THE WHITE HOUSE

WASHINGTON

April 16, 1993

PRESIDENTIAL REVIEW DIRECTIVE/NSC-27

MEMORANDUM FOR THE VICE PRESIDENT
THE SECRETARY OF DEFENSE
THE ATTORNEY GENERAL
THE SECRETARY OF COMMERCE
THE DIRECTOR OF THE OFFICE OF MANAGEMENT & BUDGET
THE ASSISTANT TO THE PRESIDENT FOR ECONOMIC POLICY
THE DIRECTOR OF CENTRAL INTELLIGENCE
THE DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION
THE DIRECTOR OF THE NATIONAL SECURITY AGENCY

SUBJECT: Advanced Telecommunications and Encryption (U)

New developments in telecommunications hold great promise for the American economy -- its productivity and global competitiveness. But they also pose risks to the government's ability to enforce laws and protect national security. We must, with some urgency, find new ways to accommodate the government's interests in law enforcement, privacy, national security, productivity and competitiveness. (U)

The President has directed in Presidential Decision Directive/ NSC-5 that agencies (1) seek the installation of a key-escrow technology in communications encryption devices for commercial sale; (2) seek the adoption of a new encryption standard based on key-escrow techniques; and (3) acquire certain encryption devices. In addition to these actions, the President has directed a thorough study of broader telecommunications and encryption issues for the purpose of determining the least burdensome and most effective methods of maintaining our current capabilities to conduct legally-authorized and effective communications intercepts and to control encryption exports. This PRD initiates that study. ~~(C)~~

BACKGROUND

The Clinton Administration is committed to the development of an information superhighway and National Information Infrastructure that depends on a developing synergy between telecommunications and computer technologies. Rapid changes in both the telecommunications and computer industries have blurred the traditional gaps that separated these technologies. The result of these changes has significantly improved both our telecommunications infrastructure and computational capability. (U)

SECRET

At the same time many of the technologies that facilitate rapid implementation of these advanced information systems inhibit lawfully authorized electronic surveillance by government agencies. For example, some advanced telecommunications that form the backbone of the information superhighway also nullify the effectiveness of traditional methods of carrying out court authorized wiretaps. The encryption technologies that can be used to protect privacy and business data can also be used by lawbreakers to prevent the government from obtaining contents of information it is authorized to intercept. (U)

This study will broadly assess trends in telecommunications and encryption technology and their impact on law enforcement and intelligence gathering. It will also evaluate the impact of the encryption technology proposed in PDD/NSC-5. This policy review should be completed with a report of the NSC Deputies Committee by June 30, 1993. It should include a full range of clear policy options/recommendations for dealing with these issues. Any difference in view among agencies should be noted. At a minimum, the review should address the questions and issues stated below. ~~(S)~~

PART I: ASSESSMENT

Telecommunications Technologies

1. What are the trends in telecommunications technologies -- both in the United States and elsewhere -- that could affect the ability of the law enforcement and intelligence communities to meet their respective missions? How widespread is the use of advanced telecommunications technologies and in what applications, both domestic and foreign? What is the estimated future demand for these types of technologies in the near, intermediate and long term? How are these trends affected by changes in encryption technology? ~~(S)~~

2. What is the impact, including risks and opportunities, of advances in telecommunications services on:

a. federal, state and local law enforcement capabilities and performance (including public safety); (U)

b. national security intelligence capabilities and performance; ~~(S)~~

c. privacy and security of personal, commercial, and government information in the U.S. and abroad; (U)

d. U.S. commercial competitiveness? (U)

Encryption Technologies

3. What are the principal encryption techniques in use within the United States and elsewhere throughout the world? How widespread is the use of each encryption technique and in what applications, both domestic and foreign? What is the estimated future demand for these encryption techniques in the near, intermediate and long term? What is driving this demand for both legitimate and non-legitimate end-users? How are these trends affected by other trends in advanced telecommunications? ~~(S)~~

4. What is the impact, including risks and opportunities, of advances in encryption technologies on:

a. federal, state and local law enforcement capabilities and performance (including public safety); (U)

b. national security intelligence capabilities and performance; ~~(S)~~

c. privacy and security of personal, commercial, and government information in the U.S. and abroad; (U)

d. U.S. commercial competitiveness; (U)

e. the security and reliability of the telecommunications network. (U)

Key-Escrow Technique for Encryption

5. What are the uses, domestic and foreign, of the key-escrow technology developed by the government in software, hardware and telecommunications applications? Assess the relative practicality of voluntary versus mandatory uses of this approach? What are the reactions of industry to this approach? What reactions to this encryption approach might be expected from foreign manufacturers and governments? For domestic and foreign licensing of the technology? What institutional agents are feasible for key-escrow safekeeping? (U)

6. Are there unacceptable risks that the key-escrow technique may be readily disabled when implemented in software encryption products? If so, what other possible solutions might assure authorized government access to information protected by software encryption and still afford reasonable encryption protection to software end-users? (U)

7. Can key-escrow techniques other than the techniques described in PDD/NSC-5 be developed by drawing on the resources of U.S. encryption and telecommunications industries, as well as on

government experts? Review of alternative techniques should consider how to prevent the development of interoperable devices that defeat the key-escrow feature. ~~(C)~~

Export Controls

8. Do export controls have an impact on these industry sectors? Is that impact quantifiable? Do they have an impact on national security? Is that impact quantifiable? What are the current and likely future techniques by which foreign governments control encryption and advanced telecommunications technologies of concern to law enforcement and the intelligence community? How effective are these controls? What has been the effect of changes in export controls over the past few years? ~~(S)~~

PART II: OPTIONS

Options should be developed to answer the following key question: How can the government accommodate: (1) the use of encryption and advanced telecommunications; (2) the need to assure government capabilities to access communications content and to decrypt such content when authorized by law; and (3) the continued competitiveness of U.S. manufacturers of encryption, advanced telecommunications equipment, and computer hardware and software? In answering this question, specific attention should be given to the key-escrow technique. The results of previous proposals to regulate advanced telecommunications and encryption should also be assessed as part of developing these options. ~~(S)~~

The following should guide the development of the options:

-- Whether and in what circumstances legislation or other regulation of encryption and advanced telecommunications is warranted; (U)

-- Whether these interests can be accommodated through (1) cooperative arrangements with manufacturers and telecommunications service providers and those who manufacture and offer encryption services; (2) alternative investigative/collection techniques; (3) technological innovation; (4) international agreements/arrangements; and (5) adjustments to domestic and international standards. (U)

In developing these options, their costs should be provided along with likely reactions of industry, the Congress, foreign manufacturers and governments, and those entities affected by the recommended option. Recommended implementing strategies should be provided. (U)

PART III: TASKING

An IWG will be established by the NSC that will include representatives from all cognizant agencies. The IWG will ensure that there are early and frequent consultations with industry throughout the course of this review, subject to appropriate protection of classified information. (U)

Anthony Lake
Assistant to the President
for National Security Affairs