White House Annoucement of the Clipper Initiative

This is the original public announcement by the White House of the Clipper initiative.

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release April 16, 1993

STATEMENT BY THE PRESS SECRETARY

The President today announced a new initiative that will bring the Federal Government together with industry in a voluntary program to improve the security and privacy of telephone communications while meeting the legitimate needs of law enforcement.

The initiative will involve the creation of new products to accelerate the development and use of advanced and secure telecommunications networks and wireless communications links.

For too long there has been little or no dialogue between our private sector and the law enforcement community to resolve the tension between economic vitality and the real challenges of protecting Americans. Rather than use technology to accommodate the sometimes competing interests of economic growth, privacy and law enforcement, previous policies have pitted government against industry and the rights of privacy against law enforcement.

Sophisticated encryption technology has been used for years to protect electronic funds transfer. It is now being used to protect electronic mail and computer files. While encryption technology can help Americans protect business secrets and the unauthorized release of personal information, it also can be used by terrorists, drug dealers, and other criminals.

A state-of-the-art microcircuit called the "Clipper Chip" has been developed by government engineers. The chip represents a new approach to encryption technology. It can be used in new, relatively inexpensive encryption devices that can be attached to an ordinary telephone. It scrambles telephone communications using an encryption algorithm that is more powerful than many in commercial use today.

This new technology will help companies protect proprietary information, protect the privacy of personal phone conversations and prevent unauthorized release of data transmitted electronically. At the same time this technology preserves the ability of federal, state and local law enforcement agencies to intercept lawfully the phone conversations of criminals.

A "key-escrow" system will be established to ensure that the "Clipper Chip" is used to protect the privacy of law-abiding Americans. Each

device containing the chip will have two unique "keys," numbers that will be needed by authorized government agencies to decode messages encoded by the device. When the device is manufactured, the two keys will be deposited separately in two "key-escrow" data bases that will be established by the Attorney General. Access to these keys will be limited to government officials with legal authorization to conduct a wiretap.

The "Clipper Chip" technology provides law enforcement with no new authorities to access the content of the private conversations of Americans.

To demonstrate the effectiveness of this new technology, the Attorney General will soon purchase several thousand of the new devices. In addition, respected experts from outside the government will be offered access to the confidential details of the algorithm to assess its capabilities and publicly report their findings. The chip is an important step in addressing the problem of encryption's dual-edge sword: encryption helps to protect the privacy of individuals and industry, but it also can shield criminals and terrorists. We need the "Clipper Chip" and other approaches that can both provide law-abiding citizens with access to the encryption they need and prevent criminals from using it to hide their illegal activities. In order to assess technology trends and explore new approaches (like the key-escrow system), the President has directed government agencies to develop a comprehensive policy on encryption that accommodates:

the privacy of our citizens, including the need to employ voice or data encryption for business purposes;

the ability of authorized officials to access telephone calls and data, under proper court or other legal order, when necessary to protect our citizens;

the effective and timely use of the most modern technology to build the National Information Infrastructure needed to promote economic growth and the competitiveness of American industry in the global marketplace; and

the need of U.S. companies to manufacture and export high technology products.

The President has directed early and frequent consultations with affected industries, the Congress and groups that advocate the privacy rights of individuals as policy options are developed.

The Administration is committed to working with the private sector to spur the development of a National Information Infrastructure which will use new telecommunications and computer technologies to give Americans unprecedented access to information. This infrastructure of high-speed networks ("information superhighways") will transmit video, images, HDTV programming, and huge data files as easily as today's telephone system transmits voice.

Since encryption technology will play an increasingly important role in that infrastructure, the Federal Government must act quickly to develop consistent, comprehensive policies regarding its use. The

Administration is committed to policies that protect all Americans' right to privacy while also protecting them from those who break the law.

Further information is provided in an accompanying fact sheet. The provisions of the President's directive to acquire the new encryption technology are also available. For additional details, call Mat Heyman, National Institute of Standards and Technology, (301) 975-2758.

QUESTIONS AND ANSWERS ABOUT THE CLINTON

ADMINISTRATION'S TELECOMMUNICATIONS INITIATIVE

Q: Does this approach expand the authority of government agencies to listen in on phone conversations?

A: No. "Clipper Chip" technology provides law enforcement with no new authorities to access the content of the private conversations of Americans.

Q: Suppose a law enforcement agency is conducting a wiretap on a drug smuggling ring and intercepts a conversation encrypted using the device. What would they have to do to decipher the message?

A: They would have to obtain legal authorization, normally a court order, to do the wiretap in the first place. They would then present documentation of this authorization to the two entities responsible for safeguarding the keys and obtain the keys for the device being used by the drug smugglers. The key is split into two parts, which are stored separately in order to ensure the security of the key escrow system.

Q: Who will run the key-escrow data banks?

A: The two key-escrow data banks will be run by two independent entities. At this point, the Department of Justice and the Administration have yet to determine which agencies will oversee the key-escrow data banks.

Q: How strong is the security in the device? How can I be sure how strong the security is?

A: This system is more secure than many other voice encryption systems readily available today. While the algorithm will remain classified to protect the security of the key escrow system, we are willing to invite an independent panel of cryptography experts to evaluate the algorithm to assure all potential users that there are no unrecognized vulnerabilities.

Q: Whose decision was it to propose this product?

A: The National Security Council, the Justice Department, the Commerce Department, and other key agencies were involved in this decision This approach has been endorsed by the President, the Vice President, and

appropriate Cabinet officials.

Q: Who was consulted? The Congress? Industry?

A: We have on-going discussions with Congress and industry on encryption issues, and expect those discussions to intensify as we carry out our review of encryption policy. We have briefed members of Congress and industry leaders on the decisions related to this initiative.

Q: Will the government provide the hardware to manufacturers?

A: The government designed and developed the key access encryption microcircuits, but it is not providing the microcircuits to product manufacturers. Product manufacturers can acquire the microcircuits from the chip manufacturer that produces them.

Q: Who provides the "Clipper Chip"?

A: Mykotronx programs it at their facility in Torrance, California, and will sell the chip to encryption device manufacturers. The programming function could be licensed to other vendors in the future.

Q: How do I buy one of these encryption devices?

A: We expect several manufacturers to consider incorporating the "Clipper Chip" into their devices.

Q: If the Administration were unable to find a technological solution like the one proposed, would the Administration be willing to use legal remedies to restrict powerful encryption devices?

A: This is a fundamental policy question which will be considered during the broad policy review. The key escrow mechanism will provide Americans with an encryption product that is more secure, more convenient, and less expensive than others readily available today, but it is just one piece of what must be the comprehensive approach to encryption technology, which the Administration is developing.

The Administration is not saying, "since encryption threatens the public safety and effective law enforcement, we will prohibit it outright" (as some countries have effectively done); nor is the U.S. saying that "every Amen can, as a matter of right, is entitled to an unbreakable commercial encryption product." There is a false "tension" created in the assessment that this issue is an either-or" proposition. Rather, both concerns can be, and in fact are, harmoniously balanced through a reasoned, balanced approach such as is proposed with the "Clipper Chip" and similar encryption techniques.

Q: What does this decision indicate about how the Clinton Administration's policy toward encryption will differ from that of the Bush Administration?

A: It indicates that we understand the importance of encryption technology in telecommunications and computing and are committed to working with industry and public-interest groups to find innovative ways to protect Americans' privacy, help businesses to compete, and

ensure that law enforcement agencies have the tools they need to fight crime and terrorism.

Q: Will the devices be exportable? Will other devices that use the government hardware?

A: Voice encryption devices are subject to export control requirements. Case-by-case review for each export is required to ensure appropriate use of these devices. The same is true for other encryption devices. One of the attractions of this technology is the protection it can give to U.S. companies operating at home and abroad. With this in mind, we expect export licenses will be granted on a case-by-case basis for U.S. companies seeking to use these devices to secure their own communications abroad. We plan to review the possibility of permitting wider exportability of these products.
