What price security?

A National Academy panel evaluates trade-offs between dangers to national security that arise from technology transfers and threats to the openness of scientific communication that are caused by too much secrecy.

Dale Corson

"There is an overlap between technological information and national security which inevitably produces tension. This tension results from the scientist's desire for unconstrained research and publication on the one hand, and the Federal government's need to protect certain information from potential foreign adversaries who might use that information against this nation. Both are powerful forces. Thus, it should not be a surprise that finding a workable and just balance between them is quite difficult." So said Admiral Bobby R. Inman, then Deputy Director of the Central Intelligence Agency, in a speech at the 7 January 1982 meeting of the American Association for the Advancement of Science.

Dale Corson, a physicist and former president of Cornell University, led the National Academy panel.

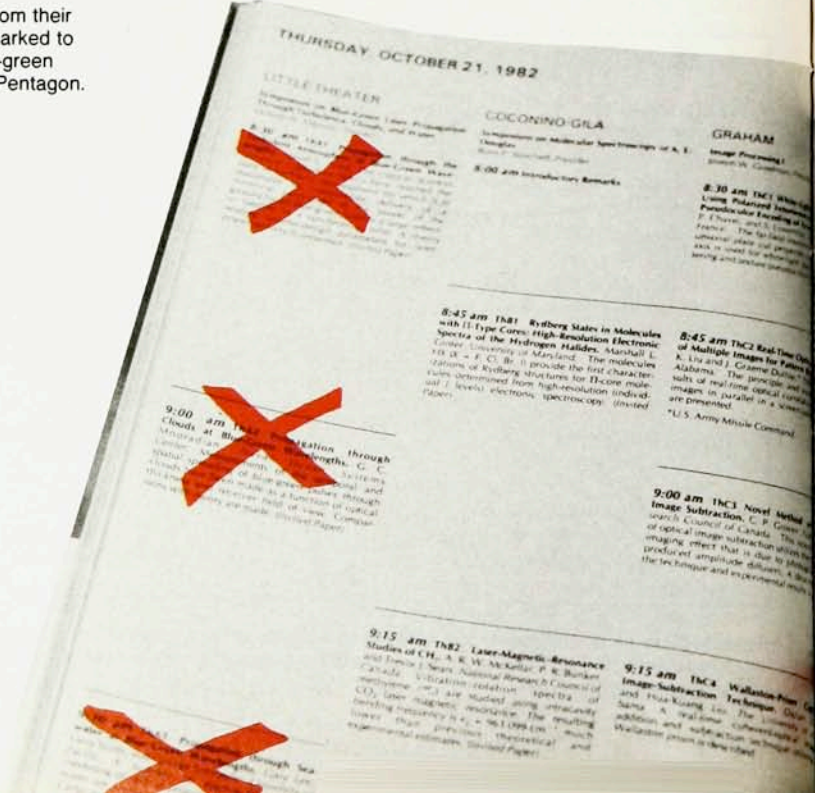
Inman's speech has since sparked widespread discussions aimed at delineating the differing needs of these two forces and suggesting ways to balance them. In fact, the tension about which Inman spoke, and the dilemma it poses, were the focus for a study recently completed under my chairmanship, entitled "Scientific Communication and National Security" (PHYSICS TODAY, November, page 69). The study, conducted under the auspices of the National Academies of Science and Engineering, considered the interests of both national security and scientific communication; attention focused on the control mechanisms now being used to restrict the flow of information and on the application of these controls; the committee also recommended specific improvements to the system.

The underlying conflict between the drive for security and the drive to open communication is not a new issue. Recently, however, concerns about national security as well as concerns about the free flow of information among scientists have increased. Why?

Recent events increase concerns

Although administrative concern over the technology-transfer problem increased during the last Administration, it has escalated sharply in the current one. This new sense of alarm has emerged, to some degree at least, from a change in perceptions. The US intelligence community, in fact, has identified four trends as significant.

- The US lead in at least some areas of military technology has diminished. The intelligence community sees this diminishing lead as a result of Soviet absorption of Western technology.
- Military systems are depending more and more on such high technol-



Optical Society program (right) from their November meeting in Tucson, is marked to indicate the invited papers on blue-green lasers that were withdrawn by the Pentagon.

ogies as state-of-the-art microelectronics, lasers and so forth.

▶ A steadily increasing share of these technologies has both military and nonmilitary applications; there is substantial difficulty in controlling leaks in non-military systems.

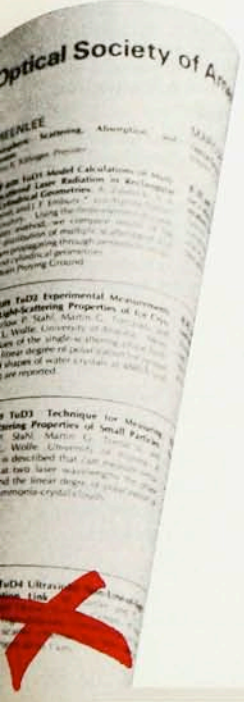
▶ Recent American foreign policy has multiplied the number of routes for leakage. Significant expansion of East/West trade in the 1970s, for example, has resulted in a variety of agreements that further encourage the transfer of technology.

Adding further to the alarm is a sense that the Soviet Union is making a concerted effort to acquire scientific and technical information. This view was expressed strongly by Lawrence J. Brady, Assistant Secretary of Commerce, in a speech before the intelligence community last March. He said:

> Operating out of embassies, consulates, and so-called 'business delegations,' KGB operatives have blanketed the developed capitalist countries with a network that operates like a gigantic vacuum cleaner, sucking up formulas, patents, blueprints and know-how with frightening precision. We believe these operations rank higher in priority even than the collection of military intelligence... This network seeks to exploit the "soft underbelly"—the individuals who, out of idealism or greed, fall victim to intelligence schemes; our traditions of an open press and unrestricted access to knowledge; and finally, the desire of academia to jealously preserve its prerogatives as a community of scholars unencumbered by government regulation. Certainly, these freedoms provide the underpinning of the American way of life. It is time, however, to ask what price we must pay if we are unable to protect our secrets?

The question of what price the Administration is willing to pay to keep information out of the hands of adversaries, particularly the Soviet Union, is perhaps the central concern of the scientific community. And now this concern has been heightened, primarily because of recent events and what they imply regarding further restrictions on scientific communication.

Notable among these events have been efforts to elicit the cooperation of universities in restricting the movements of visiting Soviet scientists. In addition, there have been repeated instances in which the Pentagon or the Department of State has sought to prevent scheduled papers from being presented at scientific conferences. One such incident that recently received wide publicity took place at the Society of Photo-optical Instrumentation Engineers' conference in San Diego in August: The Pentagon had nearly 150 papers withdrawn several days before the meeting. It now appears that many of these papers will, after all, receive clearance and be included in the published proceedings from this meeting. Similar incidents in which scheduled papers have been withdrawn from scientific meetings have taken place before and apparently will continue to take place, as the Optical Society of America discovered in November when several papers were withdrawn from its meeting in Tucson. These events stem, in part, from a confusion over how to apply the Federal regulations to the scientific and academic community.



Panel studies key issues

Our panel of 19 people included a former Under Secretary of Defense, a former Under Secretary of Energy, a former Director of the National Science Foundation, a former Presidential Science Advisor, four former members of the President's Science Advisory Committee, five members or former members of the National Science Board, six current or former university presidents, one former Director of the National Security Agency, four executives of high-technology industry, several present or former members of the Defense Science Board and two lawyers.

Our charge included four tasks:

▶ An examination of national-security issues and scientific communication interests within the context of certain fields of science and technology

▶ A review of the controls used in restricting scientific communication as well as identification of the issues arising from the use of the controls

▶ A rigorous evaluation of the critical issues concerning the application of controls, and

▶ The development of ways to make the system operate more effectively.

Although the panel's mission was to investigate the effects of restrictions on scientific communication in general, it found in reaching its recommendations that the university requires separate consideration within the context of the US research community. Restrictions on open communication have categorically different implications for universities than they do for industrial, governmental and other realms of the community; there are two main reasons for this distinction:

▶ Universities integrate research and education; thus, any adverse effects on research will also adversely effect the quality of education for the next generation of scientists and engineers.

▶ Unlike other research institutions, universities have never established broad controls on access to information to ensure that sensitive information be protected. Such restrictions, therefore, would present an unfamiliar and unwelcome challenge to the university.

Because the potential national security concerns are most likely to arise in work that is funded by the government, the panel's conclusions concentrate on government-supported research.

While much of our report applies to basic industrial research just as much as it applies to university research, there are important questions bearing on industry that we have not addressed at all. For example, how does one treat the problem of communication with a multinational company that has laboratories abroad and foreign subsidaries? For many, this may be the most important question of all; I regret I cannot help, for this question requires study by a new group constituted in a different way.

Due to both the current level of concern and the panel's limited time and resources, study focused on technology transfer to the USSR from the US.

To study these issues, the panel had

to begin by learning exactly what the nature of the technology-leakage problem was. We realized early on that we would have to operate on a classified basis; consequently we arranged for security clearance for all panel members at the secret level. In addition, six of our members, who held security clearanes at the highest level, arranged for intelligence briefings and discussions at the very highest security levels and reported back to the full panel at the secret level. They also produced a Secret report which is on file in the National Academy of Sciences. In addition, they produced an unclassified report, which is included in our panel report as an appendix, and which gives a clear picture of the technology-leakage problem.

The panel is unanimous in its conclusions and recommendations.

Major suggestions and conclusions

The evidence from all sources suggests that indeed there is a substantial and serious technology-transfer problem. There is a continuing flow of products, processes and ideas from the US and its allies to the Soviet Union, through both overt and covert means. Although much of this unwanted transfer has mattered little to US security, either because the US did not enjoy a monopoly on a particular technology or because the technology in question had little or no military significance, a substantial portion of the transfer has been damaging to national security (See the table for some evidence presented by the Central Intelligence Agency). These damaging transfers have taken place through the legal as well as illegal sale of products, through transfers via third countries and through a highly organized espionage operation.

Although a good deal of information has been transfered through open scientific communication, the panel concludes that, in comparison with other channels of technology transfer, open scientific communication involving the research community does not threaten our near-term military position. Given both this conclusion and our concern for finding an approach that will maintain the vitality of our universities and their roles in education and research, while at the same time protecting the security of our advanced technology, how should we proceed?

The panel believes that scientific research and technological development are best nurtured in an environment where such efforts are dispersed but interdependent. Openness and a free flow of information are essential aspects of such an environment. The technological leadership that the US enjoys is based in no small part on a scientific foundation whose vitality in turn depends on effective communication among scientists, and between scientists and engineers; the short-term security achieved by restricting the flow of information is purchased at a price.

After weighing the alternatives, the panel concludes that the best way to ensure long-term national security lies in a strategy of "security by accomplishment," and that an essential ingredient of technological accomplishment is open and free scientific communication. Such a policy involves risk, because new scientific findings will inevitably be conveyed to US adversaries. Nonetheless, the panel believes the risk is acceptable because American industrial and military institutions are able to develop new technology swiftly enough to give the US a continuing advantage over its military adversaries.

Against this general background, the panel comes to three specific conclusions:

▶ The vast majority of university research programs, whether basic or applied, should be subject to no limitations on access or communications.

▶ Where specific information has direct military relevance and must perforce be kept secret, it should be classified strictly and guarded carefully. The decision to accept or reject classified research projects, or to establish off-campus classified facilities, is a matter to be decided by individual universities.

▶ There are a few gray areas of research that are sensitive from a security standpoint, but where classification is not appropriate. These areas are at the ill-defined boundary between applications and basic research and are characteristic of fields where the time from discovery to application is short. (At present, a portion of the field of microelectronics is the most visible of these technologies.)

While it is impossible to specify these gray areas with precision, there are some broad criteria that help to define the few areas in question. The panel recommends that *no* restrictions of any kind that limit access or communication should be applied to any area of university research, basic or applied, unless it involves technology meeting all of the following four criteria:

▶ The technology is developing rapidly and the time from basic science to application is short; and

▶ The technology has identifiable direct military applications, or is dual-use, and involves process- or production-related techniques; and

▶ Transfer of the technology would give the USSR a significant near-term

Acquisitions from the West affecting Soviet military technology

Key technology area	Notable success
Computers	Purchases and acquisitions of complete systems designs, concepts, hardware and software, including a wide variety of Western general purpose computers and minicomputers, for military applications.
Microelectronics	Complete industrial processes and semiconductor manufacturing equipment capable of meeting all Soviet military requirements, if acquisitions were combined.
Signal Processing	Acquisitions of processing equipment and know-how.
Manufacturing	Acquisitions of automated and precision manufacturing equipment for electronics, materials, and optical and future laser weapons technology; acquisition of information on manufacturing technology related to weapons, ammunition, and aircraft parts including turbine blades, computers, and electronic components; acquisition of machine tools for cutting large gears for ship propulsion systems.
Communications	Acquisition of low-power, low-noise, high-sensitivity receivers.
Lasers	Acquisition of optical, pulsed power source, and other laser-related components, including special optical mirrors and mirror technology suitable for future laser weapons.
Guidance and Navigation	Acquisitions of marine and other navigation receivers, advanced inertial-guidance components, including miniature and laser gyros; acquisitions of missile guidance subsystems; acquisitions of precision machinery for ball-bearing production for missile and other applications; acquisition of missile test-range instrumentation systems and documentation and precision cinetheodolites for collecting data critical to postflight ballistic-missile analysis.
Structural Materials	Purchases and acquisitions of Western titanium alloys, welding equipment, and furnaces for producing titanium plate of large size applicable to submarine construction.
Propulsion	Missile technology; some ground-propulsion technology (diesels, turbines, and rotaries); purchases and acquisitions of advanced jet-engine fabrication technology and jet-engine design information.
Acoustical Sensors	Acquisitions of underwater navigation and direction-finding equipment.
Electro-optical Sensors	Acquisition of information on satellite technology, laser range finders, and underwater low-light-level television cameras and systems for remote operation.
Radars	Acquisitions and exploitations of air defense radars and antenna designs for missile systems.

Table adapted from a Central Intelligence Agency report entitled "Soviet Acquisition of Western Technology," April 1982.

0031-9228 / 83 / 0200 42-05 / $01.00

military advantage; and

▶ Either the US is the only source of information about the technology, or other friendly nations that could also be the source have control systems at least as secure as ours.

The panel recommends that in the limited number of instances in which all of the above criteria are met, but where classification is unwarranted, the values of open science can be preserved and the needs of government can be met by written agreements or contracts no more restrictive than the following:

▶ Prohibition of direct participation in government-supported research projects by nationals of designated foreign countries but with no attempt to limit physical access to university space or facilities or to limit enrollment in any classroom course or study. The danger to national security lies in the immersion of a suspect visitor in a research program over an extended period, not in casual observation of equipment or research data.

▶ Submission of stipulated manuscripts simultaneously to the publisher and to the Federal agency contract officer, with the contract officer having 60 days to seek modifications in the manuscript if he so wishes.

The review period is not intended to give the government the power to order changes. The right and freedom to publish remain with the university as they do with all unclassified research. The government nonetheless is a powerful negotiator in these discussions; it has the ultimate power to classify the research or to cancel the contract.

Knottier problems

The panel recognized the difficulty of limiting the access of foreign visitors on campuses to sensitive information, particularly when universities typically have people who are not working on federally-funded projects but who have free access to the laboratories and all that goes on within the university.

Let me simplify the problem by suggesting what might happen in a specific case. Visitors come to universities with restictions on their visas. Such restrictions may include travel restrictions, restrictions on what they can work on, and currently there might also be restrictions on what they can see. The contract officer occasionally checks up on the visitor and he also asks the university to report on what these particular visitors are up to. Certainly, according to our recommendations, the university would be alerted to the problem and notified that the visitors should not be supported with project funds over an extended period of time.

In the case of the similar research laboratory next door, performing non-government-funded research, we suggested that it would not be inappropriate for the university to respond affirmatively to requests from government agencies for information about possible attempts by the visitors to gain support to work with the nongovernment-funded project over an extended period. We reasoned that if the researchers did obtain that type of support, in doing so they would be presumably violating the terms of their visas. Thus we think it's appropriate for the university to respond affirmatively if asked, when those visa restrictions are being violated. Such requests, however, should not require surveillance or monitoring of foreign nationals by the universities.

It is important for the welfare of the country that universities' educational and research programs remain vital. The procedures recommended by the panel for dealing with the gray areas of research are intended to protect university interests, and at the same time to be responsive to the government's requirements.

The panel believes that the provisions of Export Administration Regulations and International Traffic in Arms Regulations should not be invoked to deal with these gray areas in government-funded university research. Rather, the appropriate procedure should be incorporated in research contracts or other written agreements in those rare cases where some measure of control is required. Furthermore, the panel believes that universities and industrial research laboratories should be treated in exactly the same way insofar as EAR and ITAR are concerned.

Writing the contract ahead of time poses two problems. The first is that one never knows what is going to happen; perhaps something will come up that was not anticipated in the contract. The second is that Federal contracting officers may act overzealously in protecting themselves by writing in restrictions that are unnecessary. Both are real concerns. To address the first problem—not knowing what's going to come up—we'd like to have the rules clearly understood ahead of time, insofar as they can be, so that everybody knows what the rules are and can play by the same rules. When cases come up where it is necessary to elaborate, we believe that constructive discussion can take place and problems can usually be resolved if there exists an atmosphere of good communication.

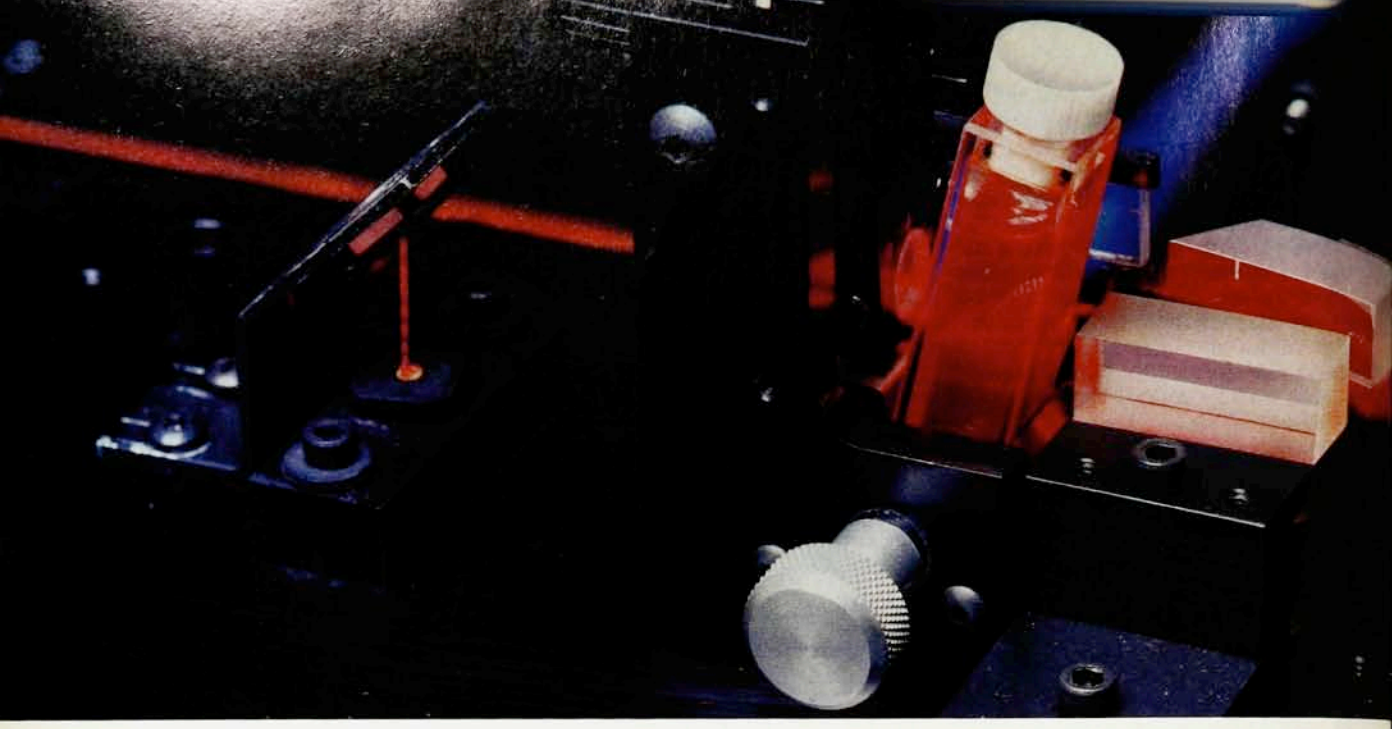
As an example of such a resolution, I can cite the situation that began several years ago in the field of cryptography. There were several instances; one in particular occurred in about 1978. A young researcher at the University of Wisconsin in Milwaukee applied for a patent on a cryptographic invention he had made. He didn't hear from the Patent Office for a long time. Eventually he received a post card as the only response to the application—a post card saying that his research program had been classified Secret and that he was not to talk to anybody about it. This action was authorized under the Invention Secrecy Act.

Admiral Inman played a major role in resolving that issue and reducing a tense situation to one that is now handled on a voluntary basis. The American Council on Education also played a lead role by convening a study group on the cryptography problem, in which the mathematicians participated. I also participated in the very first discussion of that problem at the American Council on Education, where I first met Inman. As a result of these discussions, people working in cryptography now submit their papers to the National Security Agency for comment; simultaneously they submit their papers to the publisher. Some 50 papers have been submitted under this voluntary arrangement. I think changes or suggested changes have been proposed by NSA in a couple of cases, but I have not heard of any great dissatisfaction. I also believe that there are some people working in the field who have declined to cooperate and are going ahead on their own. We spoke both with the National Security people and with people from universities with researchers in the field, and all of them expressed satisfaction with the current system. This is an example of what can happen when people get together and talk about the problem.

The panel believes, however, that one cannot extend this particular system to other research. Cryptography is a very narrow field in which everybody working in it knows everybody else working in it, and the focus of the research is limited and generally well-defined. This is not true for most other fields of research.

The second problem—the overzealous contract officer writing in unnecessary restrictions—is harder to deal with. I suspect that this problem is part of what happened at the San Diego SPIE Conference in August. In that instance, however, it wasn't the contract officer who was overzealous, but rather it was somebody in the Pentagon; I don't know how to protect against Pentagon intervention.

The Defense Department supports a significant amount of first-rate basic research, their so-called 6.1 research. Traditionally, research supported by 6.1 funding is unclassified, unrestricted, and free for publication. I suspect that now there is a move to restrict 6.1 supported research in various ways,



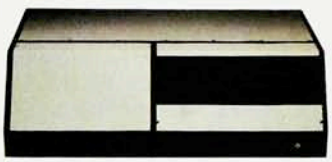
FINALLY, A MICROPROCESSOR CONTROLLED TUNABLE DYE LASER

The *new* Model 2100 Dyescan™ Tunable Dye Laser from EG&G Princeton Applied Research Corporation is a precision optical source designed specifically for spectroscopic applications. The system has been engineered for outstanding performance and ease of operation.

The dye laser output provides pulses of 1 nanosecond duration and 25 kilowatts of peak power with a linewidth of .04 nanometers. Repetition rates up to 100 pps are possible.

All laser operations are directed through the front panel keyboard and controlled by the microprocessor. The Model 2100 Dyescan is the *only* system capable of accurate and rapid optogalvanic wavelength self-calibration. Scan rates and limits within the 360 to 800 nanometer tuning range can be interchanged between wavelength and frequency units. Dye laser output power is continously monitored.

The nitrogen pump laser, dye laser, scan mechanism, and microprocessor controller have been completely integrated into a *single unit* which occupies only 0.5 m^2 of bench space. The system requires only standard electrical power and nitrogen gas for operation. No external coolant, pump, or vacuum equipment is necessary. Dye solutions are contained in standard, low volume cuvettes which may be interchanged in seconds.



SPECIFICATIONS	
Rep Rate	Up to 100 pps
Pulse Width	1 ns
Linewidth	.04 nm
Peak Power	25 kW
Tuning Range	360 to 800 nm

You owe it to yourself to find out more about our new laser. Write or call today for complete specifications and your copy of our Dyescan brochure: EG&G PRINCETON APPLIED RESEARCH, P. O. Box 2565, Princeton, NJ 08540, USA; (609) 452-2111.

EG&G PRINCETON APPLIED RESEARCH

579

See us March 7–12 at the Pittsburgh Conference, Booths 112–119
APS SHOW-BOOTH #45, 46

Circle number 17 on Reader Service Card

and there are many contract officers who are writing individual contracts for this research. Consider, for example, a situation in which somebody in the 6.1 office in the Defense Advanced Research Project Agency decides to support a certain program but he personally doesn't write the contract. Somebody at Wright-Patterson Air Development Center writes the contract. The person who writes the contract is eager not to get in any trouble, so he writes restrictions in. I don't know how to deal with that problem, except by starting at the highest level, setting major policy issues and establishing educational programs for contract officers. I am glad that the Office of Science and Technology Policy is now interested in this kind of problem.

Although these are major problems, and we recognize them, the panel felt that if we could write the agreements ahead of time, so that everybody knew the rules, we would have gained something.

The panel has studied the control system now in effect, and the report has some substantial discussion of the system and its problems. The panel's suggestions apply equally to industrial and university research. The current system is undergoing rapid change. Because the perceived nature of the technology leak problem has shifted only recently, government control mechanisms themselves are still being adjusted to meet the new perceptions.

In a fundamental sense, government is still in the early stages of the learning process as it reorients existing laws, policies and programs—designed for other purposes—to achieve a new objective, the dimensions of which are not yet fully determined. The adjustment is particularly difficult because the current effort to understand and control unwanted technology transfer is unavoidably fractionated within the Federal establishment. Four intelligence agencies—the FBI, the CIA, the Defense Intelligence Agency and the National Security Agency—share the job of gathering intelligence on the nature, extent and significance of unwanted transfers.

Major regulatory authority is also split among three separate offices: the Department of Commerce's EAR administrators, the Department of State's ITAR administrators, and the Department of State's Visa Processing Office. These offices depend heavily on outside units in the defense and intelligence communities for advice as they reach their judgments.

Similarly diffuse is the government's authority for classifying information and for monitoring results from the research and development that it funds. Regulatory enforcement shows similar diversity and includes yet another agency, the Department of Treasury's Customs Service. The panel discovered, not surprisingly, that few people inside or outside the government truly understand the government's technology-transfer control effort.

The panel believes that there is much room for improvement in targeting the government's efforts to prevent unwanted technology transfer. Priorities must be set and communicated. The panel believes that the government should concentrate on the most feasible forms of control and should avoid regulations that impose compliance burdens without significantly affecting leakage. The government should concentrate its resources more systematically on those technologies that are of greatest relevance to near-term Soviet military strength.

Finally, the panel addressed problems of inadequate staffing in agencies that deal with control measures, as well as problems of inadequate communication between the research community and the Federal agencies. The panel also identified areas where the research community might help the government assess the nature of the technology-transfer problem more reliably.

In assessing the current policies and procedures, we heard the word "confusion" from just about everybody we spoke to about both the ITAR and EAR.

Let me give you an example of the complexity of the system. In the Export Administration Act of 1979, an act which has been revised regularly and is the underlying legislation for EAR, it was specified that the Commodity Control List should be based on something called the Militarily Critical Technologies List. The Commodity Control List is the basis for licensing exports and the Militarily Critical Technologies List is now undergoing its second revision. The third version of this list is going to be issued some time in the immediate future. The second version was a 700-page book, all of which is classified Secret. If one wants to take this to its logical end, it means that the people who are going to be subject to heavy fines through the implementation of these regulations will not be able know what it is that the violation is based on. The regulations are administered somewhat more intelligently than this sounds, but nonetheless individual parts of the Commodity Control List are classified individually. For example, some are Confidential, some are Secret and some are Unclassified. Regardless of classification, all are subject to export restrictions determined by EAR. Among the unclassified technologies are such things as high-vacuum technology, or manufacturing techniques for the mass production of ultra-high frequency generators, and techniques for making certain kinds of magnets which industrial people are making every day of the week.

The list has been developed by dedicated people who have taken a military system apart piece by piece to see what went into it; those people have taken their work seriously and they've done an excellent job of finding what underlies every military system that exists.

Due to the comprehensiveness of this list and its classification, however, there seems to be no way to start from that list and arrive at a straightforward and clear definition of what it is that the regulations are going to apply to. Thus one of our recommendations is to streamline the MCTL. Our general suggestion was to build high walls around narrow areas that are clearly defined, with priorities established in words that everybody can understand. I don't have any great hope, however, that tomorrow's mail will bring such a list to my desk. □