~~SECRET/NOFORN~~ UNCLASSIFIED 21058

THE WHITE HOUSE

WASHINGTON

October 5, 1990

NATIONAL SECURITY DIRECTIVE 47

MEMORANDUM FOR THE VICE PRESIDENT
THE SECRETARY OF STATE
THE SECRETARY OF THE TREASURY
THE SECRETARY OF DEFENSE
THE ATTORNEY GENERAL
THE SECRETARY OF ENERGY
DIRECTOR, OFFICE OF MANAGEMENT AND BUDGET
CHIEF OF STAFF TO THE PRESIDENT
ASSISTANT TO THE PRESIDENT FOR
NATIONAL SECURITY AFFAIRS
DIRECTOR OF CENTRAL INTELLIGENCE
CHAIRMAN, JOINT CHIEFS OF STAFF
DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION

SUBJECT: Counterintelligence and Security Countermeasures (U)

The decade of the 1990s will pose new challenges and opportunities for U.S. counterintelligence (CI) and security countermeasures (SCM). By the end of the 1990s, we will probably see a markedly different threat environment. This dynamic situation requires thoughtful and systematic CI and SCM planning, resource commitment, and imaginative implementation. We must enhance our ability to anticipate the scope and pace of changing intelligence threats and to respond with successful operational initiatives. CI and SCM matters should continue to be handled in the 1990s as strategic issues requiring priority attention. ~~(C)~~

This decade will be marked by political turbulence and economic, social, and cultural stresses in every region. We must be prepared for diverse political transformations, for intense international economic competition, increased North-South tensions, and for growing foreign intelligence access to U.S. targets here and abroad. Through it all, classified and proprietary U.S. foreign policy, military, intelligence, and technological information, plans, and programs as well as U.S. economic strategies will remain priority strategic targets for our adversaries. U.S. technologies, both classified and proprietary, will remain a high priority for those seeking a competitive edge in international markets. U.S. policymakers will continue to be targets of covert-influence operations. ~~(C)~~

~~SECRET/NOFORN~~
Declassify on: OADR

~~UNCLASSIFIED~~

In this changing environment, our CI and SCM initiatives should focus on the following goals. We must:

- Anticipate, detect, and neutralize human and technical operations conducted by foreign intelligence services targeting U.S. interests. ~~(C)~~
- [redacted] 1.5 (c)
- Adapt to the CI and security implications of the new U.S. policy of furthering the political and economic integration of the Soviet Union and Eastern Europe into the world economy. (U)
- Reduce our vulnerabilities to intelligence exploitation by foreign services within the United States and abroad by enhancing the security and CI integrity of our programs, operations, personnel, and installations worldwide. ~~(S)~~
- Maintain an effective mechanism to plan for and forecast the changing CI and SCM environments worldwide; to recommend operational, analytic, and security initiatives; to identify priority targets and resources; and to address evolving issues. ~~(S)~~

To achieve these goals, we should emphasize offensive initiatives but also provide defensive enhancements and allocate resources in accordance with these priorities as ranked. ~~(C)~~

Offensively, we shall:

- Enhance our ability to make early identification of U.S. persons who volunteer to commit espionage and refer those cases to the appropriate agency to pursue investigation and prosecution. ~~(C)~~
- [redacted]
- [redacted]

1.5 (c)

- [redacted] 1.5 (c)
- Use our control of the domestic environment to anticipate, detect, and disrupt efforts by foreign intelligence services to exploit new operational opportunities in the United States. (C)
- [redacted] 1.5 (c)
- Improve the focus and integration of CI analysis into operational targeting programs. (S)
- Build new Automated Data Processing capabilities using expert systems and artificial intelligence to better support interagency analytic exploitation of data bases. (S)
- Mount aggressive programs to enable us to identify and operate against foreign government-sponsored or government-subsidized operations targeted against U.S. technological and economic competitiveness. (S)
- [redacted] 1.5 (c)

Defensively, we shall:

- Enhance our ability to identify foreign intelligence targeting against U.S. information security systems and keying material through better exploitation of all-source information. (C)
- Provide more secure working environments within U.S. diplomatic establishments abroad by instituting coordinated technical and personnel security standards. (C)
- Expand development and implementation of information systems security programs that dramatically improve U.S. posture in the areas of network and technical security. Evaluate espionage vulnerabilities of secure telecommunications and automated information systems. (S)
- [redacted]

[redacted] 1.5(c), (d)

- Conduct thorough espionage damage assessments to learn how the damage done in one case relates to damage from another and to implement lessons learned. (S)

- Improve our security awareness programs to ensure a full understanding of the threat and the attendant security practices necessary to limit vulnerabilities. (U)

Organizationally, we shall:

- Establish interagency training programs of CI analytic and operational elements to address new and evolving issues and threats and to disseminate key findings throughout the national security community. (C)

- Integrate analysis with CI operations to produce new methodologies, to identify our programmatic strengths and weaknesses, and to better project and forecast the changing human and technical threat environment. (C)

- Develop a highly skilled corps of CI professionals with substantive expertise and a strong commitment to better equip us to meet the CI threats in the 1990s. (C)

Legislatively, we shall:

- Ensure the administration continues to work closely with Congress on CI and SCM legislation seeking to improve U.S. Government capabilities in these areas. (C)

Furthermore, with respect to polygraph examinations, there is interagency agreement and administration endorsement of continuing a polygraph component in the overall personnel security effort. This polygraph component should be implemented by and within each agency in accordance with the policy of that agency. Agencies implementing polygraph programs will ensure that their efforts are closely coordinated to achieve maximum efficiency, effectiveness, and economy. (U)

Finally, when matters involving CI or security issues are referred to the Department of Justice for criminal investigation, the FBI will be responsible for the conduct of polygraph examinations as may be appropriate. (U)

IMPLEMENTATION

I hereby direct the recipients of this memorandum to implement the recommendations cited in NSR-18 and charge the Director of Central Intelligence, under the guidance of the National Security Council, with coordinating the interagency effort towards these goals. I also charge the DCI with soliciting specific plans of each concerned agency for implementing the strategy for the 1990s. Major issues that may arise in the implementation of this strategy shall be resolved through the NSC process in accordance with NSD 1. ~~(S/NF)~~

On an annual basis, the National Advisory Group for Counterintelligence and Security Countermeasures shall review the progress being made to implement NSR 18 recommendations and report this progress as deemed appropriate. ~~(C)~~