Collection:
Keyworth, George: Files
Folder Title:
National Security – Scientific Exchange (1 of 2)
Box: RAC Box 10

WITHDRAWAL SHEET

Ronald Reagan Library

Collection Name KEYWORTH, GEORGE A. II: FILES

Withdrawer KDB 6/8/2006

File Folder NATIONAL SECURITY - SCIENTIFIC EXCHANGE (1)

FOIA 2004-060/1 WANG, Z

Box Number ~~22~~ 10

ID	Doc Type	Document Description	No of Pages	Doc Date	Restrictions
25395	MEMO	WILLIAM ROOT TO STEVE BRYAN RE CONTROLLING TECHNOLOGY TRANSFERS AT SCIENTIFIC CONFERENCES (W/NOTATIONS)	3	9/10/1982	B1
		R 10/6/2011 F2004-060/1			

Freedom of Information Act - [5 U.S.C. 552(b)]

B-1 National security classified information [(b)(1) of the FOIA]
B-2 Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
B-3 Release would violate a Federal statute [(b)(3) of the FOIA]
B-4 Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
B-6 Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
B-7 Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
B-8 Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
B-9 Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

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

Natl. Security - Scientific Exchange

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release September 27, 1985

STATEMENT BY THE PRINCIPAL DEPUTY PRESS SECRETARY

President Reagan has issued guidance to the various agencies of the Federal Government which outlines procedures concerning the releasability of scientific, technical and engineering information generated as a result of federally funded fundamental research in universities, colleges and laboratories.

This policy addresses a widespread concern that efforts to reduce the flow of sensitive technologies to potential adversaries could restrain free and open exchange of fundamental scientific information. It is included in a directive to the heads of executive branch departments and agencies:

The new policy states that:

It is the policy of this Administration that, to the maximum extent possible, the products of fundamental research remain unrestricted. It is also the policy of this Administration that, where the national security requires control, the mechanism for control of information generated during federally funded fundamental research in science, technology and engineering at colleges, universities and laboratories is classification. Each federal government agency is responsible for: (a) determining whether classification is appropriate prior to the award of a research grant, contract, or cooperative agreement and, if so, controlling the research results through standard classification procedures; (b) periodically reviewing all research grants, contracts, or cooperative agreements for potential classification. No restrictions may be placed upon the conduct or reporting of federally funded fundamental research that has not received national security classification, except as provided in applicable U.S. statutes.

Our goal is to maintain the free and open exchange of unclassified research so necessary to a free society and an expanding economy.

# # #

Natl. Security - Scientific Exchange

Council of Scientific Society Presidents
1155 16th St., N.W., Washington, D.C. 20036 (202) 872-4452

Please reply to:

Dr. K. Florey
The Squibb Inst. for Medical Research
P. O. Box 191
New Brunswick, NJ 08903

(201) 545-9827

June 29, 1983

The Honorable Clement J. Zablocki, Chairman
Committee on Foreign Affairs
U.S. House of Representatives
Washington, D.C. 20515

Dear Congressman Zablocki:

The Council of Scientific Society Presidents has for some time followed with great interest and concern the issue of scientific communication and national security. In a resolution passed on December 2, 1982, the Council supported the recommendations of the Panel on Scientific Communication and National Security of the National Academy of Science, chaired by Dale R. Corson, and has communicated this resolution to Dr. George Keyworth.

We are, therefore, particularly gratified that an amendment to the Export Administration Act reaffirms the importance of protecting the ability of scientists and other scholars to freely communicate their research findings.

We would like to take this opportunity to express our deep appreciation.

Sincerely yours,

Klaus Florey
Chairman

KF/mb

Council of Scientific Society Presidents
1155 16th St., N.W., Washington, D.C. 20036 (202) 872-4452

Please reply to:

Dr. K. Florey
The Squibb Inst. for Medical Research
P. O. Box 191
New Brunswick, NJ 08903

(201) 545-9827

June 29, 1983

The Honorable Jake Garn, Chairman
Committee on Banking, Housing & Urban Affairs
United States Senate
Washington, D.C. 20510

Dear Senator Garn:

The Council of Scientific Society Presidents has for some time followed with great interest and concern the issue of scientific communication and national security. In a resolution passed on December 2, 1982, the Council supported the recommendations of the Panel on Scientific Communication and National Security of the National Academy of Science, chaired by Dale R. Corson, and has communicated this resolution to Dr. George Keyworth.

We are, therefore, particularly gratified that an amendment to the Export Administration Act reaffirms the importance of protecting the ability of scientists and other scholars to freely communicate their research findings.

We would like to take this opportunity to express our deep appreciation.

Sincerely yours,

Klaus Florey
Chairman

KF/mb

Natl. Security - Scientific Exchange

Council of Scientific Society Presidents

1155 16th St., N.W., Washington, D.C. 20036 (202) 872-4452

For RBF Signature 12.13.82 | Hewitt RBF

December 6, 1982

Please reply to:
Provost Robert L. Heller
515 Darland Administation Bldg.
University of Minnesota, Duluth
Duluth, Minnesota 55812

Dr. George A. Keyworth II
Office of Science & Technology Policy
360 Old Executive Office Building
17th & Pennsylvania Avenue, N. W.
Washington, D. C. 20500

Dear Dr. Keyworth:

Open and unrestricted communication is the lifeblood of science. On the other hand, there are legitimate reasons that national security may demand restrictions on the flow of such communication in certain areas. Recently problems have arisen in the reconciliation of these two principles. Therefore, a distinguished panel on scientific communication and national security under the chairmanship of Dr. Dale Corson has studied the problems in great detail and issued a report which was transmitted to Dr. Frank Press, the President of the National Academy of Science.

Members of the Council of Scientific Society Presidents are deeply concerned about this issue. At its meeting on December 2, 1982, the Council passed the following resolution:

> The Council supports the recommendations of the Panel contained in the report. It also supports the recommendation of George M. Low contained in his letter to Dr. Frank Press to "urge the establishment of a government task force to develop specific operating mechanism and guidelines in the spirit of the report. This task force should include a proportional number of experts from the university/science community." The Council stands ready to lend assistance in the promulgation of such operating mechanism and guidelines. The Council also urges that once such guidelines have been established, they should be administered to preserve the ideal of free scientific communication to the maximum possible extent.

Sincerely,

Robert L. Heller
Chairman

RLH:hm

cc: Dr. Frank Press, President, National Academy of Sciences
Dr. Dale R. Corson, President Emeritus, Cornell University
Dr. George M. Low, President, Rensselaer Polytechnic Institute

Natl. Security - Scientific Exchange

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF SCIENCE AND TECHNOLOGY POLICY
WASHINGTON, D.C. 20500

October 15, 1982

MEMORANDUM FOR JAY KEYWORTH
ED MCGAFFIGAN
VIC REIS

FROM: Denis J. Prager

SUBJECT: DOD Controls on Unclassified Research

The attached letter from the Associate Vice Chancellor for Research at the University of Illinois describes a situation in which contract language requiring Air Force approval of foreign nationals working on unclassified research forced the University of Illinois to decline an Air Force contract which it had won competitively.

I'm curious as to how this Air Force requirement strikes you three and what, if any, action you think we might take. Through discreet actions such as these, DOD can, in reality, impose restrictions inconsistent with Administration policy.

Attachment

University of Illinois at Urbana-Champaign

GRADUATE COLLEGE · 330 ADMINISTRATION BUILDING · URBANA, ILLINOIS 61801-3690 · (217) 333-0035

October 7, 1982

Dr. Denis J. Prager
Senior Policy Analyst
Human Resources and Social and
Economic Services
Office of Science and Technology Policy
Executive Office of the President
Old Executive Office Building, Room 356
Washington, D.C. 20500

Dear Denis:

I promised to send you some information on the Air Force contract which we had to decline because of language restricting participation of foreign nationals in unclassified research. Here are the particulars:

The particular instance arose in connection with a proposed contract between Wright Patterson Air Force Base and the University of Illinois at Urbana-Champaign. The proposed contract involved a mathematical analysis and evaluation of seven different mathematical approaches to reduce the time spent by a computer in transforming from polar coordinates to rectangular coordinates the data obtained from a synthetic aperature radar system. Such a transformation is necessary before a fast Fourier transform can be applied to the data and constitutes a serious burden on any computer attached to the radar system. At the end of the contract, a recommendation was to be made specifying the optimal mathematical approach.

The co-principal investigators were T. S. Huang, W. K. Jenkins, and D. C. Munson of the Coordinated Science Laboratory of the University of Illinois at Urbana-Champaign.

The history of the pertinent contract language was as follows. The draft of the contract which we initially received contained the following language:

> (xi) PCO Approval of Foreign Nationals
>
> The parties acknowledge that the technical data (see 22 Code of Federal Regulations Part 125) generated under this contract may be controlled by the International Traffic Arms Regulations (22 Code of Federal Regulations Part 121-128). Accordingly, the contractor agrees that it will obtain prior written approval from the Procuring Contracting Officer (PCO) before assigning any foreign national to perform work under this contract, or before granting access to foreign nationals to any technical data provided by the Government, or generated under this contract.

Wright Patterson Air Force Base proposed the following, after we had objected to the above language:

> 2. Employment of Foreign Nationals
>
> (a) Any foreign national excluding immigrant aliens proposed by the contractor for employment on this contract shall not be denied consideration solely because of country of origin.
>
> (b) Before a foreign national may be permitted to work on this contract, the contractor shall list in writing all contract data the foreign national will be required to have access to and shall submit this list to the Government for review to assure contractor compliance with national disclosure policy. The PCO and the Foreign Disclosure Authority and the contractor shall reach a mutual agreement regarding any changes in the list.
>
> (c) The foreign national shall not be permitted to start work on this contract nor have access to any contract data until agreement is reached on the list of data releasable to the foreign national.

In response to our request for removal of this language, they replied:

> 1. Confirming referenced telecon, your requirement of removal of the PCO Approval of Foreign Nationals clause from proposed contract F33615-82-C-1852 has been reviewed by our policy, foreign disclosure, and legal offices. It has been determined that the requirement for the removal of this clause cannot be complied with. As the PCO Approval of any foreign national employed on this contract is necessary as the final report will have a "Distribution-Limited" statement. It is noted that this clause does not prohibit the employment of foreign nationals. The clause merely directs you to seek approval with the understanding that access may not be granted. It is emphasized that we will be glad to consider any request for the employment of foreign nationals tendered by you under this clause.

This was followed by a request that we accept or reject the contract with this clause by the close of the next business day.

Our response was to refuse the contract with the following comments:

> We regret that we are unable to accept the above referenced proposed contract for unclassified research because it violates University of Illinois' policy that "no external agencies shall be entitled to exclude any individual employed by the University from participation in work which does not involve classified information." We are of the opinion further that, if security/control of data is a concern, your needs could be better matched to our own

by placing the work within the formal work of framework of classified research. By contrast, your requirement to include the "PCO Approval of Foreign Nationals" clause appears to generate a new, informal level of security of unclassified research which runs counter to the recent memo from Under Secretary of Defense, James P. Wade, Jr., which directed that unnecessary restrictions concerning the involvement of foreign students and faculty in unclassified research be avoided.

Please be assured that the University of Illinois is most interested in pursing the research endeavor set forth in the above referenced proposed contract with the hope that a resolution to the cited contractual difference can be resolved.

At the request of a staff member of the Association of American Universities, Dr. Leo Young of the DOD Office of Research and Technology investigated the problem and reported that since access to classified information was given to the principal investigators, the project officer at Wright Patterson Air Force Base could rule that these provisions concerning foreign nationals must remain in the contract without violating the Wade memo instructing DOD agencies to refrain from unnecessary restrictions of this nature.

Please let me know if you have need of any further details. I will be glad to supply them.

Sincerely,

Linda

Linda S. Wilson
Associate Vice Chancellor for Research
Associate Dean, The Graduate College

LSW:afr

cc: Harvey Stapleton
Theodore Brown
Jack Kamerer

Denis — Do I have your correct title?

Natl. Security - Scientific Exchange JK

need more information about sectors because, with structural shifts, like the contraction of the steel industry, going on thoughout the economy, industries don't move in the same way as they did in the past," says Sears & Roebuck economist John W. Skorburg.

BUSINESS LOAN DEMAND. Economists use the changes in the total of commercial and industrial loans plus commercial paper to predict interest rates. Heavy business borrowing puts upward pressure on rates, and vice-versa. Economists also use the loan demand numbers to forecast business inventories. But since companies now often roll over their short-term debt just to refinance their balance sheets, loan demand is less reliable as a gauge of borrowing to build stocks.

For all the care given to interpreting these indicators, economists have gotten into trouble by relying too heavily on instant analysis. Based on his analysis of the movement in the money supply and initial unemployment claims, Hyman in February claimed that the economy had already touched bottom, and that a recovery was under way. "Economists are getting a dirty name because we are trying to do too much too fast," concedes Ratacjzak.

Bad name or not, the financial markets have become hooked on instant analysis. Increasingly, they are reacting more strongly to forecasts of the indicators than to the actual numbers. "The market is discounting these indicators much more quickly than it used to," says Hunt. And discounting has created a twist in market reactions. Investors will react on the day the data is released only if the numbers are not what they expected.

November's elections may depend on what the day-to-day indicators show

Interpretations. Economists, for example, were forecasting that the money supply to be announced after the markets closed on Friday, Oct. 1 would be down by some $2 billion. Instead, it rose by $400 million. On Monday, stock prices fell and interest rates rose because the markets interpreted the higher-than-expected money number to mean that the Fed would have to tighten policy.

The market for instant analysis is likely to expand. With the economic outlook still uncertain, decision makers can ill afford to wait for quarterly or even monthly numbers. "The inventory-to-sales ratio numbers for September that we look at won't be released for another month and a half," says Albert G. Matamoros, chief economist at Armstrong World Industries Inc. "But by then I'm ready to start trimming my Christmas tree." ■

RESEARCH

An ominous shift to secrecy

Scientific research in the U. S. is headed toward tighter secrecy controls. Although free communication among researchers has long been the cornerstone of U. S. scientific and technological prowess, that same openness has unfortunately provided critical knowhow to American adversaries, both military and economic. Now the federal government is preparing to sacrifice some of that scientific freedom to keep U. S. technology from falling into the wrong hands.

University scientists were outraged last January when Admiral Bobby R. Inman, then deputy director of the Central Intelligence Agency, said that Washington planned to tighten controls over research unless the scientists helped it stanch the "hemorrhage of the country's technology" to the Soviet Union. A high-level study group has now conceded that some limits on unclassified but sensitive research may be necessary. "Recent trends have raised serious concerns that openness may harm U. S. security," says Frank Press, president of the National Academy of Sciences, which conducted the study.

Keeping the lid on this sensitive research, however, could not only damage the U. S. position in basic research, observers believe, but also hurt the competitive stature of U. S. industry. "Industry has a great deal of interaction with universities and professional societies," says Franklin A. Lindsay, chairman of the executive committee at Itek Corp. and a member of the National Academy panel. "If we bind our hands and feet in basic science at universities, the nation is going to suffer, and Itek's going to suffer. Basic research is the important part of the technology base which ought to be kept as free and open as possible."

Too easy access. The push for new controls stems from many Reagan Administration officials, who believe that the Soviets have too easy access to U. S. secrets. Their fears were reinforced late last year by an interagency intelligence study of technology leakage. The study found that too little attention had been paid—even by intelligence experts themselves—to Russian acquisition of scientific and technical data, manufacturing processes, and finished products. Of particular concern was computer and laser technology that could make major contributions to Moscow's military and space efforts.

While many laws and regulations already exist for controlling the export of arms and other military hardware, some Administration officials want to extend them to cover scientific and technical information, as well. These officials would limit the visits of foreign scientists, ban foreign students from research on such projects as very-high-speed electronic circuits, and curb presentation of unclassified scientific papers that could disclose critical technology.

Not surprisingly, the academic community panicked when Inman and others began suggesting such controls. It called for an urgent study of the problem by university and industry scientists. After seven months of work, including top-level government intelligence briefings on the Soviet threat, the group announced its findings on Sept. 30.

Things' vs. information. A quick reading of the report could give the impression that the universities were not part of the problem. The panel, headed by Dale R. Corson, president emeritus of Cornell University, reported no "concrete evidence" that campus research or unclassified scientific papers had contributed significantly to the leakage of important military knowledge to the Soviets. The panel also rejected the use of export laws and regulations to control information. Such laws, says Corson, were designed to control "things—packages and boxes that you could intercept," not scientific information.

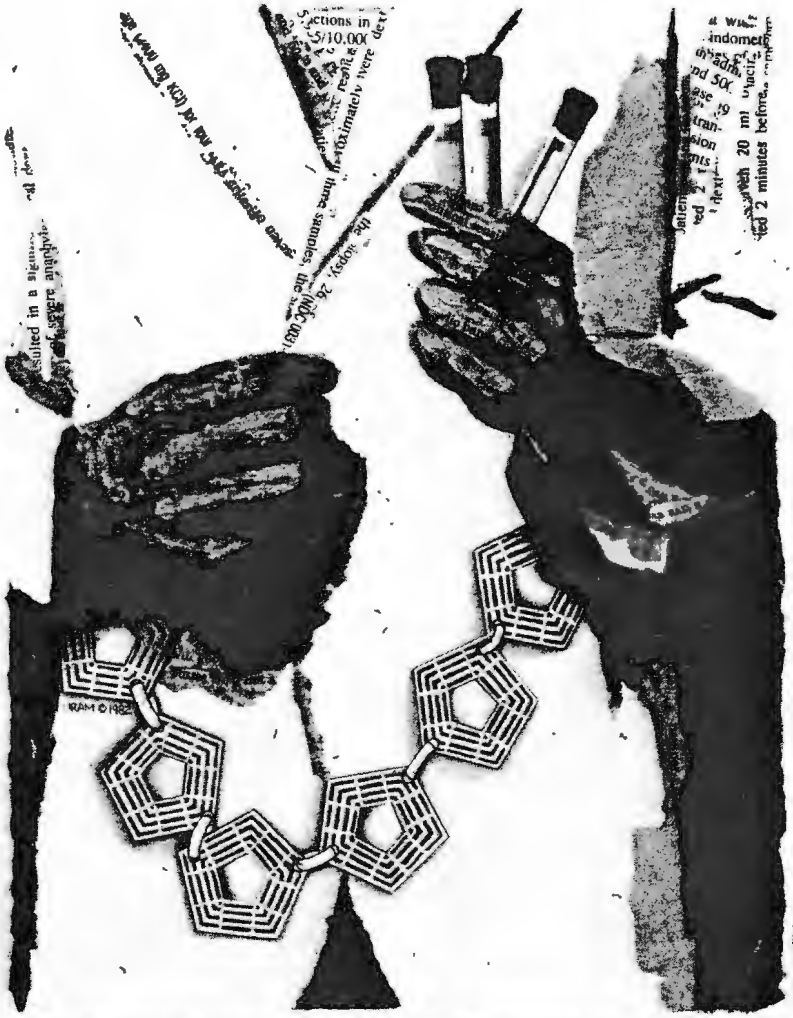
The trade-off is between open scientific communication and national security

The scientists did make some important concessions, however. They found "gray areas" between classified and unclassified research in which, they said, universities and industrial laboratories might need to accept curbs on open communications. While the panel members say they are determined to keep the flow of scientific information as free as possible, they recommended, surprisingly, that contracts or written agreements with the government may be necessary to deal with such sensitive areas of research. These agreements might include prior government review, although not veto power, over publication of research results. Since the government supports nearly all of this research, such a measure would give Washington a potent sanction over scientific publication.

In addition, the contracts could call for the exclusion of "nationals of designated foreign countries" from research studies, the scientists declared. They added that it would be "not inappropriate" if universities reported excluded foreign

nationals to the government when they tried to participate in "gray area" research. "Some universities," the scientists suggested in an apparent understatement, "will regard such reporting requests as objectionable."

Industry's role. The capitulation of the academics has heightened industry's concern. Indeed, industry has been something of a Johnny-come-lately to the whole debate. "Frankly, the sensitivity to this issue in the industrial community is lagging behind that of the scientific community—but it is growing," says Roland W. Schmitt, General Electric Co.'s senior vice-president for research and development. Now industry would like to see an examination of its role in technology leakage. Adds Schmitt: "I think the problem in industry deserves the same quality of thought and consideration given by the Corson panel."



"If we bind our hands in basic science, the nation is going to suffer."

Lauren Uram

Both industry and universities agree that discussions of the problem are just beginning. If further controls are inevitable, it is urgent that government, industry, and academia sit down and discuss all the issues, argues Lewis M. Branscomb, vice-president and chief scientist of International Business Machines Corp. "It's a terribly difficult assignment to regulate knowledge," he says, adding: "It is better to regulate less if you can't regulate intelligently."

The peril of regulating without clear guidelines was brought home to all in late August. Only two days before a San Diego meeting of the Society of Photo-Optical Instrumentation Engineers, the Defense Dept. prevailed on authors to withdraw some 170 of 626 unclassified technical papers from presentation. Even though Defense Secretary Caspar W. Weinberger approved the action, GE's Schmitt called it "a debacle." And William D. Carey, executive officer of the American Association for the Advancement of Science, said the Pentagon move leaves discussions of advanced but unclassified work "in a no-man's-land of confusion and disarray."

Semiconductor industry entrepreneur William B. Hugle finds the optical-meeting incident particularly ominous. If the same thing had happened a year earlier, he contends, he might not have even learned about the technology on which his new company, Insystems Inc., is based. It produces equipment to spot potential defects in semiconductor circuits, and at a 1981 meeting of the optics society, Hugle heard technical papers on Air Force-sponsored university research that described a better method than the one he had planned on using. "We scrapped everything we'd done and started over," he says. "If those papers, which had some defense implications, hadn't been allowed to be presented, our project wouldn't have gotten off the ground."

Pentagon split. Defense officials who initiated the withholding of the August papers are steadfast in believing that they safeguarded sensitive information. Yet the incident highlights a split within the Pentagon that is complicating the secrecy debate. Reagan appointees who monitor international trade policy have been far more alarmed over the suspected role of open research in the seepage of technical information than have other Reagan appointees who direct defense research. An industry leader calls this the battle between "lawyers and scientists," while the AAAS's Carey notes: "There is more than one Pentagon."

For example, it was the trade policy monitors who engineered the withdrawal of the optics papers. Deputy Assistant Defense Secretary Stephen D. Bryen, who directed the effort, is considered a hard-liner on the secrecy issue. But he agrees that differences in views among the intelligence agencies and the Defense, Commerce, and State Depts. have left academics and industry confused about government policies.

Whether or not a separate industry study is convened, both sides hope that the National Academy of Sciences study will spur development of a single, consistent government approach to protecting scientific information. Reporting the academy's findings at a press conference, Cornell's Corson complained that, as government tries to "reorient existing laws, policies, and programs [to halt]... unwanted technology transfer," its efforts have become "unavoidably fractionated." Academy President Press, a former White House science adviser, cited the "distrust... on all sides."

White House allies. With future policy in mind, the academy took the unusual step of briefing top government officials, including Defense's Weinberger, before it released its report. Some panelists were heartened that President Reagan's national security adviser, William P. Clark, promised to bring the report to the President's attention. In fact, some of them believe that so many agencies and laws are involved in the technology control effort that the White House must take the lead in forging a cohesive government policy. But the AAAS's Carey cautioned that "we are a very, very long way from a conclusive resolution."

Although the limits to scientific communication will undoubtedly be hotly debated for some time, the researchers clearly have already lost ground. And for many observers the issue now is to arrive at rules that are compatible with both scientific and security interests. Even though IBM's Branscomb is concerned about "barriers" to free scientific exchange, he says that it is time "to do what is doable," adding: "The answer lies in good old American pragmatism—a set of rules that you can write down on one piece of paper." ■

DEPARTMENT OF STATE

Washington, D.C. 20520

September 10, 1982

~~CONFIDENTIAL~~

MEMORANDUM

TO: Dr. Steve Bryen
Deputy Assistant Secretary for
International Economic, Trade and
Security Policy
Department of Defense

FROM: William A. Root
Director
Office of East-West Trade

SUBJECT: Controlling Technology Transfers at
Scientific Conferences

Copies for
1) RF/GAK
2) Dep P
3) VF
4) JM
5) BA
6) Cis Weiss
file meetings
conferences
return to FM

I understand that Defense is reviewing procedures concerning controlling the transfer of technology at international scientific conferences open to the public, such as the annual symposium of the International Society for Optical Engineering (SPIE) and the concurrently held International Congress on High Speed Photography and Photonics held in San Diego August 21 to 27.

I am sure you agree that timely reviews of papers to be presented by USG personnel or by USG contractors is desirable in order to avoid wholesale last-minute cancellations, which have a chilling effect on the availability at such conferences of scientific information from which USG personnel can benefit.

Perhaps some views based on first-hand observations at San Diego would be helpful. Neither authors nor SPIE's Board of Governors were clear in their own minds concerning the type of material that should be withheld. There was, of course, no doubt that classified information should not be divulged publicly. But there was considerable uncertainty as to what unclassified material should be judged ineligible for dissemination in the public domain.

There was much talk of withholding "sensitive" material. However, no clear definition of "sensitive" was available: "sensitive" is neither a security classification nor a test of whether dissemination requires

DECL: OADR

an export license. Concern was expressed that withholding information because of a subjective judgment that it was "sensitive" could lead to charges of First Amendment violations.

The conference organizers were puzzled by a communication from Commerce bringing to their attention requirements for an export license for the transfer of technology. As we understand it, the regulations are currently interpreted to presume that whatever a private individual is willing to divulge at an open conference is in the public domain and, therefore, does not require an export license. This presumption, however, provides no guidance as to what USG personnel or USG contractors should withhold from such a conference. Licenses are required for export to the USSR of unpublished data related to any industrial process. This requirement is not related to the sensitivity of the technology. USG personnel are unlikely to be privy to industrial process technology which requires a license. USG contractors might be privy to such information, but would be unlikely to voluntarily divulge it in such a setting. For example, SPIE advertised its conferences as open, with published proceedings to follow.

It, therefore, seems that security classifications are the clearest means to protect government-developed information that should not be disclosed at scientific conferences.

bcc: PM - Mr. Halper
NSC - Mr. McGaffigan
EB/TDC - Mr. Lamb
NSF - Ms. Greenstein
DOC - Mr. Skidmore
PM - Mr. Rennagel

National Security Scientific Exchange

JOEL DAVIS
Freelance Writing
902 NORTH QUINCE STREET • OLYMPIA, WASHINGTON 98506 • (206) 352-1307

RECEIVED
82 NOV 22 A10 : 33

TRACK 11.22.82 Jennings (BJ)

16 November 1982

OFFICE OF THE DIRECTOR

Dr. George A. Keyworth
Office of Science and Technology Policy
Executive Office Building
Washington, D.C. 20500

Dear Dr. Keyworth:

The 15 November 1982 Aviation Week & Space Technology (page 22) quotes you as saying the Administration is concerned about "uncontrolled dissemination of unclassified U.S. aeronautics data to foreign parties and our own weak performance in collecting and disseminating unclassified technical information from both domestic and foreign research."

I concur with the concern expressed in the second half of your statement ("our own weak performance..."). I am appalled by the implications in the first part of your statement.

The operative word, sir, is "unclassified." Would you suggest we adopt the methods of the Soviet KGB regarding the "dissemination of unclassfied...data"? I am sure you were as outraged as was I and other science writers at the secret-police-like tactics of the Defense Department at the recent SPIE symposium in San Diego.

You understand the legitimate need to keep classified data classified, and unclassified data totally available for the open exchange of knowledge that makes science possible and our country free. I urge you to work to persuade other members of the Administration that our strength lies not in secrecy, but in open dissemination of knowledge and ideas.

Sincerely,

Joel Davis
Member: AAAS/AWA/SPJ

JD/oc

THE DEPUTY SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301

[illegible] A10:40

12 NOV 1982

TRACK 11.15.82 PRAGER RBJ

[illegible]
DIRECTOR

Honorable G. A. Keyworth
Director
Office of Science and Technology Policy
Executive Office of the President
Old Executive Office Building
Washington, D. C. 20500

Dear Dr. Keyworth:

This is in response to your recent letter which announced the initiation of a study to assess the commercial and national security implications of the transfer of advanced biotechnologies and will confirm the telephone arrangements made for the first meeting.

This Department would be pleased to participate in your study efforts and agrees with your request for representation with one exception. Mr. Thomas R. Dashiell will represent the Office of the Under Secretary for Research and Engineering (OUSDRE) rather than Colonel Paul Try. Mr. Dashiell has extensive experience in the area of biotechnology as well as practical experience in the problem of technology transfer through participation on Department of Commerce working groups on the subject.

We believe that the assessment you are undertaking can have a significant impact on the national security posture since biotechnology has the potential to provide important advances in many areas of national defense interest.

Sincerely,

Frank C. Carlucci

Natl. Security - scientific exchange

NAE

NATIONAL RESEARCH COUNCIL
NAS
Routing Slip

IOM

PEWITT
TRACK
11.10.82
ABJ

FROM: Frank H. T. Rhodes, President Cornell University	DATED: 11/3/82
SUBJECT: Unanimous endorsement by the AAU Science and Research Committee to the NAS report "Scientific Communication and National Security".	
RECEIVED: 11/8/82	ACTION BY: PJ
ACTION COPY TO:	
INFORMATION COPIES TO: F. Press L. McCray D. Corson	
SUSPENSE DATE:	
REMARKS: cc members of Re Panel Weyrauch DeLauer Francis Low (MIT)	
White - Action Pink - File Copy	

CORNELL UNIVERSITY

FRANK H. T. RHODES
PRESIDENT

November 3, 1982

Dr. Frank Press
President
National Academy of Sciences
2101 Constitution Avenue
Washington, DC 20418

Dear Frank:

I am writing to inform you that the Science and Research Committee of the Association of American Universities has recently given its unanimous endorsement to the National Academy of Sciences Panel Report Scientific Communication and National Security. The Committee believes the document provides a balanced report which responds to a major national problem. It notes that, despite the fact that there is some leakage in technology transfer to potential adversaries, the contribution of universities to this leakage is minimal. It recognizes that it is appropriate to divide the products of university research into three areas: classified, open, and a so-called "gray" area, defined by meeting each of four criteria set out in the report.

While the AAU Committee on Science and Research recognizes there will be discussion over implementation of the Report, it concludes that the recommendations made by the panel for identifying and pursuing research in the gray areas, are constructive and appropriate, and the proposed restrictions not overly burdensome.

The Committee wishes to support in the strongest terms the conclusion that security by accomplishment is greatly superior to security by secrecy. It shares the conviction that openness is a vital factor in our scientific and technological achievement. It urges its representatives on the DOD/University Forum, who will be negotiating on the implementation of the report, to pay particular attention to this important principle.

The report of the Committee was received by the full meeting of the Presidents of the Association of American Universities.

I should, of course, add that the Association represents some 50 different universities, and that it may well be that there will be diverging viewpoints within the member institutions on the content of the report. I believe, however, that the unanimous endorsement by the AAU Science and Research Committee should be seen as a very positive response to an important and constructive report.

300 DAY HALL ITHACA, NEW YORK 14853 607-256-5201

I want to tell you how much I and many others appreciate the outstanding leadership that you yourself have provided in this important and sensitive area.

With kind regards,

Sincerely yours,

Frank

Frank H. T. Rhodes

File - Natl. Security Scientific Exchange
TRACK / mcbaffigan
10/18 / DH
RB7

Congress of the United States

JOINT ECONOMIC COMMITTEE

(CREATED PURSUANT TO SEC. 5(A) OF PUBLIC LAW 304, 79TH CONGRESS)

WASHINGTON, D.C. 20510

OCT 18 11 22 AM '82

October 15, 1982

The Honorable George Keyworth
Director
Office of Science and Policy
360 Old Executive Office Building
Washington, D.C. 20500

Dear Mr. Keyworth:

The Administration is to be commended for focusing attention on the problem of East-West technology transfers and U.S. security. I note with special interest the comments in the final communiques of the Western Economic Summits in Ottawa and Versailles and in the recent talks in Quebec that dealt with these issues. The Administration's new policy and its application merit the careful consideration of businessmen. A thorough and cogent statement of policy and precise methods of implementation would help guide businessmen as well as improve Congressional assessment of Administration actions. In my view, the ongoing controversies regarding U.S. policy in this area warrant the Joint Economic Committee's active attention. I feel it is very important to offer this opportunity for executive departments and Federal agencies to present their current views on relevant matters of East-West technology trade policy.

Would you and your staff provide us with some insights on the enclosed questions that will help us in our inquiry. We have asked the Congressional Research Service to organize a workshop on the subject in 1983 and to prepare a volume for Committee release.

This letter has been sent to other Secretaries with an expectation of some coordination prior to response. I would appreciate your comments on the above noted questions by the convening of the 98th Congress. Mr. Christopher Frenze of the Joint Economic Committee staff (226-2488) or Dr. John P. Hardt of the Congressional Research Service (287-8886) can provide you with technical advice and clarification of our needs. Please provide them with a contact in your agency.

Thank you for your cooperation on this project.

Sincerely,

Roger

Roger W. Jepsen
Vice Chairman

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF SCIENCE AND TECHNOLOGY POLICY
WASHINGTON, D.C. 20500

October 12, 1982

MEMORANDUM FOR JAY KEYWORTH

FROM: Denis J. Prager

SUBJECT: Study of Biotechnology Transfer

At your request, I have initiated a study of the commercial and national security implications of the transfer abroad of genetic science and technologies.

The major part of the work of this study will be carried out by an interagency working group comprising representatives of the Departments of Agriculture, Commerce, Defense, Health and Human Services, and State, and of the CIA, NSF, and NASA. We have asked Bill Walsh of DOS/OES to be Vice-Chairman and Executive Secretary of this working group. Bill has been quite active in this area and has an understanding of the Administration policy context in which the study is taking place.

Bill is currently developing a study charter, list of agency representatives, and a work plan for our approval. We are asking the working group to prepare, for submission to this office by March 31, a report assessing the need for government policies in this area and evaluating policy options. This report should form the basis for OSTP and/or NSC recommendations for specific Administration actions.

Attached for your signature are letters to Secretary Shultz and Mr. Walsh needed to release enough of Walsh's time to be sure the work of the interagency group is done well and on time.

Enclosures

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF SCIENCE AND TECHNOLOGY POLICY
WASHINGTON, D.C. 20500

September 13, 1982

MEMORANDUM FOR JAY KEYWORTH

FROM: EDWARD McGAFFIGAN

SUBJECT: Export Controls and Scientific Information

The attached paper has been prepared by Ruth Greenstein, Assistant General Counsel at NSF, for possible inclusion in the next Annual Science and Technology Report. It's an excellent overview of the issue of national security controls and scientific information. She properly criticizes the vagueness of current export controls and outlines the problems inherent in correcting this. She advocates greater use of contractual restrictions between the U.S. Government funding agencies and the performers of the R&D, since these can be made more specific and the rationale can be explained to the contractee.

Attachment

cc: Doug Pewitt
Bruce Abell
Ron Frankum
Vic Reis
John Marcum
Denny Prager

RG:DRAFT: 8/14/82

NATIONAL SECURITY CONTROLS AND SCIENTIFIC INFORMATION

Introduction

The United States today is in the midst of a debate over whether the Soviet threat to American national security requires strengthened controls on technology transfer in general and on the exchange of scientific information in specific. This paper focuses on a portion of that debate, the possible broadening of national security controls on scientific information (particularly research).

Advanced technology underpins the nation's military strategy and its economic strength. Our military strategy depends on maintaining a technological advantage over potential military adversaries; our trade position, heavily reliant on the export of goods and services involving sophisticated technology, depends on maintaining a technological advantage over current and potential commercial competitors. Both therefore depend on the continuing creation of new science and the transformation of that science into useful technology. Both also depend on denying that new science and technology to certain users and for certain purposes. There is thus a constant tension between creation and supression.

Laws and regulations imposing restrictions on the dissemination of scientific and technological information for national security objectives have existed for many years. Classification and restrictions on the export of technical data have been well-established features of American society since World War II. Such controls, however, were applied to a very narrow range of scientific information. Three

inter-related changes in the general environment have both spurred efforts to apply controls more broadly and made it more likely that such controls will seriously affect American science and technology.

First, as detente waned and Soviet efforts to acquire American technology by open or covert means became better known, and as commercial competition from Japan, Germany, and other industrialized nations increased, many Americans began to see technology export as an important cause of America's military and economic problems. Thus the control system shifted from a concentration on the export of specific goods or hardware to a concern for controlling the dissemination of technology or know-how.

Second, as control of information increased, some began to question the long-accepted premise that unclassified, non-proprietary research in general and university-based research in particular would not be controlled except in the most unusual circumstances. Although no one questions that most university research raises no national security concerns, many universities are now perceived as doing the kind of applied research once found only in commercial or governmental laboratories. Recent acceleration of industry/university cooperation in a number of fields, important to continued technological advance, contributes to this perception. If university research resembles other research, it may be controlled as other research. But once controls are applied to universities, they impinge on a new set of values -- those of academic openness and free discussion.

The third major change in the post war environment is the altered relationship between the United States and its allies, political

and military. In the early postwar period, the United States, undamaged by the war, had both an overwhelming commercial advantage and a parallel techological advantage resulting from the wartime effort within the United States and the inflow of talented scientists who had fled Hitler's Europe. These advantages, however, have eroded. Where once a unilateral American decision to withhold goods or technologies from the Soviet Union might have been effective, today the successful imposition of national security controls requires the cooperation of our military allies, principally through the Coordinating Committee (COCOM). Similarly, where three decades ago American science and technology were supreme and substantially self-sufficient, today American science, technology, and industry are dependent on the knowledge -- and the manpower -- of other nations.

The Nation's military and commercial competitive position will continue to be challenged in the years ahead. Concern about the loss of scientific and technical information is therefore also likely to persist. Such concern, however, does not lead to a single, obvious policy solution. The dissemination of technical information can be controlled in many ways. By what may simply be an historical accident, the current debate was largely triggered by the application of export controls to a scientific conference and much of the debate since has focused on export controls. There are, however, a number of other mechanisms that have or can be used with greater or lesser effectiveness to stem technology outflow. This paper reviews both export controls and those other mechanisms. First, however, it examines some of the specific reasons, beyond the

broad changes outlined above, why Government and scientific community are concerned and asks some fundamental questions about what technology needs to be controlled.

Reasons for Concern

As suggested above, the broad environmental changes do not explain why restrictions on scientific information have generated so much debate recently. Nor do events to date. The Soviet Union has acquired much advanced American technology, but almost all has come through normal commercial channels, diversion from legal sales, or espionage; only a minimal amount has come from normal scientific communication. Moreover, although there have been complaints about the application of the current laws in particular situations, most observers acknowledge that the existing control system has only rarely created serious problems for research or educational activities. Classification of scientific information occurs rarely. And while both the Arms Export Control Act (and its associated International Traffic in Arms Regulations) and the Export Administration Act (and its associated Export Administration Regulations) apply strict controls on exports of technical data to the Soviet Union, Eastern Europe, and the People's Republic of China, the licensing scheme leaves technology exchange with other nations largely unfettered.

The Government's current attention stems, in great measure, from a concern about the future. Many in the Government fear that the Soviets may in the future more consciously exploit the openness of the research environment to acquire advanced technology. They also worry that, even if very rare, improper dissemination of certain classes of state-of-the-art research could seriously damage the

nation's military position.

Concern in the scientific community, so far predominantly focused on export controls, has diverse roots. Many teachers and researchers have been dismayed to discover that the export rules apply to them; they did not previously understand that a potentially controlled "export" takes places when they discuss their research with foreign colleagues here or abroad, mail an unpublished paper to a foreign scientist, present a paper at a symposium with international participation, or hire foreign graduate students to work on an advanced research project. Recent increases in the number of foreign graduate students, faculty, and researchers on American campuses, of course means that the export rules apply more frequently. Many who have learned that the rules exist do not understand just how they apply. Moreover, sporadic enforcement of the export control laws during the past several years, recent use of the visa authority to impede scientific conferences and international exchanges, and clumsy efforts to limit foreign participation in federally-funded research suggest to some a dismal present.

Others are more concerned about the future than about the present. They see in current controls a sign of worse to come. Certain Government actions and inactions have stimulated this concern. This list includes last winter's well-publicized but often misinterpreted revision of the Executive Order on national security classification; the suggestion of the Deputy Director of the CIA that broad pre-publication clearance might be required; the announcement without any specifics of a proposed revision of the Export Administration Regulations (which set the ground rules for much technology transfer);

and continuing failure to publicly define the scope of the Defense Department's Militarily Critical Technologies List, which will be the core of the nation's control system in the years ahead. Unless reauthorized, the Export Administration Act expires in September 1983; reauthoriziation gives Congress an opportunity to shape the future, and no one knows how it will act.

Uncertainty about the present and the future begets worry. It also hampers rational discussion; lacking specifics, all interested parties talk in vague generalities and project divergent scenarios. Teachers and researchers in academia and industry seek assurance that the changes Government plans will not further hamper their normal activities. The Government can provide neither reassurance nor even a simple prediction of the likely impact of change until it answers some basic questions. In the meantime, the national debate generates heat and little light.

Fundamental Questions to be Answered

Export controls are currently the main focus of attention. To provide reassurance about them, the Government must address three fundamental questions: what destinations call for controls; what technologies will be controlled; and what forms of exchange require control.

(a) Geographic Scope of Controls. Current rules governing non-military exports to most destinations amount to almost no restrictions at all. Under the International Traffic in Arms Regulations (ITAR), military goods and directly associated technical data as well as all classified information to all foreign destinations are strictly controlled; exports to most Communist-controlled nations are

forbidden entirely. However, only a relatively small percentage of U.S. exports, and an even smaller percentage of exported scientific information, falls within the scope of these controls. Export of most U.S. goods and technical data is controlled instead under the Export Administration Regulations (EAR). Under these regulations, national security controls seriously restrict only exports to the Soviet Union, Eastern Europe (excluding Yugoslavia), the People's Republic of China, and a group of smaller nations (including Laos, North Korea, North Vietnam, Kampuchea, and Cuba). Goods and technology that are controlled for export to communist nations are also controlled to Free World destinations. However, the purpose of controls on Free World destinations generally is only to prevent transshipment to communist nations; it is not to prevent the original export.

The volume of exports to Europe, Japan, and Third World nations makes any requirement of Government approval of each wholly impractical. Imposing such a requirement would in practice ban most exports. Moreover, limitations on what could be shared with Western Europeans and others in the Free World would require a change in the nature of American society (including its campuses) that would be unacceptable to much of the population.

No such requirement for specific Government approval of all exports exists. The Export Administration Regulations provide several mechanisms that effectively exempt many transactions from the requirement of any specific governmental approval and many other transactions from the requirement of case-by-case governmental approval. All

published technical data and most unpublished scientific and educational data are covered by one of the General Licenses, and therefore require no specific Government approval. Technical data that do require specific Government approval (in the form of a Validated License) may be eligible for one or another of the "bulk" licenses (e.g., the Project or Distribution License), which are single licenses covering multiple transactions. General Licenses effectively exempt most fundamental scientific research -- and therefore most academic research -- from express Federal control. General Licenses together with bulk licenses provide similar freedom for most corporate exchanges of scientific research and technological applications.

The system then nominally controls almost everything, in practice requires formal licenses of much less, and actually prohibits the export of very little. This structure is not straightfoward. It is administratively costly. Many do not understand it. Therefore, the very existence of the present rules may discourage some -- particularly individual scientists, small universities, or small firms -- from engaging in otherwise desirable technology transfers or working in fields that appear likely to be controlled. Nevertheless, scientific exchange and technology transfer within the Free World are today virtually uncontrolled unless they involve military goods or data or classified information.

The critical question for the future is whether technology transfer within the Free World will remain so unrestricted. It is an important question for at least two reasons. First, the scientific and technological links among the Free World -- and particularly among the industrial -- nations are far stronger and far more central to

day-to-day scientific and commercial activities than technology transfers with most communist-controlled nations. For example, while over a third of the engineering doctorates awarded in this country in 1979 were to non-immigrant aliens, only __ were not Free World nationals. Similarly for industry, [some statistic showing overwhelming OECD nexus]. Second, it appears that Americans have by-and-large accepted the stringent controls on technology transfer to the communist world. The Free World is another matter. The imposition of meaningful controls on transfers among the Free World nations, many of whom are our military allies, would undermine the already shaky national consensus that national security controls are legitimate and sensible public policy. It might appear that national security controls were being invoked to allow the imposition of the functional equivalent of a protective tariff.

(b) Substantive Scope of Controls. Under the current rules, unpublished technical information may require Government export approval either if it is directly related to an item on the Commodity Control List or the Munitions List or, under Part 379 of the Export Administration Regulations, if it relates directly to any industrial process. All other published and unpublished technical data are either legally or practically uncontrolled.

The current scope of controls on technical data has been widely criticized principally on two counts. First, it is argued, much of only marginal national security importance is controlled and thus needlessly subjected to cumbersome and expensive bureaucratic procedures. Although a problem also for hardware, such overbreadth is particularly acute for technical data, because Part 379 excludes

from the most liberal General License much unpublished technical data relating to industrial processes regardless of the national security importance of the processes. And, although the Export Administration Act strongly discourages applying national security controls to any goods or technology that are widely available abroad and despite frequent efforts to pare the control lists, the lists remain long and complicated.

Second, as all agree, the current scope of controls is simply not well understood. This is in part because the technical data regulations -- and particularly Part 379 -- are so badly structured and drafted as to be incomprehensible to the average reader. More importantly, both the perception of overcontrol and the fact of incomprehensibility stem from a lack of a consensus about what should be controlled. The congressionally-mandated Militarily Critical Technologies List was supposed to determine the scope of controls. Following the recommendation of the 1976 Bucy Report that controls focus on technology and know-how rather than on hardware, the 1979 Export Administration Act instructed the Defense Department to develop a list of technologies whose export to "potential adversaries could increase their military capabilities to the detriment of U.S. national security." Efforts since to construct such a List reflect a continuing and unresolved tension between advocates of a very short list of patently critical technologies and advocates of a much longer list including most modern technologies that undergird any advanced industrialized economy. The obstacles to consensus include not only differing concepts of national security, but also the nature of many advanced dual-use (i.e., civilian and military)

technologies and difficulties in reducing general conceptual agreement into regulatory language.

Most major industries in the United States -- and probably all militarily significant industries -- use computer technology in all aspects of the life cycle of a product: definition of product requirements, development and design, production and operational support, and utilization. Computer-Aided Industrial Process Control (CAIPC) technology, even when developed for purely commercial uses, provides a strong mobilization base by permitting the rapid conversion of industrial capacity from civilian to military uses. The same is true of Computer-Aided Manufacture and Test (CAM/CAT) techniques. Both CAIPC and CAM/CAT illustrate the difficulty of drawing the line between controlled and uncontrolled. First, both techniques are strategically important, but both also have broad commercial application; much, if not most, of the research and development related to these technologies is being done by the private sector for its own use. Particularly because American manufacturing leadership may depend on sophisticated factory automation, efforts to control the dissemination either of the technology or of products embodying it would have immediate and important trade consequences.

Beyond that, the Government's own use of these technologies depends in good measure on their development by the commercial sector. And that development depends importantly on university-based fundamental research in a wide range of scientific fields (including dynamics, stress analysis, computer architecture, computational techniques, and microstructures); the lag between basic research and commercial application is likely to be very short. Restrictions that discourage

academia from working with industry in these areas will therefore have important national security as well as trade consequences.

Translating into regulatory language the limited consensus that does exist about what should be controlled has also been a problem. For example, although there is wide agreement that most fundamental research should not be controlled, defining "fundamental research" is difficult. The Export Administration Regulations speak of scientific and educational information not "related directly and significantly to design, production, or utilization in industrial processes." Executive Order 12356 on national security information speaks merely of "basic scientific research." This implied distinction between basic and applied research would be helpful were it not that whether a given research result is basic or applied depends both on the purpose of the research and the judgment of the observer. If publishing generic definitions of what is controlled runs into insurmountable definitional problems, publishing specific guidance runs head on into the "blueprint problem." If Government defines specifically the line between fundamental research that need not be controlled and other research that may require controls, that definition provides a great deal of information about American technological capabilities and the Government's strategic concerns. Publishing it might therefore give our adversaries a "blueprint" of those technologies of greatest importance to the United States.

A clear answer to the question of what technologies need to be controlled in the future is not going to arrive quickly.

(c) When does technology transfer take place? The third question is what exchanges of scientific information effectively transfer technology? Those that do not need not be controlled. Ordinary (though perhaps difficult) observation discovers whether a given piece of hardware has been transferred to an adversary. It is much harder to tell when technology has been transferred. Whether technology transfer takes place in a given situation depends on the nature of the information, the skill and training of the giver and the receiver, and the nature and duration of their interaction.

For some technical information, simple possession is enough. Steal the recipe and you should be able to produce a reasonable imitation of Coca Cola. Theft of blueprints so hardware can be produced abroad is generally not the principal national security concern today. (There are, of course, major exceptions -- particularly when dealing with military systems.) That kind of technological piracy will usually assure preservation of American lead time, precisely the objective of controls. The principal concern today is whether an adversary will be able to apply sophisticated scientific and technical principles and information to his own needs and then build further on them. American foreign aid programs have learned through hard experience that this kind of technology transfer is not easy to bring about. As the Bucy Report concluded several years ago, technology transfer does not occur casually or quickly. Effective transfer requires that the giver and the receiver actively interact with each other over a sustained period of time.

Despite wide agreement on this point, current export control regulations on technical data generally do not distinguish "exports"

that will transfer technology from those that will not. An hour's formal presentation of unpublished research findings to an audience that includes foreign scientists or a quick walk-through of a laboratory containing advanced computer equipment is as likely to fall within the scope of controls as an intensive training program. (The confusing provision in the Export Administration Regulations permitting free dissemination of unclassified information at "open conferences" may be an attempt to make such a distinction. Even if so, it deals with only one of the many kinds of contacts that are unlikely to transfer technology effectively.) As a result, licenses are theoretically required for many "exports" that all agree to be harmless. And once within the scope of controls, there are no clear and publicly known criteria to guide the Government's decision when to approve or disapprove a license.

In short then, there is still no national consensus how many technologies should be controlled; whether technologies that are predominantly civilian should be controlled; what kinds of research, if any, warrant controls and how the line between controlled and uncontrolled is to be drawn; and what kinds of exposure to American technology are sufficiently effective that restrictions are likely to be cost-effective.

Judging the Mechanisms of Control

These questions would be difficult to answer even if export controls were the only way to restrict scientific information. They are not. At least four other control tools have been used in the past and could be used more in the future: national security classification; stricter use of the Government's visa authorities to deny or set

conditions on the admission of foreigners; contractual restrictions for research performed with federal funding; and various forms of voluntary self-control.

Without agreement on what a mechanism should control, it is hard to decide what control mechanism to use. For example, mechanisms designed to deny the Soviets a mere handful of technologies may be grossly inappropriate if the policy is to deny a larger number of nations a broad range of technologies. On the other hand, these mechanisms have different characteristics and impose different costs on American society. It is difficult to know what to control without knowing the costs of controlling it, and that depends on the mechanism used. It may be useful, therefore, to analyze the merits and demerits of the mechanisms.

Many criteria are relevant. Four clusters, however, appear to be most important.

1. Effectiveness. Will the system accurately identify what needs to be controlled and will there be sufficient American and COCOM cooperation that it can be enforced?

2. Administrative Burden. Can the system be administered without imposing unacceptable administrative costs either on the U.S. Government or on the American population? Can the procedures be simplified and the uncertainty reduced?

3. Scientific/Technological Costs. Can a system be designed that avoids substantial slowing of scientific or technological progress -- whether by compartmentalizing research into controlled and uncontrolled areas, by further hindering industry/university cooperation, or by damaging the intellectual climate?

4. Political Values and Consensus. Can a system be designed and enforced that is generally accepted by the American population as a reasonable and legitimate response to a shared threat? Will industry and academia perceive the Government -- particularly the national security agencies and those charged with enforcement -- as an adversary or as a partner in a collaborative effort? Muting the current adversarial climate will require not only public understanding of the nature of the threat, but also public acceptance that the means adopted are lawful, predictable in their application and enforcement, and appropriate to the magnitude of the problem.

Clearly, these clusters are related. A system built on domestic political consensus is more likely to be effective in stemming technology outflow. A consensus is easier to build if the system is seen as effective, as administratively efficient, and as imposing the minimum possible cost on other social objectives. However, while all four clusters are important and need to be considered, this discussion emphasizes the effects on science and technology.

(a) Export Controls. Export controls are widely perceived to be ineffective in restricting the dissemination of important scientific information. They are too broadly and imprecisely defined to give Americans a clear understanding of proscribed conduct. Because of their complexity and breadth, administration is cumbersome, compliance is costly in dollars and time, and enforcement is difficult. These characteristics undermine their political acceptability. Questions about the constitutionality of using export controls to restrict the dissemination of information not directly related to some

commercial transaction further undermines that acceptability. On the other hand, because so much information is practically uncontrolled for most destinations, export controls to date have had little direct impact on progress in science and technology. Attempts to use export controls more extensively would probably make its impact closer to that of classification (discussed below) and thereby destroy this one saving grace.

(b) Classification. Since World War II, the Government has used its classification power to control certain kinds of scientific information. The advantages of classifying information are clear. Although classification requires defining what needs to be controlled on a case-by-case basis, the question of to whom is clear. Only those with a security clearance and a "need to know" may receive classified information. Denying information to almost everyone is an effective means of denying it to one's adversaries.

Perhaps because the limitations are so severe, the Government does not classify lightly; relatively little scientific information has been classified. As a result, although there are serious administrative costs to working on classified research (as well as some disputes about what is classified), those costs are imposed only on a small segment of the scientific community rather than on the population at large. The Government's self-control in classifying scientific information has also created an aura of legitimacy which itself facilitates compliance.

Classification's effectiveness in denying information to adversaries is bought at the price of denying it to non-adversaries -- scientific

colleagues, for example. Its effects on scientific and technological progress are therefore quite severe.

Classification divides the scientific community into those with clearance and a need to know and those without. As we learned from the experience of atomic energy, intellectual exchange between the two camps is limited. The normal processes of collegial criticism, of learning from the successes and failures of one's peers, of using research to train the next generation of scientists, are all impeded. Restrictions on publication make working in a classified field less attractive, so it may be difficult to recruit and retain people in the areas of greatest national security need. The lingering consequences of Vietnam mean the divisive effects of more extensive classification are likely to be even greater now than during the early Cold War period. Most major American research universities prohibit classified research on campus. Off-campus classified research is detached from mainstream university activities; student participation is minimal. These policies are not likely to change soon. Therefore, those attracted to academic life will likely avoid work in classified areas. With classified research thus largely confined to industry and Government laboratories, close collaboration between scientists in industry (who will do classified research) and those in academia (who will not) may be impeded. The result could be further separation of academic science from national security issues, from mission-related research, and from research of direct relevance to emerging industrial needs because most of the technologies of national security concern have commercial applications.

The simplicity, clarity, and precision of classification are its

great strengths. Atomic energy information may be "born classified," but in other areas the Government must affirmatively and unambiguously decide to classify information. Even in atomic energy, disputes over what is classified have been relatively manageable. These strengths are also weaknesses. Unless the Government classifies an entire broad field, like atomic energy, classification decisions are unending. Further, assuming the Government wants to classify information before it is generally disseminated, it must somehow shift some of the burden of identifying potentially classifiable information to the scientists who generate it. That would not be difficult for research performed in Government laboratories. Scientists there are likely to be aware of possible national security ramifications of their research and, like some industrial researchers, are more willing to accept publication and other restrictions as conditions of employment. As the controversy recently generated by Executive Order 12356 on national security information attests, shifting that burden will be much harder for private sector research. First, and probably most serious, is the problem of defining what may require classification. The term information "relating to the national security" has no obvious meaning, particularly for people not in daily contact with national security issues; all the much-criticized uncertainties of the current export control laws would re-emerge here. Second, people outside the Government and not working on Defense contracts do not expect their work to be classified and do not consider classification an occupational hazard. Prepublication Government review of as yet unclassified research, even when federally-funded, suggests censorship to many.

(c) Visa Controls. The Federal Government has broad powers to bar aliens from entering the United States or to set conditions on their stay. While the Government may legally bar an alien to avoid an undesirable technology loss, visas are rarely denied on that ground.

Intelligent use of the visa authority requires generalized answers to the questions of what technology needs to be controlled, to whom, and in what form. Without them, case-by-case review of all requests for non-immigrant visas would bring the entire process to a halt.

Denying a visa usually keeps an alien out of the United States. But it prevents technology transfer only if the visit was essential to an effective transfer. For someone who intended to come as a degree candidate or post-degree researcher, the denial probably does prevent transfer. For someone who would have come for a very short stay, for a symposium, or to hear a paper delivered that will soon be published in the professional literature, the denial probably does not (particularly if Americans may freely convey the same information at conferences and symposia abroad and there are no restrictions on domestic publication).

The private sector finds visa denials or restrictions attractive. The Government bears most of the administrative burden. In comparison, it has been suggested that under export control laws, universities are in some way responsible for ensuring that legally-admitted aliens are denied access to controlled but unclassified information. If so, universities must monitor the activities of their students, researchers, or visiting faculty and restrict the access of some merely on the basis of nationality. The alternative of using visa

authorities avoids conflict with strongly-held values.

Visas as a control mechanism have certain attractions for the Government as well. While broad criteria can (and should) be publicly stated, decisions on individual applications can be made by the State and Justice Departments behind closed doors in consultation with the national security agencies. The Government therefore does not have to fully explain why a particular visa was denied. Definitional and "blueprint" problems, linked to the publication of criteria sufficiently detailed to guide public behavior, need not arise.

Relatively small numbers of visa denials or restrictions, particularly if limited to nationals of countries that are proscribed under the export control laws, appear unlikely to have major consequences for science and technology (although there may be foreign policy problems).

Granting or denying aliens admission to this country is clearly an appropriate governmental function. If visa controls are exercised with restraint, they are unlikely to become a major source of contention. However, closed-door decisions influenced by the national security agencies may have an unhealthy bias toward over-control. In any event, visa authority cannot be the primary means of control; it is too easy for our technology to be transferred outside our borders. Consequently, visa denials are perhaps best viewed as a way of reducing the objectionable domestic effects of export controls.

(d) Contractual Restrictions on Federally-Funded Research. In early 1982, the Report of the Defense Science Board Task Force

on University Responsiveness to National Security Requirements suggested greater use of contractually-imposed restrictions to avoid some of the uncertainty and contentiousness of other means of control.* For example, a research agreement might limit or require approval of foreign participation or require pre-publication review of research results. Although recommending this now only for the Defense Department, the Report suggested that other federal agencies might also use contractual restrictions. Presumably, contractual restrictions applicable to industry/university collaborative research would bind both industry and the university.

Restrictive contract clauses are likely to effectively restrict dissemination of the particular information developed under contract. Researchers who value their continuing relationship with their funding agency should take these clauses seriously. However, if similar or related research is either not federally-funded or funded by an agency that does not impose these restrictions, similar information will be disseminated unless it is otherwise controlled. Sensitive information is likely to be otherwise controlled. Industry-funded research (including that on campus) promising clear, short-term commercial applications is usually subject to proprietary restrictions. If the firm seeks a patent, the Government can impose a patent secrecy order. Most other research, while not controlled, is unlikely to be sensitive on national security grounds.

Contractual restrictions impose only limited administrative burdens.

---

* A contract, for this purpose, includes any contractual instrument whether labeled a contract, grant, or cooperative agreement.

Instead of controlling entire fields, as the Atomic Energy Act does, or entire technologies, as export controls may with the Militarily Critical Technologies List, contractual restrictions can be tailored to the particular research project. Areas of concern can be identified quietly and explained to the researcher without risking a public "blueprint problem." Because contractual restrictions are likely to be drafted and monitored by research sponsors, there is reason to hope the restrictions would be reasonable. The effect these restrictions would have on science and technology depends on the way they are used. If they are applied frequently or with a heavy hand, their effects can approach those of classification. Individual scientists will have to decide whether to work in tightly controlled areas. Individual institutions will have to decide whether the conditions are compatible with their philosophy and objectives. If the universities but not industry decline to work on such terms, industry/university collaboration once again becomes more difficult.

The public is more likely to accept broader contractual restrictions than most other forms of restrictions. As with university decisions to accept restrictions to preserve patentability in industry-funded research, there is an aura of voluntarism. Because the conditions can be tailor-made, they are more likely to appear appropriate to the situation. Because the negotiations can be conducted privately, the Government is better positioned to explain why the information is sensitive. Because the contract must be signed <u>before</u> research is begun, restrictions are less likely to seem arbitrary and unpredictable than those imposed in mid-stream.

(e) <u>Voluntary Restraint</u>. The term is not consistently defined

and two uses are most common. Sometimes, it refers to arrangements, such as those in cryptography, by which researchers voluntarily submit their work to the Government for pre-publication review. These arrangements as yet have no legal basis; the NSA concluded that it lacked any ground for legal compulsion. At other times, it refers to the motivation for compliance with legally-imposed restrictions for reasons other than fear of penalties. This usage suggests that if the Government did a better job of explaining to American scientists what it was worried about and why, it could apply very tight controls (e.g., classification) on only the most critical technologies; alert researchers to other possible problem areas; and rely on their general patriotism to insure self-censorship or consultation when questions or problems arise.

Of course the Government should do a better job of communicating legitimate national security concerns to the American public (including the scientific community). But the communication-patriotism mechanism faces the now familiar difficulties of the "blueprint problem" and administrative burdens. Willing to submit to prepublication review, public spirited cryptographers asked the NSA to define its areas of direct concern; the NSA finally concluded that publication of such a list would be more damaging to the national security than publication of the research results. The Defense Department's difficulty in publishing an unclassified version of the Militarily Critical Technologies List suggests this same problem is a general one. If the Government cannot alert researchers to its specific concerns, it could alert them to broad concerns and then scan a huge quantity of voluntarily-submitted material. This may be possible

in a small, highly sensitive discipline like cryptography. But where the number of researchers is large and the security implications less compelling (or at least less obvious), this broad net approach would be slow, costly, and unlikely to lead to a high level of voluntary compliance. Patriotism works best when it is not asked to do too much.

Conclusions

This review suggests several conclusions. First, ordinary scientific communication accounts for a very small portion of undesired technology loss to the Soviet Union. Second, effective instruments for controlling the dissemination of scientific information impose great costs on progress in American science and technology (and thus on long-term national security). But even ineffective tools such as export controls may discourage scientists from working in areas subject to restriction, impose financial and administrative costs on science, and drive a wedge between the Government and important segments of the population. Indeed, mechanisms that are ineffective because of their broad but uncertain sweep may impose higher costs than effective mechanisms. And third, clear and narrow restrictions that put the definitional burden squarely on the Government's shoulders are more likely to be accepted as legitimate and appropriate Government policy than are broad restrictions that attempt to shift the task of identification to the scientific community.

It also appears likely that most scientific research of national security concern will be funded either by the Government or by industry. The dissemination of the results of research funded by the

Government can be controlled, if necessary, by contract. The dissemination of that funded by industry is likely to be restricted to the extent that the results can be quickly adapted into marketable form.

These observations and judgements have implications for policy. First, it would be both very difficult and socially disruptive to apply export controls more broadly to scientific research. Second, although classification is obviously an effective control mechanism, its costs to science and technology suggest that it cannot be used substantially more frequently without endangering the scientific endeavor that underpins our economic and military health. Third, selective use of visa denials when potential net technology loss is clearly threatened would appear to impose little scientific cost and would probably meet with substantial scientific approval. And fourth, contractual restrictions, although not without their dangers, are a reasonable approach. Because specifically-negotiated contract terms are more likely to be appropriate than generally-applicable export control regulations, compliance with federally-imposed contractual restrictions -- at least when imposed or reviewed by a national security agency -- should then relieve the research performer of further obligation under the broader export control laws and regulations.

o