REMARKS OF THE ATTORNEY GENERAL
PROTECTING AMERICAN TECHNOLOGY
COMMONWEALTH CLUB OF SAN FRANCISCO
SAN FRANCISCO, CALIFORNIA
DECEMBER 21, 1982

It is always a pleasure to come home to California. It is an even greater pleasure to come home to address so influential a group on a subject of such great importance.

You undoubtedly have heard the old story about two dedicated communists who were extolling the merits of their system. "Comrade," said the one, "Isn't it a glorious experience to live in a land in which we benefit from the privilege of sharing what we have with one another?"

"Yes," said the other, "From each according to his ability; to each according to his need."

"And if you had two eight-cylinder cars, you'd gladly give one to me?" asked the first communist.

"That's right!" said the other.

"And if you had two shirts, you'd give me one?"

"Well, no, comrade!" said the second communist.

"Why not?" asked his friend.

"Because, comrade, I actually have two shirts!"

The same Soviet attitude toward sharing -- sharing in what belongs to others -- seems to dominate their international relations as well. Where American technology is concerned, the Soviets seem especially to believe in the maxim: "From each according to his technological ability; to each according to his technological need." The Soviet's need for technology is inexhaustible. Since the beginning of its experiment in terror, the government of the Soviet Union has coveted American know-how. And in recent years, as their own technological shortcomings have become apparent, they have proven themselves exceedingly adept at stealing what they covet.

As the Assistant Director of Scientific Intelligence at the Defense Intelligence Agency has testified to the Senate:

> "...the U.S. R & D establishment is viewed by the Soviets as a Mother Lode of important and frequently openly available (scientific and technological) information. In fact, they tap into it so frequently that one must wonder if they regard U.S. R & D as their own national asset. They have enjoyed great success in this endeavor with minimal effort, primarily because, as a nation, we lack the awareness of what they are about."

There is an old but relevant story about the great jurist Oliver Wendell Holmes. Late in his distinguished career on the Supreme Court, Holmes found himself on a train. Confronted by the conductor, the Justice couldn't find his ticket. The conductor, however, recognized the distinguished jurist and told him not to worry, that he could just send in the ticket when he found it. Holmes looked at the conductor with some irritation and replied:

> "The problem is not where my ticket is.
>
> The problem is, where am I going?"

For too long, America had failed both to recognize the extent of our technology transfer problem and to develop an effective counterstrategy. Today, I want to outline for you the extent of the problem and to discuss where we are going in an effort to meet it. We now know what the Soviets are about, and we intend to stop them.

The problem is grave, but we have set in motion significant countermeasures against the threat to our national security and economic development. The loss of advanced technologies such as those developed in this area undermines our military capability and threatens future jobs and prosperity. The so-called "gray-market" domestic transfer of stolen parts or processes tarnishes the competitiveness of our industrial production. You in this area do not need to be reminded of the importance of high technology industries to our economy. More than 2700 California companies work with classified information -- including over 600 companies within thirty miles of San Francisco. The national security impact of

illegal technology transfer is, however, a story that bears telling and retelling.

During the past decade, the United States relaxed controls on trade with the Soviets in the hope that a resulting moderation in their behavior would contribute to world peace. Nevertheless, Soviet behavior has frustrated American good will and hope at every turn. Throughout this period, the Soviet Union has steadily improved its military weapons. By acquiring Free World technology, the Soviets have developed much more sophisticated weaponry than they could have otherwise produced on their own.

In one of the earliest actions of this Administration, the intelligence community -- the Central Intelligence Agency, the Defense Intelligence Agency, the National Security Agency, and the intelligence division of the Federal Bureau of Investigation -- prepared a comprehensive study of Soviet efforts to acquire U.S. and Western strategic technology. By the Fall of 1981, the first drafts of this study revealed the magnitude of Soviet efforts to acquire and use U.S. and Western technology in their weapons systems.

In April of this year, the Central Intelligence Agency published an unclassified version of its report entitled "Soviet Acquisition of Western Technology." The report described the Soviet effort, the methods of acquisition, the range of acquisitions that have contributed to Soviet military power, the projected Soviet priority needs, and the problems of effectively preventing the transfer of technology that could find application in Soviet weapons. It is now apparent, as the CIA report concluded, that stopping the Soviets' extensive acquisition of military-related Western technology -- in ways that are both effective and appropriate in our open society -- is one of the most complex and urgent issues facing the Free World today.

The acquisition of Western technology is an important aspect of Soviet foreign policy. Access to our advanced technologies has enabled Soviet-bloc countries to improve their armament and communication systems in a short time -- without the substantial research and development investment that made our achievements possible. It has allowed them to employ components in their weaponry that they are unable to manufacture in the Soviet Union and has given them the opportunity to analyze our systems and determine their weaknesses.

The Soviet effort to acquire strategic technology is massive, well-planned, and well-managed. It is a national program directed from the highest levels of the Soviet government. Our national security itself is threatened because we depend on our superior technology as a defense against Soviet military advantages in manpower and sheer volume of weaponry.

The Soviets and their Warsaw Pact allies have obtained vast amounts of militarily significant Western technology through legal and illegal means. The Soviet intelligence services -- the Soviet Committee for State Security or KGB and the Chief Intelligence Directorate of the Soviet General Staff or GRU -- have primary responsibility for collecting classified, export-controlled, and proprietary technology, using both clandestine and overt collection methods. It is estimated that these intelligence organizations have several thousand technology collection officers currently at work throughout the Free World under various covers ranging from diplomats, to businessmen, to students, to trade officials. Other quasi-independent entities in the Soviet System work closely with the KGB and GRU in these collection efforts. Through this coordinated use of resources, the Soviets have acquired militarily significant technologies and critically important industrial technologies that have benefited every major Soviet industry engaged in the research, development, and production of weapons systems. Our intelligence community estimates that about seventy percent of the military-related technology the Soviets have acquired from the West has been obtained by the Soviet and East European intelligence services.

In many instances, the Soviets have acquired Western technology through legal means. Clearly, however, Soviet assurances that legally purchased strategic technology will be used solely for civilian applications must be judged with suspicion. The mistakes of the past must not be repeated. Several examples of such mistakes are well known. The Soviet Kama River Truck Plant was built with massive imports of U.S. and West European automotive production equipment and technology. Large numbers of military trucks produced there are now being used by Soviet forces in Afghanistan and by Soviet military units in Eastern Europe.

Improvements in the accuracy of Soviet ballistic missile systems were aided by the acquisition of Western technology. Through legal purchases during the 1970s, the Soviets acquired U.S. precision grinding

machines for the production of small, high precision bearings. These purchases enabled the Soviets to manufacture the bearings that are an integral part of high quality guidance components in the latest generation of Soviet ICBMs. We are all familiar with the problems the improved Soviet missile systems have caused for our national defense -- and the consequent cost the taxpayers must bear to develop an improved U.S. missile basing system.

The Soviets have also acquired military-related technology through various covert and illegal means. The sophistication of their illegal schemes to acquire our technology is impressive. Their boldness is astonishing. In August of this year, it was discovered, based on information provided by a U.S. company here in California, that a computerized processing system designed to enhance photographs taken from reconnaissance satellites had been diverted to the Soviet Union in 1979 from its lawful destination -- a firm in Great Britain. The equipment was subsequently returned to the company in the United States through Great Britain for "upgrading and modification." This brazen incident, in which illegally obtained equipment was returned to the U.S. for repair, illustrates the confidence the Soviets have developed in the course of their efforts. It also underscores the dependence of federal countermeasures on support from the U.S. business community. Without the alertness of the U.S. firm, the equipment probably would not have been seized and would have found its way back to the USSR.

A classic example of the espionage engaged in by the Soviet Bloc is the case developed by the FBI in 1981 against William Bell and Marian Zacharski. Bell was a radar engineer employed by the Hughes Aircraft Company in Los Angeles. Since 1978, he had furnished classified documents on tactical aircraft navigation and weapons systems to the Polish intelligence service. Bell was recruited by Zacharski, a Polish intelligence operative who was the West Coast sales representative of the Polish American Machinery Corporation. There is evidence that the Polish Intelligence Service was acting under the supervision of the Soviet Intelligence Service. In 1981, we presented this case to a federal grand jury, and Bell and Zacharski were charged with espionage and conspiracy to commit espionage. Bell cooperated with the Government in this prosecution, pled guilty, testified for the Government, and received an eight-year sentence. Zacharski was convicted by a jury, and the Court sentenced him to life imprisonment.

As FBI Director Webster has said, "This case is a textbook example of espionage" -- and the techniques used by the foreign agent should be made known to every American who works in our technology industry. First, there is a chance social meeting followed by what could in some cases be months or even years of careful cultivation of that social relationship. Next, there is a deliberate sounding out of the target for information that indicates his vulnerability and his access to valuable data. Then, the unwary businessman is involved through gifts, loans, or a personal favor. Finally, the moment of truth arrives -- the hook is firmly set and confidential or classified information is requested.

Often, even after uncovering such a scheme, it is not possible for us to bring a criminal prosecution against the foreign agent because many of these people are protected by diplomatic immunity. When they are caught, they can only be deported. In other cases, we must make a very difficult judgment whether to leave a known intelligence officer in place so that we can use him or at least neutralize him in various ways. If we do not, he may well be replaced by someone whom we do not know.

In addition to their espionage efforts, the Soviets violate our export control laws -- the Export Administration Act and the Arms Export Control Act. They use corrupt businessmen to export strategic technology illegally from the United States to the Soviet Union through Western Europe and other Free World countries.

One of the largest illegal technology export operations uncovered in the United States to date was the Continental Technology Corporation case. Conducted out of the Los Angeles area for approximately three and one-half years, between January 1977 and June 1980, our investigation focused upon the formation of a number of shell-type electronics firms in California and West Germany. Soviet-controlled firms in Western Europe sent orders to the California front companies for state-of-the-art integrated circuit manufacture and testing equipment computers, computer peripheral equipment, and electronic and communication equipment systems and components. The California companies purchased the technology -- and using false statements in shipping documents, shipped the goods illegally out of the United States into Western Europe, where the goods were trans-shipped to the Soviets.

This case was jointly investigated, under the direction of the Department of Justice, by the Customs Service, the Department of Commerce, and a grand jury in the Central District of California. A multi-count indictment was returned in August 1981. And in December 1981, both U.S. defendants were sentenced to terms of imprisonment.

The cases that our investigative agencies have developed, and are in the process of developing, reveal that the Soviets know exactly what they want right down to the model numbers of specific items. A government engineering expert who analyzed the equipment purchased in the Continental Technology case concluded that, during the three-year period of the operation, the Soviets purchased everything they needed to construct at least one complete integrated circuit production plant.

High quality integrated circuits are the heart of modern military electronics. Integrated circuits form the basis for military systems that are more flexible, more capable, and more reliable than systems using discrete electronic components. It is well known in the engineering community that the Soviets are having serious problems developing their integrated circuit industry. The Continental Technology case demonstrates that the Soviets are trying to remedy their shortcomings by illegal acquisition of Western strategic technology.

The intelligence community has concluded that the Soviets will continue their attempts to acquire a broad range of U.S. and Western technology through the 1980s. They have targeted microelectronics, computers, communication, navigation and control, lasers and optics, shipbuilding, nuclear physics, manufacturing, and micro-biology. These technologies are directly related to the Soviets' plans to improve their military weapons systems.

Even this brief survey of the technology transfer problem reveals a serious challenge to the United States and its allies. The Administration has begun consultations with our allies and trading partners to coordinate our technology control policies. In addition, we seek through our consultations to ensure that U.S. business will not be asked to make empty sacrifices that their Western competitors do not make. We have also redoubled our enforcement efforts, streamlined the mechanisms that deal with this complex problem, and brought new coordination to the activities

of the revitalized intelligence services that support our enforcement agencies.

At the Ottawa summit meeting in July 1981, President Reagan raised the problem of Western technology transfer to the Soviet Union. An agreement reached at Ottawa to consult on this issue culminated in a high-level meeting in Paris in January 1982. This was the first ministerial level meeting of the Coordinating Committee for Multilateral Export Controls or "COCOM" since the late 1950s.

COCOM was created by informal agreement in 1949 and includes Japan and all NATO countries, except Iceland and Spain. It was formed among the major Western industrialized nations to achieve a fundamental agreement identifying militarily critical technologies and controlling their transfer to the Soviets.

The Paris meeting in 1982 developed a consensus that the member governments should renew their efforts to improve COCOM's effectiveness, including the revitalization of the COCOM system for multilateral export controls. As a result, we are currently working on proposals that would expand COCOM control lists into previously uncovered priority industries, such as robotics. We have also developed proposals for harmonizing the reporting and licensing procedures of the fifteen member states to make COCOM decision-making more effective. In addition, we conduct an ongoing review of the controlled technologies list to limit it to those products and procedures that are not available on the world market and whose export would adversely affect our national security.

On the domestic front, this Administration has significantly upgraded and revitalized our export control enforcement program. The Customs Service and the Commerce Department have increased the resources devoted to export control enforcement. In February of this year, the Customs Service initiated a national enforcement program, called "Operation Exodus," to prevent the illegal export of strategic technology from the United States.

Operation Exodus is being coordinated from a national command center, located at Customs headquarters in Washington. The command center is staffed with special agents and intelligence analysts who coordinate intelligence, inspection, and investigative activities both here and abroad. The fine work of the Customs

Service has resulted in several significant prosecutions, and current investigations will result in additional prosecutions. From October 1981 to October 1982, Customs agents "detained" over 2500 shipments for further investigation as part of Operation Exodus. These investigations led to almost 800 formal "seizures," valued at nearly $56 million. And since October 1982, there have been over 200 additional "seizures."

We anticipate that the Commerce Department will continue to play an important part in preventing the diversion of strategic technology to the Soviets. For example, the Commerce Department recently increased its resources in the area -- establishing the Office of Export Enforcement and opening new field offices here and in Los Angeles.

The Administration will also continue to urge the Congress to adopt amendments to the Freedom of Information Act that would exempt controlled technical data from disclosure. We all place a high value on the openness of our society and encourage legitimate public access to government records. Nevertheless, it is incongruous to prohibit the export without a license of certain types of sensitive but unclassified information concerning high technology or U.S. weapons systems, and yet not be able to deny public release of this type of information in response to a Freedom of Information request.

Many people incorrectly assume that the CIA is responsible for countering hostile intelligence activities within our territory. In reality, the FBI has that primary responsibility -- as well as jurisdiction over sabotage, international terrorist activities and assassinations conducted for foreign organizations or powers.

In fact, the FBI has a dual role in combating Soviet acquisition of our technology. As a member of the intelligence community, it develops intelligence to support its own law enforcement efforts, as well as those of the Customs Service and the Commerce Department. Although the Customs Service and the Commerce Department investigate violations of the Export Administration Act, and the Customs Service investigates violations of the Arms Export Control Act, foreign counterintelligence investigations and other criminal investigations by the FBI can also uncover violations of these Acts. When this occurs, the Bureau continues the export control investigation in appropriate coordination with Commerce

and Customs -- and integrates it into ongoing espionage investigations.

In addition, the FBI conducts a program to develop public awareness of the real threat posed by hostile intelligence services. This program -- called DECA, for Development of Counter-intelligence Awareness -- is directed at defense-related companies involved in classified work. There are currently over 11,000 of these companies, and many are located in the Bay Area. The DECA program seeks to alert each company's management and security personnel to the possible threat to that company posed by hostile intelligence services. Employees are taught how to react to a possible approach by unauthorized persons seeking secret information -- whether an approach from a "friendly neighbor," as in the Bell-Zacharski case, or a more sophisticated approach in a foreign country or at an international symposium or trade association meeting. Such training should result in the reporting of more incidents to company security officials, the FBI, or other appropriate authorities.

Of course, the Criminal Division of the Department of Justice and the United States Attorneys' Offices throughout the country play a key role in our enforcement program. Lowell Jensen, a fellow Californian who is the Assistant Attorney General for the Department's Criminal Division, is also the Chairman of a broad-based interagency committee responsible for coordinating all facets of enforcement. Mr. Jensen, his staff, and the concerned departments and agencies meet regularly to assess the direction and effectiveness of the program. He has also created a special unit in the Internal Security Section of the Criminal Division to coordinate investigations and prosecutions. Other interagency groups are also working on this complex problem. In addition, I meet personally with FBI Director Webster and CIA Director Casey to coordinate our efforts. In brief, the government is actively addressing the broad spectrum of issues presented by the Soviet threat.

We at Justice are committed to the vigorous enforcement of our espionage laws and the laws prohibiting the unlicensed export of strategic technology. We especially recognize the importance to our national security and national economy of halting the illegal transfer of strategic technology from Northern California. We are therefore intensively studying the creation of a Critical Technologies Task Force here in Northern California. Such a Task Force could coordinate

an interagency operation consisting of Assistant United States Attorneys; agents of the FBI, the Commerce Department, and the Customs Service; postal inspectors; and IRS investigators -- all of whom would cooperate with state and local police forces and concerned corporate officers.

As you know, we have found the task force concept to be quite effective and intend to use it in our campaign against organized crime and narcotics. High-technology cases also require coordinated and determined investigation. The members of a Critical Technologies Task Force could bring to bear the necessary technical expertise and prosecutorial experience to identify, indict, and convict the greedy few who attempt to betray their country by illegally exporting our critical technology. Whatever approach our study of this issue shows would be most effective, I can promise you we will implement it. Here in Northern California -- and throughout the country -- we intend to thwart the Soviet attempt to acquire our sensitive technology.

It is clear that coordination within the intelligence community and intelligence support to the concerned departments and agencies regarding technology transfer have already improved significantly. The Central Intelligence Agency has itself established a Technology Transfer Intelligence Committee to serve as a focal point within the intelligence community, to ensure that information collected on technology transfer meets the needs of the enforcement authorities.

We are developing an effective program to prevent the transfer of our strategic technology to the Soviets. Our national security and future prosperity depend upon meeting the threat of technology transfer. With your assistance -- and the assistance of other concerned citizens -- our country will meet that threat.