Transcript of a US Presentation given at a US/UK Government Meeting on Encryption Policy held in London in late 1996 or early 1997.

Initial Presentation (UK)

We welcome opportunity for consultation on the subject of encryption

- Want British views. Know given issue careful consideration. We can learn from your analysis. We appreciate your emphasis on law enforcement and national security and share your concerns.
- From what we understand of British policy, it appears our approaches are compatible. We look forward to learning more about British policy.
- Want to answer your questions on our policy. It is in the process of development and will profit from your questions and your approach to the problem.
- My mission is independent of my OECD responsibilities. I'm here as a special envoy appointed by the President and reporting to special Deputies Committee of the NSC.

Our goal is a world in which key recovery encryption systems are the dominant form of technology in the commercial market. This will provide the security to realize the full potential electronic commerce and the GII while permitting the protection of public safety and national security.

International cooperation is essential to creating this kind of global key recovery encryption environment:

- Governments need to make clear their commitment to access to encrypted files and communications so that industry will be encouraged to develop and market systems that provide for key recovery.
- Governments need to cooperate in creating the policy framework for an interoperable global key Management Infrastructure that facilitates key recovery.
- Governments need to agree that this infrastructure would provide for key recovery through key escrow and/or trusted third party regimes.
- Governments need to collaborate on key and/or plain-text sharing arrangements in the context of lawful access.
- We need to consider the need for continuing consultations given the pace of changing technology.

We are open-minded on the modalities on such international cooperation.

Context of U.S. Policy

U.S. policy evolved from the realization that the use of strong commercial encryption will grow, along with international electronic commerce. We need strong encryption to secure the Global Information Infrastructure, protecting intellectual property and other valuable information.

Governments have a strong interest in promoting 'the legitimate use of robust encryption to support international competitiveness, foster global electronic commerce, prevent computer crime, and ensure that the information superhighway is a sale place to conduct business.

On the other hand, encryption is a weapon for criminals, terrorists and drug traffickers. Strong encryption can undermine law enforcement and national security by limiting our governments' ability to exploit communications intercepts and access computer files within the law.

The recently-announced U.S. encryption initiative is an attempt to balance national security and law enforcement needs with privacy and commercial interests. It also recognizes that international cooperation is an essential element in the development of an effective key recovery system.

U.S. Approach

Encourage development and market for key recovery encryption products 'that provide key escrow/TTP.

- This is being done by liberalizing export controls for a 2-year period, but only for those firms that demonstrate a commitment to developing and marketing key recovery.

The USG was not, and is not in a position to mandate key recovery. We have to use market forces to create an environment in which key recovery dominates the market.

- We believe that key recovery will have a strong market appeal because both individuals and companies will see a need for "spare key" arrangements in case of loss of keys.
- We believe that public key (asymmetric) encryption will come to be the preferred system of assuring confidentiality, because in addition to facilitating key recovery for key recovery, it fulfils a number of other needs:
    - ❖ Key exchange (of symmetric keys)
    - ❖ Authentication (message integrity)
    - ❖ Certification (of the sender and receiver)
    - ❖ Non repudiation (that transmission/transaction took place)
    - ❖ Digital signature
        - ➢ We need strong robust system
        - ➢ No royalties
        - ➢ Not convertible into an encryption engine

International KMI

Such a system of key recovery needs an internationally interoperable key management infrastructure. We do not have a preconceived plan or solution for IKMI and are consulting with you, other trading partners, industry and law enforcement. We have identified the following key elements:

Public Key Certification. This is essential for parties to know with confidence with whom are communicating. Certification Authorities have to be established and authorized. Recognition of CAs across borders will be necessary. CAs may also serve as TTPs.

Principles of Interoperability for exchange and 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 digital signature.

Key Recovery. Our vision calls for encryption users to deposit a copy of their key with a trusted third party (private sector entity), either in the U.S. or abroad, who would provide the key to the user in an emergency, or to law enforcement officials acting under the proper authority. Foreign TTP could be recognized if acceptable to the US and host governments. Criteria procedures and standards for recovering keys from TTPs will have to be established. Limits on liability of authorized release and penalties for unauthorized release of keys will have to be set. Users of key recovery encryption products need to know what entities will be able to decrypt their encrypted data and under what circumstances.

Exchange of Keys/Plaintext. If another nation requests U.S. assistance in retrieving such data for a legitimate legal purpose, we expect to offer timely exchanges of plaintext data when the keys are kept in the U.S. We would like to work with you to put in place the necessary legal agreements to facilitate this cooperation.

Interoperability of Systems. 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 inter-operability between these sectors. Non key recovery products interoperable with key recovery products should become recoverable.

We are interested in how the British system will intemperate with U.S. and other nations' systems. We are also interested in having demonstration projects in both our countries establish interoperability, to show how this can be accomplished.

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. We are working with private sector users (especially banks) to encourage market for key recovery.

We would welcome learning how Britain plans to approach these issues and will try to answer any questions you may have on our approach.

- In addition, our Department of Commerce would welcome technical discussions on the regulations they are developing and on your draft implementing decree. They would be ready in early December with their draft regs, but we can give you a preview today. What is the schedule for their promulgating your policy?
- Our Department of Justice and FBI look forward to discussions, also in early December, with your national police authorities. [? check with Mike]

We also would like to explore your view on the forms that international cooperation might take on many of these issues, bilateral, multilateral; formal/informal. We would appreciate your assessment of the policy of other members of the EU and the Commission and in particular French law and Policy on TTP key recovery. Having just had discussions in Paris we would be happy to share our reaction.

In this connection, we believe it is important that the OECD Guidelines on Encryption recognize the right of lawful access and that they be completed soon. These guidelines will be very important in securing wider support for the key recovery approach among countries such as Japan.