urge you to take advantage of.

These are just SOME of the services I'm proud to say we provide.

CIAO

One new element of BXA's activities relates to critical infrastructure protection. There is a growing awareness that America's information infrastructure - the basis of e-commerce - has become an attractive target for sabotage and so called cyber attack. One need only look to the recent spread of the Love Bug computer virus which corrupted systems worldwide or the work of

hackers breaking into and disrupting service on a number of popular websites to see that this threat is indeed very real.

BXA's Critical Infrastructure Assurance Office has been coordinating efforts within both the federal government and private sector to protect critical infrastructures. The blueprint for this effort, the National Plan for Information Systems Protection, Version 1.0, was issued last January and stands as the first attempt by any national government to develop ways to protect important computer controlled infrastructures, like energy and water supply systems and communications, transportation, and financial networks, from sabotage or attack.

Another challenge for the CIAO is to encourage voluntary efforts among the broader business community to do the same. The Partnership for Critical Infrastructure Security has been vital to this. Comprised of industry leaders from companies who own and operate most of the nation's critical infrastructures, the Partnership is the centerpiece of the Administration's efforts in this area. The CIAO will continue to play an integral role in coordinating the Partnership's continued efforts to identify vulnerabilities and develop key solutions, but it remains the task of the private sector to see that the means of delivering our nation's important resources are fully protected.

THE FUTURE

I think that's a significant record of accomplishment, but I would not want anyone to think we are simply sitting out the last six months like sand leaking out of a bag. Substantively, more remains to be accomplished. We must finish our improvements to the licensing process and complete our own "electronic revolution." We need to pass an Export Administration Act and find long term solutions to HPC and microprocessor controls, cryptographic technology, and deemed exports. We must also settle the continuing conflict over licensing jurisdiction between the Commerce and State Departments.

This latter issue is particularly important, as we have seen the consequences for the satellite industry of asking State to license items that compete in a commercial environment. We have put ourselves in the paradoxical situation where denial or delay of exports under the rubric of national security has, in the end, done more harm than good to our nation's military and economic strength. Industry figures I cited suggest that the changed controls on satellite exports hurt the U.S. more than they hurt any intended target. While the Department of State has taken action to alleviate some of the problems, the fundamental issue remains that it is not practical or desirable to treat commercial export sales as munitions transfers. The better solution is to recognize dual use items for what they are and control them through the Commerce procedures that are designed for that purpose. In fact, Congressmen Gejdenson and Goodlatte last May introduced legislation in the House to do precisely that.

Recently, the Defense Department has led an effort to reform State's munitions licensing practices. Its motivation has been the Pentagon's desire to prevent the development of "Fortress Europe" by promoting transatlantic defense cooperation through appropriate technology transfer and joint activities. I want to make it clear that the Department of Commerce supports that effort and has been working closely with DOD to facilitate it. Many of DOD's proposals, in fact, parallel

reforms we have already undertaken at BXA. At the same time, we have also been clear that with respect to dual use items, process reform at State misses the point. You cannot successfully "tweak" a system that was designed for a fundamentally different purpose -- licensing munitions -- and our message to Congress has been not to force square pegs into round holes but instead to recognize and respect the differences in the systems.

Here once again we have become mired in a philosophical debate, as those who reject this Administration's new thinking about export controls seek to bring more items under State's control in the expectation that will produce the level of rejections they desire. This is a profoundly dangerous approach which will not only cost the U.S. market share and jobs; it will cost us our technological leadership and will compromise our security.

Thus, the stakes are not small and the challenges not minor. While I expect to make progress on some of the specific matters still pending in the time left, I have no doubt that the larger debate will continue beyond the election, just as it has for the last decade. Those still fighting the Cold War are not going to stop in November, and those who have invested their intellectual energy into trying to turn the clock back have no reason to suddenly set it right.

This Administration has stood firm on these issues, not because it is in your interest, though it is, but because it is in the interest of a stronger America. As I said earlier, we are winning --because we have the facts and the better argument --but you should not for a moment assume that the fight is over or that you can abandon your own efforts for rational export controls. And though Roger, Amanda, and I will continue our work until the last hour of the last day, you must remain ready to carry on the fight that will continue after us.



UNITED STATES DEPARTMENT OF COMMERCE
The Under Secretary for Export Administration
Washington, D.C. 20230

September 9, 1998

The Honorable Tillie Fowler
U.S. House of Representatives
Washington, D.C. 20515

Dear Representative Fowler:

Thank you for so promptly providing me with the information we discussed at the United States Pan Asian American Chamber of Commerce event on July 23, 1998.

The materials you sent to me refer to what has become known as the Garrett Engine case. Garrett, a subsidiary of AlliedSignal, has sold civil certified aircraft engines to China for use on the K-8 military trainer aircraft. Three issues have been raised with respect to these sales: 1) Was production technology transferred? 2) Could the engines be used in cruise missiles? And, 3) Do the engines use a Full Authority Digital Engine Control (FADEC)? Let me address these in turn.

1) Was production technology transferred?

No. Starting in 1990 during the Bush Administration, Garrett received permission, after full interagency review, only to export its TFE-731-2A-2A engine to China for use in the K-8 trainer. No production technology transfer was involved. While it is true that at one time Garrett explored the idea of co-producing the engines in China, the Department of Commerce advised the company that any such transfer of technology would require an export license which would likely not be approved, and, in the wake of that advice, the company did not submit an application.

2) Could the engines be used in cruise missiles?

We believe strongly that the answer to this is 'No.' Due to a host of technical reasons, including size, performance, and configuration, our engineers have consistently determined that the Garrett engines could not be used in cruise missiles. While I admit that some have argued differently, I believe that any impartial analysis will demonstrate that it would be technically infeasible and economically impractical to try to use the Garrett engines in this fashion. If you decide to pursue this question, I would recommend that you discuss it with unbiased aerospace engineers who are intimately familiar with the characteristics of both Garrett's engines and China's cruise missiles.



3) Do the Garrett engines use a FADEC?

The operation and performance of jet engines are controlled by a combination of electronic and mechanical subsystems. In current high performance engines, designers have turned increasingly to digital control technology to obtain the capability to control an ever-increasing number of variables in a fast and reliable manner. There are various types of controllers used in jet engines. The type of controller used is important, not only to the performance of the engine, but because it can decide whether a particular engine requires an export license or not. Prior to September 1991, engines with full authority or hybrid digital electronic controls required a license to China. In September 1991, Commerce published a change in the export controls for gas turbine engines (based on multinational COCOM agreement) that limited the license requirement to engines with a full authority digital engine control (FADEC) only. Full Authority Digital Engine Control (FADEC) is a very sophisticated type of controller, and if the Garrett engine employed one, it would require specific export license approvals to China. If it did not, all agencies agreed, no license would be required.

Commerce concluded in October 1991, during the Bush Administration, that the Garrett engine with a hybrid analog/digital control was not covered by the changed export control, did not include a FADEC, and thus no export license was required for sale of the engine to China. However, other agencies disagreed, and that decision was revoked in November 1991. This disagreement was the result of a lack of specificity in the then-COCOM rules on the parameters that characterized a FADEC. For the next two and a half years this issue was investigated. During that time, agencies agreed to permit Garrett to sell engines to China but only after obtaining specific export licenses. From May 1990 until December 1993, 37 engines were approved for export after full interagency review and concurrence.

Finally, in April 1994, shortly after Mr. Pope's letter was sent to Dr. Wallerstein, the interagency community, including the Department of Defense, agreed that the hybrid analog/digital electronic engine control used on Garrett's TFE-731-2A-2A did not fall within the definition of a FADEC, a determination subsequently confirmed in the issuance of an updated multilateral control list. Accordingly, the engines could be exported to China without an export license.

In short, then, for the past ten years, under both Republican and Democratic Administrations, the interagency community has permitted the export of these engines to China but has denied the transfer of production technology.

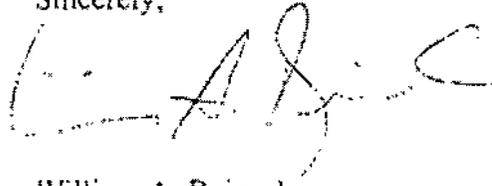
This episode contains a number of useful lessons for those interested in export control issues. First is the important role interagency discussions play in resolving matters such as these. While the initial decisions on the controllability of the engines were made unilaterally by the Commerce Department in the Bush Administration, subsequent decisions were the product of extensive interagency consultations. The latter is obviously the preferred way to do business.

Second, the case illustrates the technical complexities with which licensing officers in all agencies must grapple every day. Questions dealing with performance characteristics and the impact sales will have on the capabilities of importing countries are often difficult to resolve. Answers are not always black and white, and decisions can be easily criticized by those who do not have full access to all the facts. It was partly to ensure that these difficult types of issues are resolved systematically and comprehensively that President Clinton directed that new procedures be adopted in 1995 to maximize interagency review and consultation.

I hope that the above information has been helpful. Usually company specific information relating to export licenses like those of Garrett's are protected from disclosure by Section 12(c) of the Export Administration Act. However, in this case, AlliedSignal has waived its 12(c) protections to permit us to respond to your inquiry concerning its K-8 Trainer Program in China and TFE-731-2A-2A.

If you wish to discuss this further, I would be pleased to do so and can be reached at (202) 482-1455.

Sincerely,

A handwritten signature in black ink, appearing to read 'W. A. Reinsch', written in a cursive style.

William A. Reinsch



Bill

MEETING WITH
NEW DEMOCRAT COALITION

DATE: TUESDAY, JULY 20, 1999
TIME: 4:30 PM
LOCATION: U.S. CAPITOL, ROOM H8
FROM: BILL REINSCH *BR*
Prepared by: Amy Bellanca
x1455

I. OBJECTIVE

The purpose of the meeting is to discuss export control reforms with the members of the New Democrat Coalition (NDC).

II. BACKGROUND

The NDC was co-founded by Representatives Jim Moran, Tim Roemer, and Cal Dooley in the 105th Congress to advance a centrist, pro-growth agenda within the Democratic Caucus. Since it's creation, the NDC has become the largest members organization in Congress, with 63 current members. They have made technology, education, and trade the cornerstones of their New Economy agenda. The NDC meets every Tuesday when the House is in session for a "Topic of the Week" meeting. Past meeting speakers have included Vice President Gore, Secretary Rubin, John Podesta, Erskine Bowles, and a number of other key Administration officials.

Cal Dooley has invited you to discuss export control reform with the members of the NDC. The NDC is interested in working with the Administration to advance "reasonable reforms" of our export control policy.

The members are generally very familiar with the export licensing process, and therefore do not need a crash course in "Licensing 101." One issue of great concern to them is the length of processing time and the reasons behind the current application backlog.

Several NDC members recently traveled to Silicon Valley and are thus particularly interested in computer export control issues. They were pleased with the recent White House announcement easing restrictions on HPCs and semiconductors and are interested in hearing what you think is the long-term fix for this issue, rather than a band-aid approach.



This will be a friendly crowd who will be interested in hearing what they can do to help the Administration.

III. PARTICIPANTS

members of the NDC (see attached)

IV. PRESS PLAN

Closed.

V. SEQUENCE OF EVENTS

I will brief you in your office at 4:00 p.m. We will depart the Department of Commerce at approximately 4:15 p.m. in order to arrive at the Capitol at 4:30 p.m. The meeting is scheduled to last an hour, although ultimately, it is up to you.

Congressman Dooley will introduce you and I to the members, and then likely introduce all of the member present at the meeting. You will then have the opportunity to speak for as long as you like, I'd recommend about 15 minutes, and then you and I will take questions.

VI. LIST OF ATTACHMENTS

- talking points
- paper on HPC controls
- paper on license processing times
- paper on encryption license processing times
- paper on effects of satellite jurisdiction transfer
- NDC membership list

Meeting with New Democrat Coalition Talking Points

- I want to talk about globalization, which has prompted us to rethink our export control policies and then conclude with a word about the mythology of export controls that holds us back from the steps we need to take to be ready for the next century.
- In doing so, I'm going to talk mostly about national security -- which is our primary focus. But it is also true that export control decisions affect the economy. One of the ironies of the current debate is that many of the people attacking us today urged us in 1993 to do exactly what we've done -- largely because of the sorry state of the economy when this Administration took office, particularly in California.
- The foundation of our export control philosophy comes from President Clinton's statement in his speech commemorating the fiftieth anniversary of the GATT last year, "Economic globalization is not a policy option; it is a fact."
- This reality underlies our national security philosophy. Maintaining military superiority means maintaining the gap in capabilities between ourselves and our adversaries. That gap is sustained and expanded through policies that retard our adversaries' progress, such as export controls, and through those that help us run faster -- increased research, development and acquisition of advanced technologies here at home.
- In addition, new information technologies are instruments of our foreign policy. It was the fax, television, radio, and telephones that won the Cold War -- they allowed us to communicate our prosperity to those behind the Iron Curtain. Today, add the Internet to that.
- So, for example, when we decide not to launch a satellite on a Chinese rocket, as we seem to be doing, we are denying the Chinese people television, Internet, and cellular phone service, and thus are postponing their exposure to our ideas and their integration into Western economic and political systems.
- This is a different approach from that of the Cold War, which was based on keeping things out of Soviet hands. Instead, our approach is based on the realization that our national security is a direct function of our economic health and security for two reasons.
- Critical technologies are commonly available and hard to control. Intel, for example, has 50,000 authorized dealers worldwide. 60% of its business is exports. Microprocessors, which are the key ingredient for High Performance Computers (HPCs) as well as PCs, have become a commodity product widely available throughout the world from numerous sources

- This reality led to the President's decision two weeks ago to raise the control levels for high performance computers and to commit to reviewing those levels at regular six month intervals. He is also submitting legislation shortening the six month waiting period for the change in Tier III military end use. Otherwise, the increase to 6500 MTOPS would not take effect until next year.
- Second, our military's transition to Commercial Off the Shelf items (COTS), due to declining defense budgets and the inability of military procurement to keep up with fast-changing sectors, particularly electronics, means that the technology driver in our economy is the civilian sector, not the military contractor. That means, in turn, that our military strength is directly tied to the health of the civilian companies that produce the products the Pentagon buys and invent the technologies it needs.
- A good example is HPCs -- our defense establishment increasingly needs them for weapons design and test simulation, fluid dynamics analysis, small particle analysis, "smart weapons," command, control and communications functions, etc. The 21st century fighting force will be more reliant on computers than any before it, and whoever has an edge in this technology will have an edge on the battlefield.
- At the same time, our military does not buy enough HPCs to keep our companies healthy. In fact, exports keep them thriving. More than 50% of the sales of these companies are exports. Failure to export means fewer profits being rolled into R&D on next generation technologies and fewer funds available to address particular defense-related concerns.
- **Thus, our equation is: exports = healthy high-tech companies = strong defense. Cripple our companies by denying them the right to sell, and you set back our own military development.**
- A key reality is the capacity of our adversaries to make these products themselves or to obtain them from others. In the case of computers, for example, China, as well as India and others, have the capacity to make these machines themselves. While they do not -- and cannot -- manufacture to compete with U.S. companies, they can make machines that will function at performance levels sufficiently high to provide the military capabilities they seek. Denying them U.S. products simply encourages their own development and production -- which was precisely the effect of the Reagan Administration's decision to deny India HPCs.
- Our lead in many of these sectors is not based on our monopoly of the technology; rather it is based on our quality and efficiency of production. Close a market and we will create viable competition where there is very little now. And that competition, as we have learned in so many other sectors over the past thirty years, will not stop with China or India but will move on to compete head to head against us elsewhere to the long term detriment of our ability to retain global leadership.

- In other words, the loser in the face of closed markets is not the Chinese or the Indians but the Pentagon, whose access to cutting edge goods and technologies will be slowed, and the United States, whose technological leadership will face new challenges from new suppliers.

STOP HERE OR KEEP ON GOING -- WHATEVER YOU WANT!

THE MYTHOLOGY OF EXPORT CONTROLS

- These issues have been controversial for years. Many of you watched (or participated in) Democrats beating up Bush for exports to Iraq, and now we're enduring Republican attacks for exports to China. There are plenty of opportunities for finger pointing.
- What is odd about the issue is the extent to which a few stories can seize control of the debate and transform it into a political exercise of laying blame.
- In this Administration we have had McDonnell Douglas machine tools, and satellites and computers, and now a new element which appears to come from misreading the Cox Report.
- Many Members of Congress appear to have read only the summary and to have done so quite quickly. They seem to have concluded that because the Chinese obtained weapons secrets from our national labs, the export licensing system has failed. Whether or not it has failed is something we can debate, but I guarantee that what happened at the labs is not evidence of that failure. Trying to get our critics to identify specific cases, however, has not produced much.
- The McDonnell Douglas case actually explains a good bit about the strengths of our system. Clearly something happened that should not have -- machine tools were diverted to an unapproved location. Contrary to the mythology, these did not constitute an "entire B-1 plant" but were actually about 16% of a closed facility in Ohio. Only about half the tools were sophisticated enough to require an export license (some were up to 25 years old), and of the 30-plus tools in question, only 6 were diverted, and none of them was used before we were able to get them back and restore them to American control.
- From one standpoint, this is a failure. Items ended up in the wrong place. From another, generally forgotten, standpoint, this is a success. We got the items back under American control without them having been used, and the investigation into what happened continues. Our enforcement system worked. **Perhaps most telling, however, was the aftermath for the Chinese. They replaced the most significant diverted item, a large stretch press, with a new one from a European producer. The result of our efforts to get our stretch press back is that the Chinese now have a better one from someone else.**

- On satellites, they involved launches licensed by both State and Commerce, suggesting that the process is not the problem, and they concern events that occurred prior to the transfer of most satellite jurisdiction to Commerce in October 1996. To the extent there were problems, we believe the additional procedures we put in place in late 1996 corrected them, and we believe there have not been problems since then.
- Congress opted last year to transfer jurisdiction back to State, impose additional procedures, and, in general, create a climate hostile to Chinese launches. This is already having a sharp adverse impact on our industry's competitiveness, as industry witnesses testified on June 24th.
- On computers, the Cox Committee report attacks us but presents no actual evidence that computers sold on our watch are being used for proliferation purposes.
- Even if there were, there are real limits on what we can do about it. This is a ubiquitous fast-moving technology, but it is also a technology with military applications. You can use them to design nuclear weapons, though we designed ours originally without them. You can use them for test simulations, which will be increasingly important in a Comprehensive Test Ban Treaty world, although state of the art simulations require computing power far beyond levels that we have decontrolled. You can use them to accelerate a wide variety of industrial processes, though the processes can be run without them. Our military needs them, which certainly suggests that other militaries will want them too.
- To most people, however, they are an essential tool of commerce, communication, and entertainment. Last May, I was struck by two articles that appeared simultaneously in my daily clips. One said, "Chinese hackers raid U.S. computers." The other said, "Internet emerges as news source for the Chinese." And there is the central dilemma of this technology. If we want to spread our ideas and values we must penetrate the communications Maginot Lines that authoritarian regimes erect. At the same time, doing so carries undeniable risks. But that dilemma is a long way from the mythology of evil that some of our friends have so successfully built up around these machines.
- Our solution has been -- and continues to be -- to control the high end of computer capability. Our problem is that what is "high end" changes so rapidly.
- To close my mythology comments on a lighter note, I would mention the time during a Senate hearing when a senator asked Secretary Brown why we had sold the Chinese an aircraft carrier -- an allegation that was news to him. Upon looking into it, we discovered that the senator was referring to a ship built in the early 1940s and decommissioned in 1970. Both the Navy and the Defense Logistics Agency had certified in writing that it was usable only for scrap and that its weapons had been either removed or cut into pieces. As it turned out, it had been inspected by a Member of Congress before it left the United

States, and it was not sold to China, it was sold to India. Aside from that, the senator had his facts straight. But you can be sure there are others in the Congress who believe to this day that the Department of Commerce compromised our security by selling China an aircraft carrier.

-- With that, I think I'll stop and leave it to you on how you want to proceed.

BACKGROUND

High Performance Computers (HPCs) Export Control Talking Points

- On July 1, President Clinton unveiled new export controls on High Performance Computers (HPCs) and semiconductors. This new policy may not end the debate over HPC controls, but it does include changes critical to maintaining the strong, vibrant high-technology industry which is critical to America's national security interests.
- The revised controls announced by the President maintains the four country groups announced in 1995, but amends the countries in, and controls levels for, those groups as follows:
- **First**, the President's decision moved Brazil, the Czech Republic, Hungary, and Poland from Tier II to Tier I country group allowing a license exception for all computers.
- **Second**, the control level for Tier II countries was raised from 10,000 to 20,000 MTOPS with the expectation that it will be raised again in six months to the 32,000-36,000 MTOPS range.
- **Third**, the two-level system for civilian and military/proliferation end-users was maintained in Tier III countries; however, individual license levels for civilian end-users will be immediately raised from 7,000 to 12,300 MTOPS.
- **Finally**, as you may already know, prior NDAA notice of exports for systems above 2,000 MTOPS is currently required to all Tier III end-users. This announcement, after Congressional approval, raises the NDAA notification level to 6,500 MTOPS. After this approval, 6,500 MTOPS will become the individual license level for military/proliferation end-users.
- In addition to revising computer export controls, the control level for general purpose **microprocessors has been raised from the 1,200 MTOPS to 1,900 MTOPS**. On July 8, the regulation implementing this change was published.
- BXA anticipates that an interim rule implementing President Clinton's HPC announcement will be published shortly.
- This is an evolutionary process. Our policy must continue to adapt to changes. The president has directed us to send him new recommendations for these export controls every six months. We believe this commitment is as important as the changes we have just made.

BACKGROUND

Overall License Processing Times Talking Points

- By the end of this fiscal year, we will likely surpass 12,000 license applications, which will represent the largest number of applications received since FY 1994. Last year, in FY 1998, we received 10,693 applications. By the end of the third quarter of this fiscal year, we had already received 9,570 applications, coming close to our FY 1998 total.
- In FY 1998, we processed 11,016 applications with an average processing time of 33 days (15 days for non-referred cases and 36 days for referred cases). By the end of the third quarter of FY 99, we had completed 9,084 applications with an average processing time of 39 days (20 days for non-referred applications and 42 days for referred). This increase in processing time can be attributed to the increase in license applications and a strain on resources by shifts in workload priorities, i.e., NDAA and Congressional/IG requests.
- In the first three quarters of FY 1999, 86 percent of all cases required referral (a one percent increase over FY 1998). Percentage of applications reviewed by each agency in FY99: Defense Dept. (94 percent); State Dept. (86 percent); Energy Dept. (14 percent), and Justice Dept. (14 percent). The average processing time for all agencies is well below their allotted 30 day review period: Defense (14 days); State (13 days); Energy (23 days); and Justice (14 days).
- Total dollar value of all approved licenses in FY 1998 was \$13.5 billion. In the first three quarters of FY 1999, it was \$24.9 billion. The transfer of satellites back to State Dept. jurisdiction will result in a large decrease in total dollar value of approved licenses (over \$7 billion were approved under this Export Control Classification Number (ECCN) during the first portion of FY 1999).

BACKGROUND

Encryption License Processing Times Talking Points

- The small decrease in approved applications for information security systems/equipment, software and technology is primarily due to the liberalization of encryption products (128 bit or higher) for banks, financial institutions, health facilities and on-line merchants.
- By the end of the third quarter of FY 1999, we had approved 412 applications for information security systems/equipment, compared to a 1998 fiscal year total of 639. The FY 1998 total for information security software was 794; during the first three quarters of FY 1999, we have already approved 718 licenses, suggesting that we may approach 1,000 by the end of the fiscal year.
- In FY 1998, the average processing time for encryption hardware was 34 days (11 days for non-referred, 35 days for referred cases); in the first three quarters of FY 1999, the average processing time rose to 38 days (11 days for non-referred, 41 days for referred).
- In FY 1998, the average processing time for encryption software was 38 days (9 days for non-referred applications, 40 days for referred); in the first three quarters of FY 1999, the average processing time was 39 days (9 days for non-referred, 43 days for referred.)
- In FY 1998, the average processing time for encryption technology was 35 days (8 days for non-referred, and 36 days for referred); in the first three quarters of FY 1999, the average processing time increased to 38 days (7 days for non-referred and 39 days for referred.)
- Dollar Value of Approved Licenses:

	<u>FY 1998</u>	<u>FY 1999 (3 Qtrs.)</u>
Hardware:	\$ 1.250 billion	\$ 813 million
Software:	\$ 731 million	\$ 802 million
Technology:	\$ 73 million	\$ 41 million

BACKGROUND

Satellites and Satellite Parts & Components: The Impact of the Transfer of Licensing Jurisdiction on U.S. Industry

Satellites

The Commerce and State Departments control exports under different legal and regulatory frameworks. The State Department's rules are for arms exports and require separate licenses for all phases of the transaction, including sales discussions. In a recent GAO report, it was noted that for a single satellite launch/sale, there may be a requirement for as many as 10 separate licenses under the State Department system. Under Commerce Department jurisdiction, however, that same satellite launch/sale would normally be authorized under a single license, and sales data could be provided under a license exception.

There are also differences in how the two agencies process license applications. Licensing at the Commerce Department changed dramatically in December 1995, when the President issued Executive Order 12981. This Executive Order made two fundamental changes in how Commerce issues a license. First, it gave other agencies the right to review any Commerce license application they wished to see. Second, it defined an escalation process to move disputed licenses from the working level to more senior levels for review and decision. These procedures have worked well for Commerce, but they do not apply to State Department licenses. During the time that Commerce had licensing jurisdiction for satellites, all cases were reviewed by the Defense and State Departments, and most were reviewed by the CIA. Again, as noted in the recent GAO report, the average processing time for satellite cases under Commerce was 142 days while those previously processed by State was 242 days.

From Congressional testimony by Defense and State Department officials since satellite jurisdiction has been transferred back to the State Department, it is expected that satellite license processing time will exceed 180 days. This is likely to continue until the State Department is able to hire and train new licensing officers, a process that itself is projected to take about 18 months.

In testimony given in a Senate hearing on June 24, 1999, Lockheed Martin and Merrill Lynch representatives noted that the transfer of licensing from Commerce to State has had a very negative impact on the industry. Lockheed Martin has been told by long-time Asian and European customers that they will look to other sources for satellites due to the lack of transparency and timely responsiveness of the State Department licensing system. The Merrill Lynch representative testified that, based on a similar impression in the venture capital market, U.S. satellite manufacturers are now seen to have a negative risk vs reward relationship.

Satellite Parts and Components

At the time of the transfer of communications satellites from Commerce to State, certain "related equipment" was also returned to State jurisdiction. While the term "related equipment" was defined in our regulations as items such as fuels or explosive bolts that are used in the launch of satellites, other "space qualified" items also used in the manufacture and launch of satellites, i.e., dual use items that have been certified for use in space applications, were not specifically addressed. This has caused uncertainty on the part of exporters as to the jurisdiction for their products. Recently the Defense Department has challenged the jurisdiction on a number of Commerce license applications for such items, and in those cases in dispute, the commodity jurisdiction has almost always been assigned to the State Department. This continues to be an issue of debate within the interagency community.

NEW DEMOCRAT COALITION

[BACK TO HOME PAGE](#)

Membership List

[Cal Dooley \(CA\)](#) | [Jim Moran \(VA\)](#) | [Tim Roemer \(IN\)](#)

Tom Allen (ME)	Jim Maloney (CT)
Brian Baird (WA)	Bob Matsui (CA)
James Barcia (MI)	Carolyn McCarthy (NY)
Ken Bentsen (TX)	Karen McCarthy (MO)
Shelley Berkley (NV)	Mike McIntyre (TX)
Marion Berry (AR)	David Minge (MN)
Earl Blumenauer (OR)	Dennis Moore (KS)
Lois Capps (CA)	Grace Napolitano (CA)
Bob Clement (TN)	David Phelps (NC)
Bud Cramer (AL)	David Price (NC)
Jim Davis (FL)	Silvestre Reyes (TX)
Peter Deutsch (FL)	Steve Rothman (NJ)
Anna Eshoo (CA)	Loretta Sanchez (CA)
Bob Etheridge (NC)	Max Sandlin (TX)
Harold Ford, Jr. (TN)	Brad Sherman (CA)
Charlie Gonzalez (TX)	Ronnie Shows (MS)
Baron Hill (IN)	Adam Smith (WA)
Ruben Hinojosa (TX)	Vic Snyder (AR)
Joseph Hoeffel (PA)	John Spratt (SC)
Rush Holt (NJ)	Debbie Stabenow (MI)
Darlene Hooley (OR)	Charlie Stenholm (TX)
Jay Inslee (WA)	Bart Stupak (MI)
Chris John (LA)	John Tanner (TN)
Ron Kind (WI)	Ellen Tauscher (CA)
John LaFalce (NY)	Mike Thompson (CA)
Nick Lampson (TX)	Jim Turner (TX)
John Larson (CT)	Tom Udall (NM)
Ken Lucas (KY)	Bob Weygand (RI)
Bill Luther (MN)	Robert Wexler (FL)
Carolyn Maloney (NY)	David Wu (OR)

[NDC HOME PAGE](#) | [PRESS COVERAGE](#)

CRS Report for Congress

Received through the CRS Web

Technology Transfer to China: An Overview of the Cox Committee Investigation Regarding Satellites, Computers, and DOE Laboratory Management

June 11, 1999

Marcia S. Smith, Glenn J. McLoughlin, and William C.
Boesman
Resources, Science, and Industry Division

ABSTRACT

This report provides an overview of the findings and recommendations of the House Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China as they relate to satellite launches, high performance computers, and management of Department of Energy (DOE) laboratories. The Select Committee, often called the "Cox Committee" after its chairman, Representative Christopher Cox, released an approximately 900-page, three-volume unclassified version of its report on May 25, 1999. This CRS report also provides background information on the satellite, computer, and DOE laboratory management issues to set the Cox committee findings and recommendations in context. This report will not be updated. CRS Issue Brief IB93062, *Space Launch Vehicles: Government Requirements and Commercial Competition*, and CRS Issue Brief IB10036, *Restructuring DOE and Its Laboratories: Issues in the 106th Congress* contain updated information on legislative activities resulting from the Cox committee recommendations on satellites and DOE laboratory management, respectively. CRS Report RL30220, *China's Technology Acquisitions: Cox Committee's Report—Findings, Issues, and Recommendations*, provides an overview of the entire Cox committee report.

Technology Transfer to China: An Overview of the Cox Committee Investigation Regarding Satellites, Computers, and DOE Laboratory Management

Summary

In 1998, the House of Representatives created the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China (PRC). Chaired by Representative Christopher Cox, the "Cox committee" was created partially in response to allegations that two satellite manufacturing companies—Loral and Hughes—might have transferred technology to China in the course of launching satellites on Chinese launch vehicles. The committee's mandate was broader, however, and it investigated other instances in which technology transfer might have occurred, particularly in high performance computers and nuclear weapons information from laboratories managed by the Department of Energy (DOE). The five Republicans and four Democrats on the committee unanimously adopted a multi-hundred page, classified report on December 30, 1998 and transmitted it to the President on January 3, 1999. Public release of the report was delayed until May 25, 1999 pending preparation of a declassified version (the committee's final report itself remains classified).

On the satellite issue, the Cox committee found that Loral and Hughes deliberately provided information to China that helped improve the reliability, though not the range or accuracy, of Chinese missiles. The companies are under a Justice Department investigation regarding alleged export violations. Loral concedes that it provided a report to Chinese officials without U.S. government approval, but both companies deny violating export regulations.

Regarding high performance computers (HPCs), the committee determined that U.S. HPC export policy has been circumvented by PRC end users, not properly monitored or enforced by U.S. officials, and that U.S. industry generally has been unaware of PRC applications of HPCs.

As for DOE management of its laboratories, the Cox committee found that security at DOE's nuclear weapons laboratories does not meet even minimal standards and the PRC has stolen design information on the United States' most advanced thermonuclear weapons.

The Cox committee issued 38 recommendations. In its response to the committee's report, the White House stated that it already was implementing most of those recommendations and that while it does not agree with all of the committee's analysis, it shares the objective of "strengthening export controls and counterintelligence, while encouraging legitimate commerce for peaceful purposes."

Congress passed legislation in the 105th Congress in response to the satellite export issues investigated by the Cox committee and is expected to pass further legislation in the 106th Congress to implement some of the Cox committee recommendations.

Contents

Introduction	1
Launches of U.S.-Built Satellites by the PRC	2
Background	2
Cox Committee Findings	3
Cox Committee Recommendations	4
White House and Congressional Responses	6
High Performance Computers (Supercomputers)	8
Background	8
Cox Committee Findings	9
Cox Committee Recommendations	10
White House and Congressional Responses	11
Management of Department of Energy Laboratories	12
Background	12
Cox Committee Findings	13
Cox Committee Recommendations	15
White House and Congressional Responses	16

Technology Transfer to China: An Overview of the Cox Committee Investigation Regarding Satellites, Computers, and DOE Laboratory Management

Introduction

The House of Representatives created the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China (PRC) on June 18, 1998. Chaired by Representative Christopher Cox, creation of the "Cox committee" was spurred partially by allegations that two U.S. satellite manufacturing companies, Loral and Hughes, had improperly transferred technical information to China in the course of launching satellites on Chinese launch vehicles. The committee's charter also included investigation of other instances of possible improper transfer of technology, information, advice, goods, or services to the PRC.¹

The committee was composed of nine Members: Republicans Cox, Porter Goss, Doug Bereuter, James Hansen, and Curt Weldon, and Democrats Norman Dicks, John Spratt, Lucille Roybal-Allard, and Robert Scott. The Members unanimously adopted a multi-hundred page report on December 30, 1998, which was presented to the President on January 3, 1999. Originally, the committee's existence would have expired at the end of the 105th Congress, but the House extended the committee's term into the 106th Congress to allow time for a declassified version of the report to be prepared (the committee's final report itself remains classified). The three volume public version,² approximately 900 pages long, was released on May 25, 1999 and is available at the House of Representatives Web site [www.house.gov].

Although transfer of satellite and launch vehicle technology had been the major public focus at the time the committee's work began, attention later shifted to findings concerning the leakage of information regarding nuclear bomb design allegedly from Los Alamos National Laboratory, one of the three U.S. nuclear weapons laboratories managed by the Department of Energy (DOE). The committee also investigated the transfer of high performance computer technology and other technologies. The

¹ The committee was created pursuant to H. Res. 463, which specifies its charter (see pages H4748-52 of the June 18, 1998, Congressional Record).

² U.S. Congress. House. Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China. *U.S. National Security and Military/Commercial Concerns with the People's Republic of China*. 106th Congress, 1st session. Washington, U.S. Govt. Print. Off., 1999. 3 v., various pagings.

committee made 38 recommendations covering a spectrum of issues involving U.S.-PRC relations. This report provides an overview of the Cox committee findings and recommendations concerning satellite exports, high performance computers, and management of DOE laboratories. References to the appropriate volume and page number of the Cox committee report are shown in parentheses (such as "v. 1, p. 16" for volume I, page 16).

Launches of U.S.-Built Satellites by the PRC

Background ³

In 1988, the Reagan Administration granted permission to export three U.S.-made satellites to China for launch once China met three requirements: signing three international treaties regarding use of space; signing a bilateral trade agreement so China would not undercut Western prices for launching satellites; and signing a Technology Safeguard Agreement to ensure that no technology would be transferred during the time that American-made satellites were in China awaiting launch. China met those conditions and export of the three satellites, all manufactured by the U.S. company Hughes, was approved by the State Department and by the now-defunct COCOM (Coordinating Committee for Multilateral Export Controls).

China's decision to offer launches on a commercial basis came shortly after the U.S. space shuttle *Challenger* tragedy in 1986. At that time, commercial launches were offered only by Europe's Arianespace and the National Aeronautics and Space Administration (NASA) in the United States. The Reagan Administration and Congress had taken actions to facilitate the emergence of U.S. private sector competitors to NASA for launching satellites beginning in 1983, but private companies argued that they could not compete with government-subsidized prices for launching on the shuttle. The loss of *Challenger* and a subsequent policy decision that commercial satellites would not be launched on the shuttle except in unique circumstances opened opportunities for companies in the United States and elsewhere, including China, to compete in the launch services business.

The Reagan Administration decision to allow exports of satellites to China met mixed reactions because it could harm U.S. launch services companies just entering the market, but help U.S. satellite manufacturers by increasing competition in launching satellites into orbit. Concern about potential technology transfer during the time the satellite was in China awaiting launch was also a significant issue at that time, hence the requirement for a Technology Safeguard Agreement. Such an agreement was signed by the two countries in 1989 (revised version was signed in 1993).

The first commercial Chinese launch of a U.S.-built satellite occurred in 1990. By May 31, 1999, 20 commercial Chinese launches of U.S.-built satellites had been accomplished, of which 16 were successes, three were complete failures, and one was

³ For further background information, see: Congressional Research Service, *Space Launch Vehicles: Government Requirements and Commercial Competition*, by Marcia S. Smith, CRS Issue Brief IB93062, updated regularly.

a partial failure, placing the satellite into the wrong orbit.⁴ A total of 26 U.S.-built satellites were launched (some launch vehicles carried two satellites into orbit at one time).

The Cox committee focused its examination on whether technology transfer occurred from Hughes or Loral to China during the investigations of the three launch failures, but also looked more generally at whether U.S. satellites are adequately secured while in China and whether information provided to insurance companies that insure the launches is subjected to adequate export control scrutiny.

The first two failures, on December 21, 1992 and January 25, 1995, involved satellites built by Hughes Space and Communications (hereafter "Hughes"), part of Hughes Electronics, a subsidiary of General Motors. The satellites were Optus 2 (owned by Australia) and APStar-2 (owned by Asia Pacific Telecommunications Satellite Co., Ltd., which is 75% owned by Chinese government-backed companies), respectively. The third failure, on February 14, 1996, was of the Intelsat 708 satellite built for the International Telecommunications Satellite Organization (Intelsat) by Space Systems/Loral (hereafter "Loral"), part of Loral Space & Communications.

Attention to the activities of satellite manufacturers following satellite launch failures in the PRC was sparked by Loral's actions following the 1996 failure. To ameliorate concerns of satellite insurance companies, the PRC asked Loral to convene a committee to review the PRC's analysis of the Intelsat 708 failure. Loral complied, establishing a committee that included representatives of Hughes, since Hughes had been involved in two failure investigations already. Loral concedes that in violation of its own internal policies, a copy of the committee's report was transmitted to Chinese officials without obtaining U.S. government approval. The Justice Department began investigating Loral in 1997 to determine if it had violated export regulations in the course of its review of the PRC's Intelsat 708 failure analysis. In February 1998, the Clinton Administration approved the export of another Loral satellite to China even though the Justice Department investigation was ongoing, raising additional congressional concerns. Further allegations subsequently surfaced that Hughes may have violated export guidelines during investigations of the 1992 and 1995 failures, as well as in conjunction with the 1996 failure. The Justice Department reportedly also is now investigating Hughes. Both companies deny violating export regulations.

Cox Committee Findings

According to the Cox committee, Hughes and Loral transferred information to the PRC in violation of export guidelines during the course of the failure investigations in 1992, 1995, and 1996. The committee found that following the failures, "U.S. satellite manufacturers transferred missile design information and know-how to the PRC without obtaining the legally required licenses. This information has improved the reliability of PRC rockets useful for civilian and military

⁴ For further information on China's space program, see: Congressional Research Service, *China's Space Program: A Brief Overview Including Commercial Launches of U.S.-Built Satellites*, by Marcia S. Smith, CRS Report 98-575 STM, September 3, 1998.

purposes. The illegally transmitted information is useful for the design and improved reliability of future PRC ballistic missiles, as well" (v. I, p. xiv). In the 1992 and 1995 failures, which involved only Hughes, the committee concluded that Hughes "showed the PRC how to improve the design and reliability of PRC rockets. Hughes' advice may also be useful for design and improved reliability of future PRC ballistic missiles. Hughes deliberately acted without seeking to obtain the legally required licenses" (v. I, p. xvii). The report adds that there are differing views within the government as to how much the information might assist PRC missile development, but "There is agreement that any such improvement would pertain to reliability and not to range or accuracy" (v. II, p. 4). In the case of the 1996 failure review, which involved both companies, the committee concluded that "Loral and Hughes showed the PRC how to improve the design and reliability of the guidance system used in the PRC's newest Long March rocket. Loral's and Hughes' advice may also be useful for design and improved reliability of elements of future PRC ballistic missiles. Loral and Hughes acted without the legally required license, although both corporations knew that a license was required" (v. I, p. xix).

While in the PRC awaiting launch, U.S. satellite manufacturers are supposed to provide 24-hour physical security for the satellite to prevent the PRC from obtaining technical information. The Cox committee found "numerous" instances in which the satellite manufacturers or the security personnel they hired performed inadequately. "In light of the PRC's aggressive espionage campaign against U.S. technology it would be surprising if the PRC has not exploited security lapses that have occurred in connection with launch of U.S. satellites in the PRC" (v. I, p. xxi). DOD provides personnel to monitor compliance with export regulations during the course of launches of U.S. satellites on PRC launch vehicles, and the committee also found problems with the manner in which DOD executes that role.

The committee furthermore examined whether export guidelines are adequately followed in connection with providing technical information to insurance brokers and underwriters that insure satellites and satellite launches. The committee concluded that "... U.S. export control authorities may not be adequately enforcing these [export control] laws in the space insurance industry context, nor paying sufficient attention to these practices" (v. I, p. xxiii).

After reviewing the satellite launch business, the committee also concluded that by launching Western satellites, the PRC obtained launch experience that improved its position as a long-term competitor to U.S. companies and thus "It is in the national security interest of the United States to increase U.S. domestic launch capacity" (v. I, p. xxiv).

Cox Committee Recommendations

The committee made the following 10 recommendations regarding satellite exports (v. III, p. 170-172):

- Satellite export control provisions in the FY1999 Strom Thurmond National Defense Authorization Act should be implemented aggressively.
- The State Department should have sole satellite licensing authority.

- The executive branch and Congress should ensure that the State Department has adequate personnel and resources devoted to processing export license applications so export licenses can be acted upon in a timely fashion.
- The appropriate congressional committees should report necessary legislation to ensure that satellite manufacturers are not disadvantaged in collateral areas such as tax credits because of the transfer to the State Department of the responsibility to license satellite exports.
- High priority should be given by the Department of Defense (DOD) to recruiting, training, and maintaining a staff dedicated to monitoring launches in foreign countries of U.S. satellites and establishing and monitoring technology control plans to prevent any transfer of information that could be used by the PRC to improve its missile capabilities
- DOD, rather than satellite manufacturers, should contract for security personnel required at the launch site; the number of security personnel should be sufficient to maintain 24-hour security; and the satellite export licensee should be required to reimburse DOD for all associated costs of such security.
- DOD should ensure sufficient training for its personnel who monitor space launches from initial discussions through launch, and, if necessary, failure analysis (called the "launch campaign") and assign adequate numbers of monitors; ensure continuity of service by monitors for the entire space launch campaign period from marketing to launch and, if necessary, launch failure analysis; and adopt measures to make service as a monitor an attractive career opportunity.
- DOD monitors should maintain logs of all information authorized or transmitted to the PRC and that information shall be transmitted on a current basis to the Departments of Defense, State, and Commerce, and to the CIA; documents should be retained for the period of the statute of limitations for violations of the International Traffic in Arms Regulations (ITAR); and DOD should adopt clear written guidelines providing monitors the responsibility and the ability to report serious security violations, problems, and issues at the overseas launch site directly to the headquarters office of the responsible DOD agency.
- Relevant executive branch departments and agencies should ensure that the laws and regulations establishing and implementing export controls are applied in full to communications among satellite manufacturers, purchasers, and the insurance industry, including communications after launch failures.
- Appropriate congressional committees should report legislation to encourage and stimulate further the expansion of U.S. launch capacity.

White House and Congressional Responses

In its May 25, 1999 press release responding to the Cox committee report,⁵ the White House stated that the Administration "agrees with and is carrying out all of the Committee's recommendations concerning satellite launches." The press release stated:

- The Administration has implemented the provisions of the FY1999 Strom Thurmond National Defense Authorization Act.
- The State Department has taken steps to ensure that U.S. companies understand and comply with the requirements of law and regulation for data that may be provided to space insurance companies.
- DOD is implementing several measures to strengthen monitoring of foreign launches, including establishment of a new Space Launch Monitoring Division within the Technology Security Directorate of the Defense Threat Reduction Agency and hiring 39 additional staff for this function who will receive enhanced training and provide end-to-end monitoring of controlled space launch and satellite technologies.
- DOD is examining the recommendation that it be responsible for hiring security personnel to provide physical security for satellites at foreign launch sites.
- The Administration is encouraging development of the U.S. domestic launch industry through DOD's Evolved Expendable Launch Vehicle program, NASA's Reusable Launch Vehicle program, and Administration efforts to assure range modernization at U.S. launch sites.⁶

Prior to the conclusion of the Cox committee investigation, Congress took action to transfer responsibility for export decisions for commercial communications satellites back to the State Department from the Commerce Department. The State Department had responsibility for exports of commercial communications satellites until 1993. The Clinton Administration transferred that authority to the Commerce Department in two steps (1993 and 1996). The FY1999 Strom Thurmond National Defense Authorization Act (P.L. 105-261) returned export control responsibility to the State Department effective March 15, 1999. It also expanded the requirements set forth in the FY1990-91 Foreign Relations Authorization Act (P.L. 101-246, Section 902) that prohibit the export of U.S.-built satellites to China unless the President grants a waiver and reports to Congress that (1) China has achieved certain political and human rights reforms, or (2) it is in the national interest of the United

⁵ The White House, *Response to the Report of the Select Committee on U.S. National Security and Military/Commercial Concerns With the People's Republic of China*, May 25, 1999.

⁶ For further information on these programs, see CRS Issue Brief IB93062.

States.⁷ Under the new language in the FY1999 National Defense Authorization Act, the President also must provide a detailed justification for granting such a waiver, including information such as a description of all militarily sensitive characteristics integrated within or associated with the satellite and the impact on U.S. jobs of permitting the export. A number of other provisions were included in P.L. 105-261, such as specifying that investigations of launch failures are covered by export guidelines and require a license.

Following release of the Cox committee report, Congress has taken further action⁸ both in response to the report and to concerns expressed by the U.S. aerospace industry. For example, aerospace companies have complained that State Department implementation of the new satellite export regulations is affecting exports for launches on non-PRC launch vehicles, such as Europe's Ariane, and that the State Department has insufficient personnel to carry out its responsibilities under that Act.

During deliberations on the FY2000 National Defense Authorization bill (S. 1059) on May 26 and 27, 1999, the Senate adopted an amendment by Senator Lott that requires the President to notify Congress promptly whenever an investigation is undertaken of an alleged violation of export laws in connection with a commercial U.S.-built satellite and whenever an export is approved for a U.S. person or firm that is the subject of such an investigation. This provision responds to concerns that the Clinton Administration approved the export of a Loral-built satellite even though Loral was already under investigation by the Justice Department. The Lott amendment includes language regarding the Defense Threat Reduction Agency (DTRA, part of DOD) monitors who are assigned to assure compliance with export regulations by U.S. companies during each launch campaign. The amendment directs the Secretary of Defense to establish regulations that allocate funds to assure the necessary number of DTRA launch campaign monitors, establish appropriate professional and technical qualifications and training for them, grant them authority to suspend launches for purposes of U.S. national security, increase their reporting requirements and the systematic archiving and preservation of those reports, and require exporters to reimburse DOD for expenses incurred in monitoring launch campaigns. The Lott amendment furthermore requires DOD to establish a counterintelligence program within DTRA as part of its satellite launch monitoring program, requires the State Department to provide timely notice to exporters of the status of their license requests, requires the State and Defense Departments to consult with the Director of Central Intelligence on commercial communications satellite export decisions, and requires those agencies to submit annual reports to Congress on implementation of satellite technology safeguards.

On June 9, 1999, the House adopted amendments to its version of the FY2000 DOD authorization bill (H.R. 1401) as well. A Cox amendment, *inter alia*, requires reports on implementation of the satellite export control authority and satellite export

⁷ For a list of waivers granted under P.L. 101-246, see Congressional Research Service, *China: Possible Missile Technology Transfer from U.S. Satellite Export Policy—Background and Chronology*, by Shirley Kan, CRS Report 98-485, May 10, 1999.

⁸ For updated information on congressional action, see CRS Issue Brief IB93062.

licensing authority, requires a technology transfer control plan for satellite export licenses, specifies that DOD space launch monitors provide 24-hour, 7-day per week coverage, and establishes a DOD Office of Technology Security. Amendments by Representative Curt Weldon establish a Technology Security Division within DTRA as a separate DOD agency and require DOD to provide an annual report to Congress assessing the cumulative impact of individual export licenses by the United States to countries of concern. An amendment by Representative Gilman requires the Secretary of State to ensure that adequate resources are allowed for the Office of Defense Trade Controls for reviewing and processing export licenses in a thorough and timely manner and to obligate \$2 million for additional staff for that office which had been identified by Congress last fall in the report accompanying the FY1999 Omnibus Appropriations Act (P.L. 105-277).

The Gilman amendment is similar to a provision in the FY2000 Foreign Relations Authorization bill (HR. 1211) as reported (H.Rept. 106-122) from the House International Relations Committee which Representative Gilman chairs. H.R. 1211 also directs the Secretary of State to establish an export regime that includes preferential treatment and expedited approval for exports to NATO allies, major non-NATO allies and other friendly countries.

High Performance Computers (Supercomputers)

Background

High performance computers (HPCs) are computers that can perform multiple, complex digital operations within seconds. Sometimes also called supercomputers, HPCs are actually a wide range of technologies that also include bundled workstations, mainframe computers, advanced microprocessors, and software.⁹ The benchmark used for gauging HPC computing performance is to count the millions of theoretical operations per second, or Mtops, that the computer can perform. The actual Mtops performed by an HPC over a period of time can vary, based on which operations are performed (some can take longer than others or can be performed while other operations are taking place) and the real cycle speed of the computer.¹⁰

HPC technology has removed many of the technical constraints in advanced computing by reducing long computing times and complex computing functions that hindered solving mathematical, scientific, and engineering problems. Recent HPC applications range from accurate real-time weather forecasting and climate change modeling to simulations of nuclear weapons tests. Global market leaders are IBM and Sun Microsystems/Cray, followed by Japan's NEC (v. 1, p. 144). The PRC has a limited ability to produce HPCs, and U.S. firms dominate the PRC HPC market (v.

⁹ A supercomputer is usually defined as a single, complex, mainframe computer that can undertake a series of specific computer functions. Michael S. Malone, ed., "Big Iron: Supercomputers Are Back and Changing Business, Science, and Even You," *Forbes* ASAP, February 22, 1999. 96 pages.

¹⁰ See: [<http://www.whatis.com/mtops.htm>].

I, p. 144-145). Generally, most U.S. high technology industry leaders have sought to increase, not limit, HPC exports.¹¹

U.S. policy has recognized the importance of this technology by adjusting export control policy to reflect advances in HPC technologies. In 1992, the U.S. Commerce Department defined an HPC as 195 Mtops; any export above this level required an export license (v. I, p. 118). This definition was revised in 1994 (1,500 Mtops), reflecting new HPC technologies and expanding applications (v. I, p. 119). In 1996, the Department of Commerce once more revised its HPC definition, setting its benchmark for export licenses at 2,000 Mtops. The agency also forecast that 7,000 Mtop computers would likely become available in global markets by the end of 1997 (v. I, p. 121).

Also in 1996, the Department of Commerce created four Computer Country Groups for export controls of computers. These four categories — or “tiers” — of countries have different HPC export criteria. The PRC is a Tier 3 country, characterized as a security risk because of proliferation, diversion, or other security issues (v. I, p. 127-128). To sell to a PRC customer, an exporter must obtain a license from the Department of Commerce when exporting computers above 2,000 Mtops to the Chinese military or to a nuclear proliferation end user (or use); and an export license for any computer above 7,000 Mtops for all other Chinese end users (or use). Any export of a computer below 2,000 Mtops to a Tier 3 country does not require a license; any export of a computer below 7,000 Mtops to a non-military and non-proliferation end user does not require a license. U.S. exporters must maintain records of exports of computers from 2,000 Mtops to 7,000 Mtops to the PRC (v. I, p. 127-128).

Cox Committee Findings

The Cox Committee has determined that U.S. HPC export policy has been circumvented by PRC end users, not properly monitored or enforced by U.S. officials, and that U.S. industry generally has been unaware of PRC applications of HPCs. The major Cox Committee report findings on HPCs are summarized below.

- First, the Cox Committee estimates that since 1996, the PRC may have received a total of 603 HPCs from the United States. According to the Committee, this number has grown rapidly since 1996, when HPC export controls were greatly relaxed. It also encompasses a wide range of computing capacity, from lower-end 1,500-2,000, to 10,000 Mtops and above (v. I, p. 144-145). This wide range of computing has provided PRC end-users with different combinations of computing power and speed, and is linked to the second finding.
- Second, the Cox Committee has determined that PRC end users are clustering lower-end HPCs together to increase computing power and speed. Such actions could allow an end user to obtain several 500 Mtop HPCs — without needing an export license — and combine these into a single HPC with 2,000

¹¹ Richard E. Cohen, *Hot Trade Winds*, The National Journal, 29 May 1999, P. 1471-1472.

Mtops processing capability. Similarly, several 2,000 Mtop machines could be linked together and provide high-end HPC functions to any PRC user. In both instances, U.S. export control policy would be circumvented, as PRC end users obtain needed HPCs without the proper export licenses (v. I, p. 134; 157-158).

- Third, the Cox Committee expressed concern regarding the blurred distinction between PRC private companies and state-owned enterprises (SOEs). This has resulted in high-end U.S. HPCs destined for civilian use finding their way to military and proliferation end users (or use), without a license. Since the mid-1990s, China has embarked on a long-term plan to privatize many SOEs.¹² However, domestic technology transfer between civilian and military end users has occurred in the past and is documented (v. I, p. 137; 138). The Cox Committee also contends that PRC students visiting federal laboratories and universities with HPC technologies may act on behalf of the Chinese intelligence organizations (v. I, p. 141-142), further blurring civilian, military, and academic lines among PRC users.
- Fourth, until June 1998, the U.S. government's ability to verify the location and use of HPCs in the PRC was blocked by that country's resistance to post-shipment, on-site verification visits. According to the Cox Committee report, the U.S. government has conducted only one post-shipment HPC verification in the PRC. A 1998 agreement affords the United States the right to request access to some HPCs, but includes substantial limitations on such requests and visits. Moreover, the post-shipment visits that are allowed can verify the location of an HPC, but not how it is used (v. I, p. 134-137).

According to the Cox Committee report, these findings raise significant security implications for the United States. A major implication addressed by the Cox Committee is the use of HPCs by the Chinese military to advance its nuclear weapons testing capability. If China complies with the Comprehensive Test Ban Treaty, "its need for HPCs to design, weaponize, deploy, and maintain nuclear weapons will be greater than that of any other nation possessing nuclear weapons, according to the Department of Energy" (v. I, p. xxix-xxx). HPC modeling and simulations could also be used by the PRC in its biological and chemical weapons programs, to advance methods of cryptology (the design and breaking of coded communications), and for other forms of information warfare (v. I, p. 112-117).

Cox Committee Recommendations

The Cox Committee report provided four policy recommendations.

- Legislation to require testing of HPCs and technology which may be potentially used for clustering and other combinations of computers. This would be undertaken by the Department of Energy, in consultation with the

¹² See: Congressional Research Service. *Technology, Trade, and Security Issues Between the United States and the People's Republic of China: A Trip Report, August 1997*. By Glenn J. McLoughlin, CRS Report 98-617, 30 June 1998, p. 17-18.

Department of Defense, to provide a comprehensive review of actual and potential HPC technology before it leaves the United States (v. III, p. 172).

- An annual threat assessment of HPC exports to the PRC. The U.S. intelligence community would be required by legislation to conduct an annual comprehensive threat assessment of the national security implications of the export to the PRC of HPCs (v. III, p. 173).
- Legislation to require end use verification of PRC use of HPCs. This would include, as a condition of continued HPC export licensing, an open and transparent system of HPC verification by the PRC by September 30, 1999. Failure to establish such a system by the PRC would result in actions by the United States to lower the benchmark levels of HPCs sold to the PRC, denial of export licenses for computers to the PRC, and other appropriate measures. As part of this legislation, an independent evaluation of the feasibility for improving end use verification in the PRC and prevention of the use of HPCs for military purposes would be required (v. III, p. 173).
- Legislation to require that the executive branch encourage other computer-manufacturing countries, especially those countries that manufacture HPCs, to adopt similar export policies towards the PRC (v. III, p. 173).

White House and Congressional Responses

In response, the Clinton Administration agrees with the Cox Committee report that sales of computers to the PRC should be for commercial, not military, purposes.¹³ The Administration also states that it is reviewing the potential national security uses of various configurations of computers, the extent to which these computers can be controlled, and the impact of controls on the U.S. industrial base. The Administration agrees that the United States needs the capability to visit U.S. HPCs licensed for export to China and observe how they are being used (although the Administration contends that it is not possible to obtain no-notice verification visits to any country, including the PRC). On this last point, the Administration did come to an agreement with the PRC for increased site visitations in 1998, but also contends that requiring the U.S. to visit every site where an HPC is installed, regardless of what business the end-user is in or how many times it has been visited before, would be ineffective and wasteful.¹⁴

HPC technology transfer and export control policies, including those related to the PRC, will likely be considered during congressional inquiry into the Cox committee's findings. In the 106th Congress, legislation was introduced by Rep. Hunter on May 26, 1999 that would prohibit the export of HPCs to certain countries

¹³ The White House, *Response to the Report of the Select Committee on U.S. National Security and Military/Commercial Concerns With the People's Republic of China*, May 25, 1999.

¹⁴ Statement by Under Secretary for Export Administration, "Commerce Report: Growing Demand for U.S. High Performance Computers." Washington: U.S. Department of Commerce. 8 January 1999.

until application of existing defense authorization export control policy is implemented. This bill, the Supercomputer Post-shipment Verification Act of 1999 (H.R. 1962), would also require the Secretary of Commerce to conduct post-shipment verification of each digital 2,000 Mtop computer exported from the United States since November 18, 1997 to all Tier 3 countries. The legislation has been jointly referred to the Committee on International Relations and the Committee on Armed Services of the House of Representatives, and awaits further action. On June 9, 1999 the House of Representatives unanimously approved an amendment to the DOD Authorization Act for FY2000 and FY2001 (H.R. 1401) that incorporates several of the recommendations from the Cox Committee report. Among several recommendations, the amendment requires that DOD provide reports to Congress on the national security implications of HPC exports to the PRC.

Management of Department of Energy Laboratories

Background

The Department of Energy (DOE) has nine large, multipurpose, national laboratories and a number of smaller, program-directed or specific-purpose laboratories. Of the former, three are nuclear weapons laboratories: Los Alamos National Laboratory in Los Alamos, NM; Lawrence Livermore National Laboratory in Livermore, CA; and Sandia National Laboratories in Albuquerque, NM and Livermore, CA. These three laboratories account for about 14% of DOE's FY2000 budget request for its laboratories and about 13% of its laboratory personnel (in full-time equivalents). The Cox report judged that the PRC's nuclear weapons intelligence efforts were focused mainly on DOE's three weapons laboratories plus Oak Ridge National Laboratory in Oak Ridge, TN. Oak Ridge also contributes to DOE's national security program, although most of its research and development (R&D) is devoted to DOE's science and energy resources missions (v. I, p. 62). DOE's Pacific Northwest National Laboratory in Richland, WA, also was mentioned in the Cox report as a primary focus, along with the four laboratories mentioned above, of DOE's new counterintelligence plan (v. I, p. 94).

DOE's laboratories comprise the federal government's largest laboratory system. They, especially the nine multi program laboratories, are widely considered to be an important national resource which conducts world-class science and engineering. The nine multipurpose laboratories, and thus the three weapons laboratories and the other two laboratories dealt with in the Cox report, are Federally Funded Research and Development Centers (FFRDCs), which are owned by the federal government but operated by private sector organizations under contract. The contractor of Los Alamos and Lawrence Livermore is the University of California; of Sandia is Lockheed Martin Corp.; and of Pacific Northwest is Battelle Memorial Institute.

Cox Committee Findings

The Cox report's findings that involve the DOE laboratories deal mainly with three areas of concern: *espionage* at the three nuclear weapons laboratories; the *culture of free scientific exchange* at DOE laboratories (common to most scientific laboratories, including the weapons laboratories and the two other DOE laboratories mentioned above) that it believes contributed to the loss of highly classified R&D information from these laboratories; and *management problems* at DOE headquarters and the contractor-operated laboratories that might have contributed to the losses of classified information through espionage or exchanges of scientific information between DOE and foreign scientists.

- The Cox report found that the "People's Republic of China (PRC) has stolen design information on the United States' most advanced thermonuclear weapons; . . . the PRC's next generation of thermonuclear weapons, currently under development, will exploit elements of stolen U.S. design information; and PRC penetration of our national weapons laboratories spans at least the past several decades and almost certainly continues today." These thefts of information "enabled the PRC to design, develop, and successfully test modern strategic nuclear weapons sooner than would otherwise have been possible" (v. I, p. ii). The stolen materials reportedly include classified information on every one of the seven currently deployed U.S. nuclear warheads and their reentry vehicles (including the nation's most sophisticated warhead, the W-88, for the Trident submarine-launched intercontinental ballistic missile), the nondeployed neutron bomb, and other information that could not be identified in the unclassified Cox report because the Clinton Administration has determined that it should not be made public.
- The Cox report states that, in spite of "repeated PRC thefts of the most sophisticated U.S. nuclear weapons technology, security at our national nuclear weapons laboratories does not meet even minimal standards" (v. I, p. x). This finding refers mainly to the counterintelligence activities of DOE and its laboratories, that is, their active combating of espionage activities. After becoming aware of the security problems at DOE's weapons laboratories, the President issued, in February 1998, Presidential Decision Directive 61 (PDD-61), which requires DOE to implement improved counterintelligence procedures. DOE began to implement its improved procedures in November 1998. The Cox report judged that these procedures "will not be even minimally effective until at least the year 2000" (v. I, p. 64). An indication of the counterintelligence problems at the weapons laboratories is that it apparently cannot be determined whether or not the "legacy codes," which are very important in the design of nuclear weapons, have been stolen. This is because "no procedures are in place that would either prevent or detect the movement of classified information, including classified nuclear-weapons design information or computer codes, to unclassified sections of the computer systems at U.S. national weapons laboratories," thus making them accessible, for example, to visitors to unclassified areas of the laboratories (v. I, p. 85).
- A second problem area addressed in the Cox report is the contribution that the scientific "culture" of free information exchange — although restricted by law

in laboratories engaged in classified R&D related to national security — might have played in the transfer of classified R&D information to the PRC.

Scientific information exchanges are important to scientists, including those in the U.S. nuclear weapons laboratories, because such exchanges are considered to be scientifically beneficial to all parties involved. Thus, there is a tradeoff between preventing the transfer of information for national security reasons and promoting the transfer of information for scientific reasons. Following the dissolution of the Soviet Union in December 1991, which marked the end of the Cold War, there was a relaxation of restrictions on scientific exchanges (visits to laboratories, attendance at scientific meetings, and exchanges of scientific information and papers by scientists) with the former Soviet Union and other nations. U.S. and PRC laboratory-to-laboratory exchanges, however, ended in the late 1980s, although they resumed in 1993 (v. I, p. 82). This relaxation of restrictions might have contributed to more relaxed attitudes among scientists and DOE and laboratory management in their interchanges with foreign scientists.

- The report stated that DOE has no “mechanism for identifying or reviewing the thousands of foreign visitors and workers at the U.S. national weapons laboratories” (v. I, p. 94). Another problem identified in the Cox report, which contributes to the natural tendency among scientists to exchange scientific information, is the increasingly widespread use of email and the difficulties associated with controlling information stored on computers and accessible for email transmission (v. I, p. 94).
- The Cox report found that the PRC used scientific exchanges for espionage. “In several cases, the PRC identified lab employees, invited them to the PRC, and approached them for help, sometimes playing upon ethnic ties to recruit individuals” (v. I, p. 80). At an organizational level, the Cox report found that the “China Academy of Engineering Physics [CAEP] has pursued a very close relationship with the U.S. national weapons laboratories, sending scientists as well as senior management to Los Alamos and Lawrence Livermore” (v. I, p. 81). CAEP reports to the Commission of Science, Technology, and Industry for National Defense (COSTIND), the organization in charge of China’s nuclear weapons program.
- A third area of focus of the Cox report is whether management problems at DOE and its contractor-operated laboratories contributed to the theft of classified R&D information by Chinese espionage or the loss of such information through scientific exchanges. For example, although the Central Intelligence Agency (CIA) had evidence in 1995 that secret information on the W-88 warhead had been obtained by the PRC, a DOE “investigation of the loss of technical information about the other five U.S. thermonuclear warheads had not begun as of January 3, 1999, after the Select [Cox] Committee had completed its investigation” (v. I, p. 84). DOE’s new Counterintelligence Director reported in November 1998 that DOE, in effect, has not had a counterintelligence program “for many, many years” (v. I, p. 93).

PDD-61, discussed above, is an attempt to remedy some of these management problems. It requires that a senior Federal Bureau of Investigation (FBI) agent be placed in charge of DOE’s counterintelligence program and that the national security

community submit a report to DOE, with recommendations, on its counterintelligence program. DOE approved that report's substantive recommendations in November 1998. The Secretary of Energy's new counterintelligence plan, based on those recommendations, directs, among other things, that DOE's Office of Counterintelligence "fund counterintelligence positions at individual laboratories so that they work directly for the Department of Energy, not the contractors that administer the laboratories" (v. I, p. 92). DOE's new Counterintelligence Director also has direct access to the Secretary of Energy, unlike his predecessors (v. I, p. 93).

Cox Committee Recommendations

The first eight recommendations of the Cox report refer to DOE's laboratories (v. III, p. 166-168):

- The President should report to Congress, at least every six months, on the steps being taken by DOE and other agencies to respond to PRC espionage, such as the theft of nuclear weapons design information from the laboratories.
- As a matter of urgent priority, DOE should implement, as quickly as possible, an effective counterintelligence program.
- Appropriate congressional committees should review the steps the executive branch is taking to implement PDD-61 and determine if the Administration and Congress are providing enough resources to establish an adequate counterintelligence program at DOE as soon as possible.
- Appropriate executive branch departments and agencies should conduct a comprehensive damage assessment of the security breaches at DOE's laboratories since at least the late 1970s and report to Congress.
- Appropriate congressional committees should report legislation, if necessary, to achieve effective counterintelligence in DOE.
- DOE and four other agencies should direct their inspectors general and counterintelligence officials to examine risks to U.S. national security due to the international scientific exchange programs of the DOE laboratories, and report their findings to Congress by July 1, 1999.
- Congress should examine whether DOE can protect nuclear weapons and related research and technology from theft and exploitation and whether it should retain responsibility for the nation's nuclear weapons development, testing, and maintenance.
- Because the executive branch failed to report adequately to Congress about thefts of secrets from the laboratories, as required by law, Congress should require strict compliance.

White House and Congressional Responses

The White House responded to the release of the declassified version of the Cox report on May 25, 1999 with a press release¹⁵ on the same day. Noting President Clinton's written response to the recommendations on February 1, 1999, the press release stated that, although the Administration does not agree with all of the analysis of the report, it does agree with all of the recommendations concerning laboratory security, "many of which we have been implementing for months, and in some cases, years." The press release noted that the President, recognizing the need to respond to the national security threat to the DOE laboratories in 1997, issued PDD-61, calling it "the most comprehensive and vigorous attempt ever taken to strengthen security and counterintelligence procedures at the labs."

The press release identified how the Administration has responded or is responding to the recommendations of the Cox report:

- On March 29, 1999, DOE submitted to Congress its annual *Report on Safeguards and Security at the Department of Energy Nuclear Weapons Facilities* and the CIA, in coordination with other agencies, is preparing a semiannual report to Congress on the measures being taken to protect against PRC's efforts to obtain nuclear weapons and other classified information.
- DOE is implementing PDD-61 on an "expedited basis" according to the plan submitted to Congress on January 5, 1999 and has instituted additional counterintelligence actions at the laboratories, including in the "critical area of cyber security" involving its classified computers.
- The CIA, at the direction of the President, conducted an assessment of damage caused by PRC espionage, which was reviewed by an independent panel headed by Admiral David Jeremiah. Congress received a briefing on the review on April 21, 1999.
- The President directed DOE to complete an interagency assessment of laboratory-to-laboratory programs with China, Russia, and other sensitive countries by June 1, 1999.

In addition to these responses to the Cox report's recommendations, the President directed former Senator Warren Rudman, Chairman of the Foreign Intelligence Advisory Board, to evaluate security at DOE's laboratories, and directed the National Counterintelligence Policy Board to make recommendations to strengthen controls on nuclear information at facilities other than the laboratories that deal with nuclear weapons issues.

The Administration's response did not deal explicitly with the Cox report's seventh recommendation that Congress examine "whether [the] Department of

¹⁵ The White House, *Response to the Report of the Select Committee on U.S. National Security and Military/Commercial Concerns With the People's Republic of China*, May 25, 1999.

Energy should maintain U.S. nuclear weapons responsibility" (v. III, p. 167). This is an issue that has arisen in the 104th, 105th, and 106th Congresses in the context of legislation introduced to restructure, and possibly abolish, DOE and transfer its laboratories to other federal agencies or privatize or close them. Under many of these bills, the DOE weapons laboratories would be transferred to the Department of Defense. The national security issues addressed in the Cox report might contribute to congressional debate on these types of bills, none of which was enacted in the 104th and 105th Congresses. Thus far in the 106th Congress, two bills to abolish DOE (S. 896 and H.R. 1649) have been introduced. These bills, among other things, would transfer the nuclear weapons laboratories to DOD.¹⁶

Other legislation in the 106th Congress also would affect DOE's laboratories. The Senate, for example, in its consideration of the National Defense Authorization Act for FY 2000 (S. 1059) following the release of the Cox report, debated an amendment (no. 446) to create a "National Security Administration" within DOE which would have responsibility for nuclear weapons production facilities and the national laboratories. Although this amendment was withdrawn, it was announced that the proposal would be offered as an amendment to the Intelligence Authorization Act for FY 2000 (S. 1009). S. 1062 (the DOE National Security Act for FY 2000, passed by the Senate as Division C of S. 1059) also includes a provision for a moratorium on DOE's laboratory-to-laboratory and foreign visitors and assignments programs. H.R. 1401, the House version of the National Defense Authorization Act includes a provision to establish a "Commission on Nuclear Weapons Management" which, among other things, would examine DOE's nuclear weapons laboratories and propose and evaluate alternative organizational and management structures, including possibly transferring authority for the laboratories to DOD. The Cox amendment to H.R. 1401 includes, among other things, a moratorium on foreign visitors at national laboratories pending background reviews. The Costello amendment to H.R. 1401 would make the contractors that operate and manage DOE laboratories subject to civil penalties of up to \$100,000 per violation of any DOE rule, regulation, or order relating to the security of classified or sensitive information. Another recent bill, S. 887, also would establish a moratorium on the foreign visitors program at DOE's nuclear laboratories

¹⁶ For a discussion of these issues and current legislation, see Congressional Research Service, *Restructuring DOE and Its Laboratories: Issues in the 106th Congress*, by William C. Boesman, CRS Issue Brief 10036, updated regularly, 10 p.



U.S. DEPARTMENT OF COMMERCE
Office of Special Matters

To : *Bill R.*

From : John F. Sopko
Chief Counsel

*I thought you would
be interested in this time
line. It's a very rough and
does not include all of John Henry
etc. This is what the
Republicans will be doing
to try to put DOC back
into the controversy*

JF

FORM CD-82A LF
(REV. 10-83)
DAO 214-2

Please keep close hold on this.

To: File

From: John Sopko

Subject: China Spy Timeline

Date: 3/17/99 5:26 PM

[Chronology based on NY Times, Washington Post, and discussions with media, DoE, FBI and CIA officials. All open or unclassified sources]

--April 1995: DoE analysts discovered similarities between Chinese weapons tests of small nuclear weapon and W88 warhead and bring their concerns to DoE Office of Intelligence's Notra Trulock, who suspects espionage.

--June 1995: CIA obtained a document from Chinese official, re its nuclear weapons program. W88 is specifically mentioned.

--October 1995: Johnny Chung brings Chinese energy officials to meet with Secretary of Energy Hazel O'Leary. Chung introduces same officials to Clinton that night at Africare Dinner...unknown if any connection with spy scandal.

--February 1996: DoE and FBI began search of lab travel records and other data, which identify five possible suspects, including Wen Ho Lee.

--April 1996: Sandy Berger, then deputy NSA, was briefed on the possible theft of W88 design data. No specific suspect was identified.

--May 1996: DOE completed its security review in conjunction with the FBI

--June 1996: FBI opened a formal investigation into the case.

--July 1996: China completed its evaluation of new warhead technologies.

--July 1996: the FBI and DOE briefed the Senate Intelligence Committee.

--August 1996: the FBI and DOE briefed the House Intelligence Committee.

--September 1996: first stories re Asian campaign fund-raising break in the LA Times.

--November 1996: Clinton reelected.

--December 1996: DoE asked FBI re status of the case; is convinced FBI has devoted few resources to the case;

- January 1997: Federico Pena becomes Secretary of Energy.
- March 1997: Trulock requested a meeting with Pena
- April 1997: FBI issued a classified report on the labs, recommending reinstatement of background checks on foreign visitors.
- July 1997: Thompson committee hearings began.
- July 1997: Trulock finally met with Pena, was immediately sent to White House to meet with Berger.
- July 1997: Berger briefed Clinton.
- July 1997: DoE briefed CIA, FBI, DoJ, others over several weeks in late July, early August re progress of investigation.
- August 1997: CIA Director George Tenet and FBI Director Louis Freeh met with Pena to discuss lax security at the labs. Pena expresses shock.
- August 1997: Berger flew to Beijing to meet with Chinese officials to prepare for the summit.
- August 1997: Berger asked Gary Samore, proliferation expert on NSC staff, to order up a CIA analysis on Chinese development of the smaller warhead.
- September 1997: Samore told Berger CIA is less conclusive than DoE on extent of damage.
- September 1997: Freeh told DoE officials the bureau did not have enough evidence to arrest Lee. The case was seen as inconclusive. But he reportedly added there was no reason to let him keep his security clearances. DoE denies this.
- October 1997: CIA and DoE analysts met with Samore at White House to discuss their competing analyses of the warhead issue.
- October 1997: Clinton in China for summit.
- February 1998: Clinton signed Presidential Decision Directive 61 requiring better security at the labs.

Appendix Item 8

THIS FORM MARKS THE FILE LOCATION OF ITEM NUMBER 1
LISTED IN THE WITHDRAWAL SHEET AT THE FRONT OF THIS FOLDER.

THE FOLLOWING PAGE HAS HAD MATERIAL REDACTED. CONSULT THE
WITHDRAWAL SHEET AT THE FRONT OF THIS FOLDER FOR FURTHER
INFORMATION.

--February 1998: DoE begins process to find director of the office of counter intelligence to fulfill recommendations of PDD 61.

--April 1998: Edward Curran, former FBI agent, begins work as director of office of counterintelligence at the DoE, begins three month overall assessment of lab security.

--May 1998: First stories re Loral helping Chinese missile program break in New York Times.

--July 1998: Pena leaves DoE; Betsy Moler becomes acting secretary.

--July 1998: House Intelligence Committee requested an update from DoE. Trulock, who has been passed over by DoE Secretary William Richardson, for counterintelligence job, says Moler ordered him not to brief committee. **(Check source on this, was it Moler or was it Richardson? What role did Dick Clark play?)** DoE denies this. [REDACTED]

--September 1, 1998: Trulock briefs Cox committee re HPC's

--September 1998: Bill Richardson becomes Secretary of Energy.

--September 1998: On his second or third day as secretary, Freeh and Tenet briefed Richardson on lab security. He reacts immediately.

--October 1998: Trulock claimed he was not permitted to discuss espionage activities at the lab in his statement to the House Intelligence Committee. He answered questions however when questioned by committee members.

-- November, 12 & 14, Trulock briefs Cox committee re proliferation issues.

--November 1998: Lee lost security clearances, 14 months after Freeh reportedly told DoE he had no objection to DoE removing clearances. Richardson denies this, says he did not have assurances from FBI until March 1998.

--December 1998: Lee was given first lie detector test. Results were inconclusive.

--December 16, 1998: Trulock briefs Cox committee re proliferation issues.

--January 1999: allegations of espionage are included in Cox Committee report on Chinese-US relations and effect on national security.

--January 1999: Wall Street Journal and Washington Post report on allegations.

--February 1999: Lee was given second lie detector test. He fails it.

--March 1999: New York Times report on allegations, providing more details.

--March 1999: Lee fired.

EASMSATELLITENERGY~1.

Barry Phelps

From: The White House [Publications-Admin@pub.pub.whitehouse.gov]
Sent: Thursday, January 11, 2001 9:50 AM
To: Public-Distribution@pub.pub.whitehouse.gov
Subject: 2001-01-10 Telephone Briefing by Podesta Reinsch and DeLeon

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release

January 10, 2001

TELEPHONE BRIEFING BY
CHIEF OF STAFF JOHN PODESTA,
UNDER SECRETARY OF COMMERCE BILL REINSCH,
AND DEPUTY SECRETARY OF DEFENSE RUDY DELEON
ON U.S. EXPORT CONTROLS ON HIGH PERFORMANCE COMPUTERS

1:37 P.M. EST

MR. PODESTA: Why don't I start. And I think Secretary DeLeon and Mr. Reinsch will be following onto what I am about to say. I will try to be relatively brief and I think we all will be, so that we can get to your questions. I believe you have paper in front of you, but as you know, the President today is announcing the sixth revision to U.S. export controls on high performance computers since 1993.

We have been controlling them, I think as most of you know, controlling high performance computer exports, using a hardware performance measure called MTOPS -- Millions of Theoretical Operations Per Second. Our policy goal in doing that was to limit the acquisition of high performance computing capabilities by potential adversaries and countries of particular proliferation concern, and to ensure that U.S. -- simultaneously ensure that the U.S. computer industry could compete in most foreign markets.

Until recently, we kept pace with growth in high performance computing hardware availability by periodically adjusting controls. As I've said, we've revised them five times between 1993 and the year 2000. At the President's direction, DOD has been reviewing alternatives to this control mechanism as the ability of the hardware and the availability of essentially commercial end technology was outpacing this methodology for being able to control high end computing performance.

He asked the DOD to review alternatives to these control measures since mid 1999. The review included relevant agencies and brought in private sector experts. That review concluded that our ability to control the acquisition of HPC capabilities by controlling computer hardware is already ineffective and it will be increasingly so within a very short time frame.

So we set about to focusing on enhancing the already strong controls on critical software applications, such as nuclear, military, radar cross section applications. Rudy can go into more. And based on this review, the President has decided to adopt a number of consensus -- and I say consensus, I mean consensus amongst the agencies recommendations -- from his national security agencies.

Again, if you have the fact sheet in front of you, you will note that what we are doing is combining the old tier one which were essentially friends in our allied countries with Tier 2, the countries that posed a proliferation risk, into a new Tier 1. And those exports to the new Tier 1 countries won't require a license, although there will be some continued post shipment reporting requirements. And that change

will be effective when Commerce publishes the rule, which we expect to do before we vacate the premises on January 20th.

We are moving Lithuania from Tier 3 to the now combined new Tier 1, based on improvements to its export control system, and continued good cooperation on export controls. That will be effective pursuant to legislation. That will be effective 120 days after notice goes to Congress, which will be in the next several days, I guess. And then we will raise Tier 3 licensing and defense authorization act notification level to 85,000 MTOPS. This is the performance level of uncontrolled computers the DOD has determined can be easily networked together by relatively unskilled individuals. That new level will be effective 60 days after notice goes to Congress.

Q Did you say 60 days?

MR. PODESTA: Yes, 60 days. Again, Congress changed that provision. It used to be six months. They shortened that time period to 60 days during the last year. And finally, we will maintain the virtual embargo on exports to terrorist countries.

Let me see, before I turn it over to Rudy. I just wanted to mention one more thing, which is that it is our recommendation that we will be making to Congress that we repeal the 1998 Defense Authorization Act provisions that require notification and licensing of certain computer hardware exports and waiting periods for adjustments in control levels, which eventually will permit the elimination of Tier 3 hardware controls.

I think I want to turn it over to Rudy for his comments, and maybe some comments on our ability to work towards strong controls on critical software applications from a national security prospective.

DEPUTY SECRETARY DeLEON: This is Rudy DeLeon at the Department of Defense. Let me just make some brief comments. High performance computing capability is -- this capability is linked to a healthy U.S. computer industry, and the ability of that industry to continue to produce products with increased capabilities. Computer hardware controls are no longer effective, and in fact, this intensifies American computer development.

Eighteen months ago we recognized that the MTOP metric was becoming ineffective, and we undertook a study to see if alternative measures could be developed. We found no effective hardware export control measures. However, after extensive review, determined that we could effectively control critical application software. So on software controls, effectively exploit high performance computing capabilities, one needs critical application software. Software cannot be produced over night. Much of it requires very extensive coding and data obtained from -- adjusting for validations.

We recently completed a study that recommends technical control measures for application software. The Secretary of Defense has allocated additional funding in the fiscal '02 budget that we're working on to implement these initiatives and further develop these technologies that will restrict adversaries from using and reverse engineering critical application software.

We have in play policy measures for controlling the release of our critical application software, which if adequately enforced, prevents dissemination to adversaries. We intend to introduce additional education and training to make measures even more effective.

So with this revised strategy, we will ensure the performance computing capabilities that are critical to national security will continue to be effectively protected. And I think on the basis of this reasoning, able to strongly --

MR. PODESTA: You just faded out, Rudy. Could you go back over that point again?

DEPUTY SECRETARY DeLEON: Which is the piece?

MR. PODESTA: Just the last sentence you were just about to do.

DEPUTY SECRETARY DeLEON: Just that with this revised strategy, we will ensure that those high performance computing capabilities that are critical to the national security of the United States continue to be effectively protected. And on the basis of this line of analysis, and after our studies, we strongly support the direction that the President is announcing today.

MR. PODESTA: Bill?

UNDER SECRETARY REINSCH: If I can add a little bit, as Rudy mentioned, this is first and foremost a national security decision. One element of this, as we've made clear -- one element that's central to our national security is maintaining the good health of the computer industry, so they can continue to make cutting edge products, which are useful for our military and intelligence establishments.

More than 50 percent of the sales of these companies come from exports. And so capturing market share abroad and staying on the cutting edge of the market is very important to them to. You would have to talk to the industry to get specific statements about likely impact. Our judgement is that this decision will have a favorable impact on their marketplace in several ways.

At the high end of these machines, you're talking about large servers. And these are servers whose primary applications are in financial services, banking and the like, essentially account customer maintenance, things like that. And also for inventory use for large retail establishments or manufacturing establishments, taking care of complex inventories where there might be multiple manufacturing locations is also a use of these servers. They also have applicability in automobile manufacturing and other kinds of manufacturing units, where there's a lot of machines that have to be controlled.

One area of very rapid growth for all those activities is in Asia and Southeast Asia, and these are primarily formerly two-tier countries. So we envision that combining the tiers into one will give our companies a substantial opportunity to market products at this higher end in countries where there has been a rapid growth in all of the sectors that I just described.

Q I was wondering if you could talk about the decision to collapse one and two, given some -- it just seems like a significant shift in attitude. Is that -- and also why this is coming out just now.

UNDER SECRETARY REINSCH: Well, I think the core of the decision here, frankly, is that the Defense Department came to the conclusion that we were not able to effectively control hardware. The technology is simply ubiquitous and out there, and that, in fact, our national security needs to be met through the other means that Rudy described.

Given that situation, the distinction between Tier 1 and Tier 2 is no longer particularly important. Now, we have a statutory requirement via the National Defense Authorization Act which, as John Podesta pointed out, the President is supposed to repeal, to maintain a control parameter for Tier 3. But the essence of this decision is that there is no longer utility to maintaining those parameters, and so the best way to implement that is to collapse the two tiers into one.

Q I just wanted to follow up on that, and maybe this is a question for Mr. Reinsch -- just to put this in sort of context for us and help us understand the importance of what you've done, merging one and two, that I would assume is more important for you than bumping up the MTOPS in the Tier 3 to 85,000 -- is that a fair presumption?

UNDER SECRETARY REINSCH: In the short term, yes. In terms of

the Tier 2 market -- the Tier 3 market has consistently been in the 5-10 percent range of total sales. At the same time I should note that two of the most rapidly growing and largest economies of the world, India and China, are in Tier 3. So what we do in Tier 3 is not insignificant in commercial terms. But that's a little bit down the road. The immediate advantage I think will be in precisely where you said, in combining the two tiers.

MR. PODESTA: There was a separate question of why now. We have been on a track actually for some time, working with industry, to review -- especially because of what was a six-month and now a 60-day lag time in shipping to Tier 3 exports -- to review where we were to make sure that we weren't effectively impeding our computer companies from being able to compete in terms of shipping product to markets that was essentially off-the-shelf kind of standard product. And I think that we had gotten -- because the statute was on a kind of six-month review cycle, we were kind of on a six-month review cycle. And although we had proposed shortening that to 30 days, Congress ultimately settled on 60 days.

We're in the throes of doing our regular review of progress that was being made in the industry in terms of what they were shipping as essential commodity-style, off-the-shelf product, and that led to the timing taking place now, in January.

Q I want to ask about your stance that controlling of hardware is not as easy or may not be as effective as controlling software, when it seems that bits would probably flow through borders surreptitiously much easier than maybe crates of computers.

DEPUTY SECRETARY DeLEON: This is Rudy DeLeon. I think we spent much time looking at what a proper regulatory mechanism was. The industry is moving production where the MTOPS measure became meaningful. And as we looked at it further, application of the hardware that becomes critical for national security purposes -- it's not the hardware, but rather the software that allows you to do the applications that becomes critical.

Some significance -- (breaking up) -- transitioned in a decade from a era dominated by -- (breaking up) -- computers to a nation where computers and networks together can give you just as much -- (breaking up) -- ability. So what becomes critical in this environment are two things -- is there knowledge on the software through the applications of the software that allows hardware to do these computations. Then second, you have skilled people who know how to maximize software -- (breaking up) -- after examining it in great detail -- (breaking up) -- are very much committed to the national --

Q Rudy, you're breaking up. Could you repeat that?

DEPUTY SECRETARY DeLEON: What part? People here are very much dedicated -- (breaking up) -- national security interest came to the conclusion that hardware -- (breaking up) --

Q Rudy, you're breaking up, like the past three sentences.

DEPUTY SECRETARY DeLEON: Okay, I'll repeat it again. The dedicated people here that are really focused and concerned about national security issues came to the conclusion that it is the application software plus trained and skilled people who know how to utilize the capabilities that is embodied in the hardware, that that is the critical path.

Q Who makes this type of software? I mean, is there a small core of specialized developers?

DEPUTY SECRETARY DeLEON: This is a highly specialized software industry that is unique to the national security side.

MR. PODESTA: Yes, when Rudy is talking about controlling software, we're not talking about either going on-line or walking into a

-- and buying something on a floppy disk. These are big, complicated, sophisticated programs that are done largely for our national security industry. And that, I think, goes back to Ted's original question, which is how do you control this stuff. Well, there are controls in place on that now and we're really after the most cutting-edge, I suppose, if you will, kinds of big programs.

Q Someone there mentioned the Tier 3 distinction might have been simply done away with. Could you elaborate on that a little more?

UNDER SECRETARY REINSCH: Yes, John mentioned it in the President's proposed repeal of the statute that requires it. But to go back to something that I said a couple minutes ago, once you come to the conclusion that the Defense Department has come to -- namely, the futility of hardware controls -- there is no longer a national security rationale for maintaining those controls on any countries except the embargoed states, the terrorist states.

We are required by law to maintain a control standard based on MTOPS for Tier 3. But the President has recommended that provision be repealed, and if the Congress were to do that, then the next administration would be in a position to remove the MTOPS limit on Tier 3 as well if it wanted to do so.

Q So this move today includes recommendations that Tier 3 be repealed --

UNDER SECRETARY REINSCH: Well, you have to phrase it a little bit differently than that. It contains a recommendation that the provisions in the National Defense Authorization Act to require a Tier 3 and an MTOPS limit be repealed.

Q In the paper you handed out, you noted that the Clinton administration recognizes that the incoming administration needs an opportunity to examine such a proposal and intimated there that you might be doing less than you might have done if you didn't have just two weeks left to go. Is there anything more that you would have liked to do or that you're recommending that the Bush administration do, aside from the congressional repeal?

MR. PODESTA: Well, if I'm not mistaken, the President-elect's over at the Pentagon as we speak, or has just left. (Laughter.) So I think that we want to brief their team about the study that was undertaken and coordinated interagency, but led by the Defense Department, and where we see the ability to be able to control the critical, from a national security perspective, technology going in the future, and also I think share our views on the necessity of keeping our own computer industry and our own software industry first in the world, because that is really another element of not only our continued economic performance, but our continued ability to provide the national security community with the highest level of capability and capacity.

And I think we want to share that with them, and they will have to kind of pick up this issue and pick up this ball and decide whether the suggestions we're making, for example, on these legislative proposals are wise and ought to go forward, and to -- hopefully, to continue the dialogue that I think we've had, which has been constructive with not only interagency, but with our high tech community.

Q Can I ask how broadly will the definition be of the restricted software -- and the national security and proliferation related software? That could theoretically be a pretty ambiguous definition.

UNDER SECRETARY REINSCH: If I can interject there -- and I think Rudy will comment, too -- I think we are talking about a universal software that is already classified, already controlled, already clearly defined.

DEPUTY SECRETARY DeLEON: It is already controlled from the --

regime, and that is because most of this application software is based upon empirical data that is classified.

MR. PODESTA: And we're not talking about expanding that.

DEPUTY SECRETARY DeLEON: Correct.

Q But getting back to the next administration, in order to get rid of Tier 3, that's something that Congress would have to do, that hardware review. Or, is there something that, administratively, this administration or the next administration could do that would eliminate those regulations?

UNDER SECRETARY REINSCH: As a legal matter we have interpreted the NBAA to require the creation of a Tier 3 and a control of Tier 3 on the basis of a number of MTOPS. Now, Tier 3 was an administrative creation of the Executive Branch, as were Tiers 1, 2, 3 and 4, and it might have some utility that goes above and beyond computers. It's not the existence of a tier that is the important question as much as it is in the statute the requirement that exports to those locations be controlled on the basis of the number of MTOPS. And that's what we would propose repealing.

Q Who is saying this?

UNDER SECRETARY REINSCH: This is Bill Reinsch saying that.

Q Bill, for analogy's sake, so our readers can understand this, 85,000 MTOPS -- can you equate that to X-number of Pentium Xs linked together?

UNDER SECRETARY REINSCH: It's 32 Pentium IIIs.

Q This won't allow the export of --

UNDER SECRETARY REINSCH: Well, two things. The President's decision doesn't include the export of individuals. It doesn't change anything with respect to the export of individual chips, which are also subject to their own MTOPS requirement, which is not the subject of this conference, so we haven't changed anything there. There is a limit on those, and I don't know the plural of itanium is -- itania or itaniums that go over 6,500 MTOPS would be subject to license one by one.

Computers that contain them would not come under this restriction as well, depending upon what their overall power was.

UNDER SECRETARY REINSCH: I'll be around if people have follow-up questions and want to call me at my own office, which is: 482-1455. I can follow up there if anybody is interested.

DEPUTY SECRETARY DeLEON: And this is Rudy DeLeon, and I'm reachable here at the Pentagon, and we have a team of people that can be available as well. Let me just say that on the issue that hardware controls are no longer effective, this is really a conclusion that DOD has come to. We're really looking for an alternative mechanism and we appreciate the support from the White House and the Commerce Department to find an alternative mechanism.

Q Thank you. Good-bye.

END 2:07 P.M. EST

U.S. National Security And Chinese Espionage

General Observations

- 1) Allegations about the extent of Chinese espionage over the past 20 years or more concern all of us who care about America's national security.
- 2) The problem of security at our nuclear laboratories goes back through several Administrations and is being aggressively addressed by the President and the Department of Energy.
- 3) These are fundamental national security concerns that require nonpartisan solutions. It doesn't help to start pointing fingers; we need to point the way upward safeguarding our future, not scapegoating our past.

Intelligence Community Perspective

- 1) The Intelligence Community completed a damage assessment April 21st and released an unclassified version of its findings. Those findings differ from recent news reports, particularly on how much nuclear weapons information China has acquired from our labs and how significant this information is for China's modernization program.
- 2) The damage assessment found that:
 - 1) China obtained some nuclear information from the U.S. that probably accelerated its modernization program, but experts don't believe they are seeking to replicate U.S. weapon designs.
 - 2) Chinese technical advances have been made on the basis of a wide variety of information, including classified and unclassified sources, contact with American and foreign scientists, and its own resources. The relative contribution of these various sources cannot be determined.
 - 3) Chinese efforts to acquire nuclear secrets have not resulted in any apparent modernization of their deployed strategic force or any new nuclear weapons development.
 - 4) The Intelligence Community's report was endorsed by a highly respected, bipartisan group of experts headed by Admiral Jeremiah and including former National Security Advisor to President Bush, General Sewareff.

Historic & Strategic Context

- 1) We should not lose sight of the historic and strategic context of the current debate. Much of the nuclear weapons related information was acquired by China in the 1970's and 1980's and involved technology and concepts that are even older.
- 1) Theft and security concerns involving our nuclear laboratories is, in a word used by Rep. Cox, an "endemic" problem spanning several administrations. News reports dating back to 1990 revealed the theft of nuclear secrets from an American nuclear laboratory.
- 1) Numerous GAO reports throughout the 1980's and 1990's highlighted concerns about lax security at our nuclear laboratories.
- 1) China, despite its size, remains a very small nuclear power, with fewer than two dozen long-range missiles. We have over 6,000 strategic nuclear warheads. France is a greater nuclear power than China.

Partisan Charges

- 1) The Cox-Dicks Committee was charged with investigating, among other things, whether there was any connection between campaign contributions and national security decisions. But, as Representative Dicks has said himself, "campaign contributions played no role in any decision that was made."
- 1) Suggestions by some critics that the White House worked to keep the Cox-Dicks report from getting out, or to remove accurate, but politically damaging information are absolutely false. Rep. Cox himself said on ABC last Sunday that "it would essentially be the same report" if the House of Representatives had had the sole authority to declassify it.
- 1) Similar charges that the Congress was not adequately briefed are not true. The Administration briefed appropriate committees and members of Congress on a number of occasions over the last several years.
- 1) The President's remarks about Chinese nuclear espionage at the national laboratories are accurate. We know of several instances in the late 1970's and the 1980's in which China obtained nuclear information from the labs. But reporting about a loss of nuclear information to China in the mid-1990's does not link the loss to the labs.

What To Do

- 1) The bottom line is that China, like a number of other countries, has attempted to obtain secrets from us and other nations over many years, and we need to be vigilant. We must continue to take strong measures to protect our nuclear secrets from theft and to safeguard our high technology products from misuse.

- The President recognizes these concerns, and that is why he issued a wide-ranging presidential directive in February, 1998 that ordered sweeping measures to strengthen counterintelligence at our nuclear laboratories (this directive was issued before the Cox-Dicks Committee was even formed).
- Under the leadership of the President, and at the direction of Energy Secretary Bill Richardson, the Department of Energy has:
 - Appointed an FBI official (Ed Curran) to oversee DOE's counterintelligence program.
 - Established a program for polygraph tests for key scientists and thorough background checks for foreign visitors from sensitive countries.
 - Instituted major improvements in computer security at the labs.
- The Clinton Administration also has dramatically increased DOE's counterintelligence budget. This year's \$15.6 million budget is itself six-times bigger than 1996's \$2.6 million. And the Administration is requesting \$40 million in next year's budget.
- The White House has embraced the vast majority of reforms recommended by the Cox-Dicks Committee. In fact, many of those changes were already underway when the Committee began its work last year.
- We also have the tightest controls of any major country on high tech exports to China, and we have been very effective in preventing diversion of such items, such as high performance computers and satellites, to military purposes.
- The President and members of Congress from both parties are determined to work together to do whatever is necessary to safeguard our nuclear and technological secrets and ensure our nation's security in the 21st century.
- We are determined to move ahead with a clear-eyed policy of strategic engagement with China, so that we can continue to encourage China to prevent the proliferation of weapons of mass destruction, to work with us to build a stable and lasting peace in Asia and to promote greater democratization and respect for human rights.
- This policy has already yielded important results. China signed important arms control agreements, including the Comprehensive Test Ban Treaty in 1996, which will limit China's ability to modernize its nuclear weapons. China has ended nuclear assistance to Iran and to Pakistan's unsafeguarded nuclear program. And China is working with the U.S. to deal with proliferation concerns in North Korea and South Asia.

Security At U.S. Nuclear Weapons Laboratories Is An Issue Affecting Republican And Democratic Administrations. Government And News Reports About Potential Leaks Go Back More Than A Decade.

From The New York Times, 1990

"Chinese intelligence agents succeeded in stealing nuclear-weapons secrets from the Government's Lawrence Livermore National Laboratory in the 1980's, and the Federal Bureau of Investigation later conducted a long espionage inquiry into the theft, American intelligence experts said today....

Officials in Washington said the Chinese had sought an array of nuclear-weapons information from Livermore and other Government-financed weapons laboratories....

...another [official] said the Chinese apparently got most, if not all of the data they needed by exploiting lapses in routine security procedures....

The New York Times, November 22, 1990

From The Associated Press, 1990

"Information that helped China develop a neutron bomb was stolen from Lawrence Livermore National Laboratory through espionage, according to a published report....

George Carver, a former deputy director of the CIA, said publicly last month that the Chinese success was based on U.S. nuclear research.... 'In 1989...the Chinese blossomed forth with the neutron bomb, which was made from data stolen from U.S. research centers,' he said in a speech to Lawrence Livermore employees. ...

The General Accounting Office reported in 1988 that foreign intelligence agents posing as visiting scientists had gained access to Lawrence Livermore and America's other two nuclear weapons design laboratories. "

The Associated Press, November 22, 1990

"... a General Accounting Office (GAO) report 10 years ago that warned the Reagan administration of 'major weaknesses' in the foreign visitors program at the nation's nuclear weapons laboratories. Including suspected foreign agents from Russia, China and other 'sensitive' countries being able to make visits 'without prior DOE knowledge.'

The October 1988 GAO report followed an FBI investigation of alleged spying at the Lawrence Livermore National Laboratory in the early 1980's and numerous internal DOE studies critical of security.

Brent Scowcroft, President George Bush's national security adviser, said lab security 'was not an issue' during his time in office. He said he was unaware of the GAO report and was surprised to hear that stories were published about the alleged Chinese stealing of secrets about the neutron warhead at the labs.

Rep. Christopher Cox...said yesterday in reference to the early GAO report that security at the labs "is best understood as an endemic problem.

The 1988 GAO report referred to a 1983 DOE study that concluded 'a significant amount of important technology may have been lost to potential adversaries through visits.' In addition, DOE's own vulnerability studies in 1984 and 1985 found that 'information on classified programs could be derived from...observing activities at these facilities.'

Although background checks were required for all visitors from communist countries, the study found that such checks were not done for 119 of 181 individuals sampled during 1987...."

The Washington Post, March 19, 1999

Director Freeh: "In terms of the overall counterintelligence deficiencies in the national laboratories, as I mentioned, Senator Glenn first highlighted this, at least in terms of our search, in 1988. He had hearings, he wrote a report, and there were a series of other reports...So the problem in terms of a problem has been around for a long time...."

House Appropriations Committee Hearing, March 17, 1999

Representative Dicks: "The most important thing [the American people] will learn is that for 20 years, starting in the '80's, we had a major counterintelligence failure at Los Alamos and at the other national labs that is now being corrected but will only be corrected if we stop playing the blame game and start working together to make sure that the resources are provided and the oversight is provided to implement that plan...."

NBC Meet The Press, March 14, 1999

There Has Never Been Any Connection Between Campaign Contributions And The Clinton Administration's National Security Policies And Decisions.

Rep. Dicks: "...in our investigation, we found that campaign contributions played no role in any decision that was made. I asked witness after witness, 'Were you put under any pressure to change a decision on a national security matter because of political influence,' and the answer was no in every case."

NBC Meet The Press, March 14, 1999

"China's ballistic missile advances and its efforts to influence the 1996 elections were addressed in separate sections of the report. This was done, committee aides said, at the insistence of an influential Democrat, Senator Carl Levin of Michigan, to underscore that no link between the two matters had been found."

The New York Times, May 7, 1999

Security Concerns At America's Nuclear Facilities
Excerpts From GAO Reports, 1980 - 1992

March 1980 "Nuclear Fuel Reprocessing And The Problems Of Safeguarding Against The Spread Of Nuclear Weapons"

"Adequate safeguards to prevent the theft or diversion of weapons-usable material from commercial nuclear fuel reprocessing plants have not yet been developed."

May 1986 "DOE Has Insufficient Control Over Nuclear Technology Exports"

"DOE has... authorized exports without review for sensitive nuclear technology..."

March 1987 "DOE Reinvestigation of Employees Has Not Been Timely"

"In summary, we found that DOE headquarters and some field offices have been unable to meet DOE goals to reinvestigate security clearances....(DOE offices) have almost 76,000 employees who have not been reinvestigated within the last 5 years as DOE now requires."

August 1987 "Department Of Energy Needs Tighter Controls Over Reprocessing Information"

"...countries that pose a proliferation or security risk routinely obtain reprocessing information published by DOE....DOE has transferred to other countries information appearing to meet the definition of sensitive nuclear technology...DOE places no restrictions on foreign nationals' involvement in DOE-funded reprocessing research at colleges and universities.... Each year between 15,000 and 20,000 foreign nationals visit or are assigned to work at DOE's facilities...In 1983 DOE found that its monitoring of these activities had not been adequate, and significant energy information may have been lost to foreign countries."

December 1987 "DOE Needs a More Accurate and Efficient Security Clearance Program"

"...DOE has not maintained accurate clearance data bases...Clearance files...contained over 4,600 clearances that should have been terminated, and in over 600 other cases employees had clearance badges but did not have active clearances listed on the clearance files."

June 1989 "Better Controls Needed Over Weapons-Related Information and Technology"

"...communist-controlled nations, countries suspected of developing nuclear weapons, or those viewed as a national security risk -- have obtained information dealing with detonators, explosives, and firing sets that could assist or enhance nuclear weapons development. Foreign nationals obtain some information directly from DOE's weapons laboratories; DOE does not require the laboratories to track these requests."

April 1990 "DOE Oversight of Livermore's Property Management System Is Inadequate"

"...as of mid-January, laboratory managers could not locate 16 percent, or 27,528, of the items recorded in the laboratory's property management data base....The laboratory does not have adequate accounting controls to ensure that property in its custody is safeguarded...."

October 1990 "Potential Security Weaknesses at Los Alamos and Other DOE Facilities"

"...GAO found that most of the regular security force lacked one or more of nine skills that DOE officials say are needed to ensure the minimum level of protection for the site. Over 75 percent of the regular security force lacked such skills during an unannounced April 1990 exercise...."

February 1991 "Accountability for Livermore's Secret Classified Documents Is Inadequate"

"A substantial number of secret documents cannot be located....These documents cover a wide range of topics including nuclear weapons and laser design...a recent inventory of secret documents at the laboratory identified over 12,000 missing secret documentsneither the laboratory nor DOE can provide assurance that the national security has not been damaged."

March 1991 "DOE Needs Better Controls to Identify Contractors Having Foreign Interests"

"Overall, neither DOE nor its government-owned contractor-operated weapons laboratories fully complied with DOE's regulations and procedures for determining whether contractors are subject to foreign interests and for preventing associated risks....DOE has several internal control weaknesses that could cause further problems in safeguarding classified matter."

May 1991 "Property Control Problems At DOE's Livermore Laboratory Continue"

"The laboratory's claim that most of the missing equipment has been found is inaccurate....only about 3 percent of the inventoried equipment, acquired at a cost of \$26.8 million, has been located. About 13 percent...is still missing."

July 1991 "DOE Original Classification Authority Has Been Improperly Delegated"

"...DOE has delegated original classification authority to over 50 contractor personnel....The misclassification of national security information could seriously impact and threaten U.S. national security interests....DOE cannot provide assurance that U.S. national security interests have been or are being adequately protected."

December 1991 "Safeguards and Security Weaknesses at DOE's Weapons Facilities"

"Despite the critical importance to national security of effective safeguards and security at DOE's weapons facilities, DOE security inspections have identified numerous weaknesses in this area...over 2,100 weaknesses were identified at 39 of DOE's important weapons-related facilities...The identified weaknesses cover a wide range of security activities, including poor performance by members of DOE's security force, poor accountability for quantities of nuclear materials, and the inability of personnel to locate documents containing classified information."

June 1992 "Weak Internal Controls Hamper Oversight Of DOE's Security Program"

"The lack of complete or readily available records at DOE headquarters prevented us from determining whether DOE's written policies and procedures for reviewing and approving exceptions have been followed...of the 312 exception requests on file...114 were missing such key records as the exception request letter or the Office of Safeguards and Security's response."

October 1992 "Safeguards and Security Planning at DOE Facilities Incomplete"

"As of September 1992, DOE had not completed safeguards and security plans for 15 of its 27 sensitive facilities. At the 12 facilities where plans were complete, the planning process often identified significant vulnerability to theft or sabotage."

November 1992 "Improving Correction of Security Deficiencies at DOE's Weapons Facilities"

"...DOE's review of contractors' plans to correct deficiencies is sometimes untimely, potentially resulting in prolonged security risks."

April 1999 "Key Factors Underlying Security Problems at DOE Facilities"

Statement Of Victor S. Rezendes, U.S. General Accounting Office

"...We found in 1988, and again in 1997, that foreign visitors are allowed into DOE's nuclear weapons design laboratories with few background checks and inadequate controls."

"In 1987, 1989 and 1991, we reported that foreign countries routinely obtain unclassified but sensitive information that could assist their nuclear weapons capability."

"Ineffective management of personnel security clearance programs has been a problem since the early 1980's."

"We reported in 1980 and again in 1991 that, at some facilities, DOE was not properly measuring, storing and verifying quantities of nuclear materials. Also, DOE was not able to track all nuclear material sent overseas for research and other purposes..."

China And U.S. Nuclear Secrets: Separating Fact From Fiction

The Clinton Administration Kept Congress Informed About Security At U.S. Nuclear Weapons Laboratories

Senator Bob Kerrey: "...I think they are trying to respond to a problem. I was notified -- now that it's been public -- I was notified in July of 1996.... We did respond in '97 and '98 with increased money for counterintelligence.... I think there's been a substantial response...."

Wolf Blitzer: "And as far as being fully briefed on this, and consulted, informed as the ranking Democrat on the Intelligence Committee, you have grave problems with the way the administration dealt with you."

Senator Kerrey: "Well, I don't -- I do not. I mean, they've been -- they've notified me on many occasions on lots of different things.... They had substantial notification of us...."

CNN Late Edition, March 21, 1999

The Department Of Energy Worked In Concert With The FBI In Its Investigation Of Wen Ho Lee And The FBI Is "Very Satisfied" With Energy's Counterintelligence Efforts

Tim Russert: "In September of 1997, Louis Freeh, head of the FBI, a very tough cop, said there was no longer any investigative reason that Wen Ho Lee should stay in his position, and he stayed there and he stayed there for a year and a half until you removed him...."

Energy Secretary Bill Richardson: "Tim, there's some inconsistencies in those statements. Louis Freeh has stated with the FBI that we acted in concert with the FBI, the Department of Energy, on running operations on this individual, trying to find whether he was spying. He was moved out of sensitive areas early on. There appears to be, in your questioning, that we haven't been acting in concert with the FBI. We have been. Especially right now. I terminated this individual not until after the FBI gave me the green light.... But we have worked very closely with the FBI. They have acted vigorously, effectively and I think Louis Freeh, with me, in this investigation, has been terrific."

Mr. Russert: "So the FBI did not recommend in 1997 that there was no investigative reason to keep Mr. Lee in his position?"

Secretary Richardson: "You'll have to ask the FBI, but I don't believe so. They have stated that we acted in concert throughout the investigation and in the processing of Wen Ho Lee as we moved on this issue."

NBC Meet The Press, March 21, 1999

China And U.S. Nuclear Secrets: Separating Fact From Fiction

Clinton Administration Kept Congress Informed About Security At U.S. War Weapons Laboratories

7, 1999

Senator Bob Kerrey: "...I think they are trying to respond to a problem. I was notified -- that it's been public -- I was notified in July of 1996.... We did respond in '97 and '98 with a lot of money for counterintelligence.... I think there's been a substantial response...."

icks

Wolf Blitzer: "And as far as being fully briefed on this, and consulted, informed as the top Democrat on the Intelligence Committee, you have grave problems with the way the administration dealt with you."

Senator Kerrey: "Well, I don't -- I do not. I mean, they've been -- they've notified me on a number of occasions on lots of different things.... They had substantial notification of us...."

cor

CNN Late Edition, March 21, 1999

Department Of Energy Worked In Concert With The FBI In Its Investigation Of Wen Ho Lee And The FBI Is "Very Satisfied" With Energy's Counterintelligence Efforts

et on
in
e
wa
l."

4, 1999

Tim Russert: "In September of 1997, Louis Freeh, head of the FBI, a very tough cop, here was no longer any investigative reason that Wen Ho Lee should stay in his position, he stayed there and he stayed there for a year and a half until you removed him...."

IS
INS.

Energy Secretary Bill Richardson: "Tim, there's some inconsistencies in those statements. Freeh has stated with the FBI that we acted in concert with the FBI, the Department of Energy, on running operations on this individual, trying to find whether he was spying. He was cleared out of sensitive areas early on. There appears to be, in your questioning, that we haven't acted in concert with the FBI. We have been. Especially right now. I terminated this individual not until after the FBI gave me the green light.... But we have worked very closely with the FBI. They have acted vigorously, effectively and I think Louis Freeh, with me, in this investigation, has been terrific."

no
y
'and

Mr. Russert: "So the FBI did not recommend in 1997 that there was no investigative reason to keep Mr. Lee in his position?"

4, 1999

Secretary Richardson: "You'll have to ask the FBI, but I don't believe so. They have stated that we acted in concert throughout the investigation and in the processing of Wen Ho Lee and we moved on this issue."

NBC Meet The Press, March 21, 1999

**Security At U.S. Nuclear Weapons Laboratories Is An Issue Affecting
Republican And Democratic Administrations. Government And News
Reports About Potential Leaks Go Back More Than A Decade.**

From The New York Times, 1990

"Chinese intelligence agents succeeded in stealing nuclear-weapons secrets from the Government's Lawrence Livermore National Laboratory in the 1980's, and the Federal Bureau of Investigation later conducted a long espionage inquiry into the theft, American intelligence experts said today....

Officials in Washington said the Chinese had sought an array of nuclear-weapons information from Livermore and other Government-financed weapons laboratories....

...another [official] said the Chinese apparently got most, if not all of the data they needed by exploiting lapses in routine security procedures....

The New York Times, November 22, 1990

From The Associated Press, 1990

"Information that helped China develop a neutron bomb was stolen from Lawrence Livermore National Laboratory through espionage, according to a published report....

George Carver, a former deputy director of the CIA, said publicly last month that the Chinese success was based on U.S. nuclear research.... 'In 1989...the Chinese blossomed forth with the neutron bomb, which was made from data stolen from U.S. research centers,' he said in a speech to Lawrence Livermore employees....

The General Accounting Office reported in 1988 that foreign intelligence agents posing as visiting scientists had gained access to Lawrence Livermore and America's other two nuclear weapons design laboratories."

The Associated Press, November 22, 1990

"... a General Accounting Office (GAO) report 10 years ago that warned the Reagan administration of 'major weaknesses' in the foreign visitors program at the nation's nuclear weapons laboratories, including suspected foreign agents from Russia, China and other 'sensitive' countries being able to make visits 'without prior DOE knowledge.'

The October 1988 GAO report followed an FBI investigation of alleged spying at the Lawrence Livermore National Laboratory in the early 1980's and numerous internal DOE studies critical of security.

Brent Scowcroft, President George Bush's national security adviser, said lab security 'was not an issue' during his time in office. He said he was unaware of the GAO report and was surprised to hear that stories were published about the alleged Chinese stealing of secrets about the neutron warhead at the labs.

Rep. Christopher Cox...said yesterday in reference to the early GAO report that security at the labs "is best understood as an endemic problem."...

The 1988 GAO report referred to a 1983 DOE study that concluded 'a significant amount of important technology may have been lost to potential adversaries through visits.' In addition, DOE's own vulnerability studies in 1984 and 1985 found that 'information on classified programs could be derived from...observing activities at these facilities.'

Although background checks were required for all visitors from communist countries, the study found that such checks were not done for 119 of 181 individuals sampled during 1987...."

The Washington Post, March 19, 1999

Director Freeh: "In terms of the overall counterintelligence deficiencies in the national laboratories, as I mentioned, Senator Glenn first highlighted this, at least in terms of our search, in 1988. He had hearings, he wrote a report, and there were a series of other reports....So the problem in terms of a problem has been around for a long time...."

House Appropriations Committee Hearing, March 17, 1999

Representative Dicks: "The most important thing [the American people] will learn is that for 20 years, starting in the '80's, we had a major counterintelligence failure at Los Alamos and at the other national labs that is now being corrected but will only be corrected if we stop playing the blame game and start working together to make sure that the resources are provided and the oversight is provided to implement that plan...."

NBC Meet The Press, March 14, 1999

00000