Transcript of a Signal From Washington to the US Embassies in London and Paris

Date: 22nd November 1996
From: Secretary of State, Washington DC
To: American Embassy, London
American Embassy, Paris

Subject: **US Encryption Initiative: Instructions for Ambassador Aaron**

For OECD Ambassador D. I. Aaron

Ref: (a) 96 State 239684, (b) 96 State 219420, (c) 96 State 203456

1. The following instructions have been approved by the Interagency Working Group on Cryptography. London please pass to ambassador Aaron upon his arrival.

2. Begin text:

The objective of your mission is to foster the international cooperation needed to achieve the goals of the Clinton administration encryption initiative; specifically to promote the world-wide use and development of strong encryption products and a global key recovery architecture that provide security for the global information infrastructure while protecting public safety and national security.

3. Your initial task is to explain U.S. policy to key countries as set forth in the vice president's statements of July 12 and October 1 and seek their views on establishing compatible approaches to encryption policy. In this connection, you should draw on State 203456, State 219420 and the subsequent decisions of the deputies' committee on the implementation of the encryption initiative. During these discussions, you should seek a consensus that the fullest use of the GII will require international cooperation to ensure the interoperability of encryption products, certification, and authentication. At the same time, you should seek acceptance of the principle that public safety and national security require timely lawful access to encrypted materials, including transnational accessibility to keys and/or plain text. Finally, you should keep in mind the U.S. national interest in the continued strong presence of U.S. firms in overseas markets for encryption products and services.

4. To this end, you should seek endorsement of the cryptography guidelines being developed at the OECD and urge support for completion in February 1997. Your discussions should also be aimed at facilitating ongoing bilateral discussion between responsible agencies of key and/or plain-text sharing arrangements for valid law enforcement purposes. You should seek general agreement that such arrangements would be based on a key management infrastructure that provides for key recovery through key escrow and/or trusted third party regimes.

5. In addition, your consultations should begin the process of determining, with other nations, how to build an internationally interoperable key management infrastructure with key recovery. You should emphasize that the United States does not have a preconceived solution to this problem and plans to consult with industry and law enforcement. You should, however, share our views on the following

issues, laying the groundwork for technical discussions as our own domestic discussions evolve:

Public Key Certification

This is essential for parties to know with confidence with whom they are communicating.

Principles of Interoperability

Principles of interoperability for exchange of public key certificates will be essential for transnational communication. These principles will need to address:

- Mutually recognized standards for certificate issuing authorities.
- What information the certificate should contain - e.g., who is being certified, the authority of the certifier, etc.
- What should be the process of certifying the identity of the parties.
- How certification is validated – internationally recognized forms of electronic signature.

Key Recovery

Users of key recovery encryption products need to know what entities will be able to decrypt their encrypted data and under what circumstances.

In addition, there will be a need to address common standards to promote interoperability of encryption systems for various sectors such as banking, electronic commerce and private mail, as well as interoperability between these sectors.

Private Sector Leadership

While governments must provide the appropriate policy framework, the task of building an international key management infrastructure with key recovery features should lie with the private sector. This policy framework will need to provide incentives to the private sector to build the KMI quickly. In this connection, you are authorized to have informal contacts with foreign industry leaders where appropriate to explain U.S. policy.

6. Following your initial round of consultations, you should report your findings to the Deputies' Committee along with recommendations for further action and issues for resolution.

End text of instructions to Ambassador Aaron.

Talbott