MEMORANDUM FOR [redacted]

The attached is for the DCI's meeting with the [redacted].

It contains:

- A paper on what might be done to stop technology transfer losses.
- A copy of the material (in table form) of what I presented the PFIAB S&T Working Group (John Foster's group) in April.
- Several copies of the Unclassified paper.

[redacted]

Date

FORM 5-75 101 USE PREVIOUS EDITIONS

GPO : 1981 O - 345-783

Next 1 Page(s) In Document Denied

Background Notes

TECHNOLOGY TRANSFER LOSSES AND SOME ACTIONS TO STOP THEM

1. The loss of militarily significant US technology can be traced to three basic technology transfer channels:

1. Open Source Acquisitions
2. Trade-related Transfer
3. Soviet Bloc Intelligence Operations

The principal responsibility for stemming losses through the first two channels, Trade and Open Sources, resides within the Export Control Community and other appropriate Government Departments. The Intelligence Community can help with these efforts and does; for example:

-- by providing intelligence support for export control license and CoCom List reviews;

-- by providing intelligence for export control enforcement activities, particularly those involving evasion or diversion of CoCom countries' controlled exports;

--by alerting government and private organizations that Soviet acquisition of their publications, S&T information, and data bases is contributing to Soviet military capabilities; and

--by working with joint government public groups such as the one underway now at the National Academy of Sciences seeking to find an equitable way to protect defense-sensitive technology being developed on University campuses.

SOVIET INTELLIGENCE THREAT:

2. Stopping Soviet Bloc Intelligence operations--clandestine, technical and overt -- aimed at the acquisition of US and other Western (including Japanese technology), both in the US and abroad, is viewed as solely an Intelligence Community (IC) responsibility, whether the technology is classified, export controlled, company proprietary or openly available. The IC is expected to stop the Soviet and East European intelligence service acquisitions of technology that can harm our national security.

3. Based on recent analyses of extremely hard intelligence we now believe that the vast majority--as much as three-fourths (3/4)-- of militarily significant Western technology being acquired by the Soviet Bloc is the result of Soviet and East European intelligence activities. Furthermore, we believe:

-- that the overwhelming majority of classified US technology is being acquired abroad,

-- that East European intelligence services are significant contributors to the Soviet acquisition effort,

-- that Soviet and East European intelligence services, working closely with their ministries of foreign trade, play the key role in illegal trade acquisitions, both in the United States and abroad, operating through agents, cooperating businessmen, and cover organizations in Soviet Bloc trade and manufacturing ministries,

-- that more and more, militarily significant technology is being acquired through the illegal acquisition of company

proprietary technology and defense-sensitive but unclassified government S&T publications and sponsored research, and

-- that Soviet Bloc intelligence acquires some of the militarily significant technologies through overt collection from open sources such as universities, S&T conferences, and exchange programs, and trade fairs in the United States.

4. Possible Countermeasure Actions: To effectively counter Soviet Bloc intelligence efforts, the US must develop a strategy and plan to cope with all three intelligence related acquisition activities simultaneously: clandestine, technical (mainly SIGINT), and overt. At the same time these US intelligence counter actions must be closely coordinated with Export Control enforcement and Government-led efforts to protect open sources and alert the general public to the problem. And, possibly even more important, the US effort to stop the loss of our technology in the US must be projected abroad. Among the actions that can be initiated to accomplish this are the following:

First

-- The US Government must develop an integrated program to cope with US technology losses abroad.

-- US counterintelligence-- CIA and the Military-- must be explicitly focused on the problem as a joint effort, with the protection of US defense related technology, persons (including companies), and organizations, located abroad

being the primary objective.

-- Allied counterintelligence and internal security services must be alerted to our concerns for the protection of US technology abroad and the nature of the overall threat. John McMahon's recent European trip has now started this process.

-- US intelligence elements abroad should be directed to support US export control efforts at each key post, working as part of a country-team effort. US counterintelligence should also assist US Customs' efforts worldwide in their efforts.

-- A foreign public awareness effort concerning technology transfer losses should be mounted through CIA's liaison activities with allied intelligence services.

Secondly

These international efforts of the US Intelligence Community should be closely coordinated with new programs and initiatives being implemented in the United States:

-- Counterintelligence operations aimed at stopping the losses of classified and export controlled US technology in the US should be conducted through normal CIA-FBI channels, such as is presently being done.

-- A long-range strategy for disrupting the Soviet technology acquisition programs and undermining Soviet Bloc intelligence services in the minds of their military-industrial consumers should be developed for

counterintelligence and covert action operations; this should be done with great care and high security.

-- Defense contractor industrial security, which is mainly directed at protecting classified documentary technology, must be improved to account for the HUMINT threat posed by Soviet Bloc intelligence that often seeks company unclassified proprietary technology associated with defense production and not the weapon system itself.

-- Foreign intelligence operations involving US technology and US persons should be closely coordinated through the Justice Department-led Interagency Working Group (IAWG) on Domestic Enforcement; such activity is just now beginning.

-- Protection of unclassified, defense-sensitive S&T information and related Government sponsored research must be better protected from Soviet Bloc intelligence activities.

-- Protection from hostile intelligence services must be developed for non-defense firms engaged in high technology R&D that may either assist Warsaw Pact military efforts or may be used as critical components in future US weapons.

If we are to be successful in stopping the flow of militarily significant technologies to our military adversaries, all of these intelligence related activities will have to be as well coordinated as the overall Soviet acquisition program itself.