

PUBLIC ENCRYPTION MANAGEMENT

FACT SHEET

Note: The following was released by the White House today in conjunction with the announcement of the Clipper Chip encryption technology.

The President has approved a directive on "Public Encryption Management." The directive provides for the following:

Advanced telecommunications and commercially available encryption are part of a wave of new computer and communications technology. Encryption products scramble information to protect the privacy of communications and data by preventing unauthorized access. Advanced telecommunications systems use digital technology to rapidly and precisely handle a high volume of communications. These advanced telecommunications systems are integral to the infrastructure needed to ensure economic competitiveness in the information age.

Despite its benefits, new communications technology can also frustrate lawful government electronic surveillance. Sophisticated encryption can have this effect in the United States. When exported abroad, it can be used to thwart foreign intelligence activities critical to our national interests. In the past, it has been possible to preserve a government capability to conduct electronic surveillance in furtherance of legitimate law enforcement and national security interests, while at the same time protecting the privacy and civil liberties of all citizens. As encryption technology improves, doing so will require new, innovative approaches.

In the area of communications encryption, the U. S. Government has developed a microcircuit that not only provides privacy through encryption that is substantially more robust than the current government standard, but also permits escrowing of the keys needed to unlock the encryption. The system for the escrowing of keys will allow the government to gain access to encrypted information only with appropriate legal authorization.

To assist law enforcement and other government agencies to collect and decrypt, under legal authority, electronically transmitted information, I hereby direct the following action to be taken:

INSTALLATION OF GOVERNMENT-DEVELOPED MICROCIRCUITS

The Attorney General of the United States, or her representative, shall request manufacturers of communications hardware which incorporates encryption to install the U.S. government-developed key-escrow microcircuits in their products. The fact of law enforcement access to the escrowed keys will not be concealed from the American public. All appropriate steps shall be taken to ensure that any existing or future versions of the key-escrow microcircuit are made widely available to U.S. communications hardware manufacturers, consistent with the need to ensure the security of the key-escrow system. In making this decision, I do not intend to prevent the private sector from developing, or the government from approving, other microcircuits or algorithms that are equally effective in assuring both privacy and a secure key-escrow system.

KEY-ESCROW

The Attorney General shall make all arrangements with appropriate entities to hold the keys for the key-escrow microcircuits installed in communications equipment. In each case, the key holder must agree to strict security procedures to prevent unauthorized release of the keys. The keys shall be released only to government agencies that have established their authority to acquire the content of those communications that have been encrypted by devices containing the microcircuits. The Attorney General shall review for legal sufficiency the procedures by which an agency establishes its authority to acquire the content of such communications.

PROCUREMENT AND USE OF ENCRYPTION DEVICES

The Secretary of Commerce, in consultation with other appropriate U.S. agencies, shall initiate a process to write standards to facilitate the procurement and use of encryption devices fitted with key-escrow microcircuits in federal

communications systems that process sensitive but unclassified information. I expect this process to proceed on a schedule that will permit promulgation of a final standard within six months of this directive.

The Attorney General will procure and utilize encryption devices to the extent needed to preserve the government's ability to conduct lawful electronic surveillance and to fulfill the need for secure law enforcement communications. Further, the Attorney General shall utilize funds from the Department of Justice Asset Forfeiture Super Surplus Fund to effect this purchase.