THE DIRECTOR OF CENTRAL INTELLIGENCE
WASHINGTON, D.C. 20505

11 September 1996

ACTION

MEMORANDUM FOR THE PRESIDENT
THE VICE PRESIDENT

FROM: JOHN DEUTCH

SUBJECT: Encryption Policy

Purpose

To recommend three actions to promote the development of commercial key recovery encryption products.

Background

In July, Vice President Gore announced that in September, a Cabinet Committee would make recommendations "to encourage the use of strong encryption in electronic commerce and private communication while protecting the public safety and national security."

The use of strong, affordable commercial encryption will grow, along with international electronic commerce. We want U.S. industry to retain its dominant market share by incorporating strong encryption into communications, computer systems and software products. Yet strong encryption can undermine law enforcement and national security by limiting U.S. and other governments' abilities to exploit communications intercepts and access computer files, consistent with the law.

The policy we recommend charts a middle of the road approach that will promote encryption worldwide, but, we hope, limit the negative effects. The heart of the policy is to encourage U.S. industry to adopt an encryption key recovery system. In this system, encryption keys are deposited with certified "trusted parties" either here or abroad, who would provide access to the key for authorized law enforcement purposes. Many end-users, especially large companies, need such a system to manage the keys distributed to their employees.

Our goal is global adoption of such a system. We believe other countries share our public safety concerns and have similar national security concerns. Indeed, if the U.S. were to lift our export controls, several countries, like France, would almost certainly adopt import restrictions on commercial encryption. Although predicting outcomes in this rapidly moving technology is difficult, such restrictions could slow the development of secure international electronic commerce. Thus we believe our allies will welcome our leadership in advancing a middle of the road solution.

At present, there are no domestic controls on encryption. Our principal lever is export controls, which can influence industry because it seeks to develop products that work worldwide. Thus, our proposal would ease export controls in exchange for industry commitment to build key recovery products and supporting infrastructure.

This policy does not satisfy industry, which argues that strong encryption technology without key recovery is already widely available and that its use should be encouraged. Further, building and selling a key recovery infrastructure will take years. Industry wants to export stronger products now, to preserve their market share. The recent National Research Council encryption policy report supports industry's position.

The policy also does not satisfy our law enforcement community, which argues that key recovery should be made mandatory, so that domestic and international law enforcement capability is not eroded. We have rejected the policy option of mandatory control because we believe legislation to ban use of encryption in private communications will not be adopted here or abroad, notably in Germany and Japan. We have also rejected the policy option of doing nothing, because it risks unacceptable decontrol legislation from Congress, would encourage the development of foreign encryption while continuing the constraint on U.S. industry, and ultimately undermine the U.S. Government's ability to influence the development of encryption technology.

We need to act now to minimize the risks to national security and public safety, cut short the widespread use of encryption that is inaccessible to law enforcement, spur the development of key recovery, and assure that U.S. products retain their market dominance worldwide.

As approved by the Vice President in August 1995 we would continue to expand the purchase of key recovery products for U.S. government use, promote key recovery in international discussions, and stimulate the development of innovative key recovery products.

If you agree with this middle of the road approach, three recommendations require your decision:

1. Temporary relaxation of export controls.

We propose to permit the export of 56-bit key length Data Encryption Standard (DES) encryption products, without key recovery, on the same terms as we now permit the export of 40-bit key length products. This relaxation would last two years, renewable annually thereafter. Export licenses would be contingent on exporters' commitment and adherence to explicit benchmarks and milestones for developing and incorporating key recovery into their products (including an identified trusted party) and building the supporting infrastructure internationally. Once key recovery is globally viable, only such products would be licensed for export.

We would consult with industry and monitor progress closely, using licensing regulations and a special government-industry group. We would suspend licenses if milestones were not met.

This approach promotes continued U.S. leadership in secure electronic commerce, increases the chance that key recovery will spread worldwide, and lowers risk to U.S. intelligence collection and law enforcement from use of even stronger, foreign made encryption products. However, there is a risk that this liberalization could create a de facto standard without key recovery that will hamper intelligence and law enforcement in the future.

State, Commerce, Defense, NEC, NSC, and OMB support this proposal, provided that we obtain credible commitments from industry.

Justice opposes this proposal. It believes that we cannot ensure that industry will abide by its commitments, and that there are inadequate incentives for it to do so in the absence of legislation. Therefore, this option will result in the proliferation of strong encryption for an indefinite period. Justice proposes instead that this proposal be refashioned as

legislation that would: (1) permit the export of 56-bit for two years; (2) after two years, permit the export only of key recovery products; and (3) after two years, ban the import [and domestic manufacture, sale or distribution] of encryption that does not have key recovery.

OSTP also opposes the recommendation, arguing that the liberalization will be difficult to retract, especially if foreign companies are selling similar products. OSTP would make the 56-bit liberalization permanent (except for companies that fail to meet their commitments), and focus instead on promoting key recovery for the even stronger encryption products the market will demand.

Proponents' response to Justice: We have administrative authority to implement the first two parts of the Justice proposal. Seeking this legislation would cause unacceptable delay and create unpredictable outcomes. Proponents' response to OSTP: The two-year cap is needed to signal our seriousness about key recovery.

If you agree, we will issue a statement like that at Tab A.

Approve _____

Disapprove _____

2. Transfer encryption export controls from State to Commerce.

The export of encryption is currently controlled by State under the Arms Export Control Act. Industry believes control by Commerce under the Export Administration Act (EAA) is more consistent with encryption's dual-use nature. Industry also views the Commerce licensing process as more predictable, timely and export friendly. The transfer is thus an important carrot to convince industry to promote key recovery.

We would accomplish the transfer through a new Executive Order, which would remedy provisions in the EAA which are inappropriate for encryption, and a Presidential directive. Justice would be included in licensing decisions (currently limited to Commerce, State, Defense, Energy and ACDA). We would also insist that the new EAA being considered by Congress contain protections for encryption (in particular limiting judicial review of export decisions). Jurisdiction would be transferred back to State if the new EAA did not contain such protections.

All agencies and EOP offices support the transfer of jurisdiction, as reflected in the draft EO and PDD at Tabs B and C.

Approve _____

Disapprove _____

3. Key recovery legislation.

We are drafting proposed legislation that will facilitate the development of a market for key recovery products and key management infrastructure, by authorizing:

- The Secretary of Commerce to license key recovery agents;
- Legal conditions for keys to be released to law enforcement;
- Criminal charges for misuse of another's keys;
- Protection of key recovery agents from liability for complying with legal orders to produce keys; and,
- Criminal charges for using encryption in committing a crime.

If you agree, we will refer draft legislation to OMB for interagency review and forwarding to Congress.

Approve _____

Disapprove _____

Attachments

Tab A Draft Encryption Policy Statement
Tab B Draft Presidential Decision Directive
Tab C Draft Executive Order

Attachment A

DRAFT Statement on Encryption Initiative

The Clinton Administration today announced a major initiative to liberalize export controls for commercial encryption products. Under this initiative, the export of 56-bit key length Data Encryption Standard (DES) encryption products will be permitted under a General License after one-time review. The treatment is similar to that currently provided for 40-bit mass market products that use the RC2 and RC4 algorithms. This policy would apply to hardware and software products. The relaxation of controls will last two years.

Exporters will be asked to make commitments to support the development and sale of products that promote the key recovery framework proposed by the Vice President in July 1996. That framework permits encryption users voluntarily to deposit a spare encryption key with a trusted private sector party who would provide the key to the user in an emergency, or to law enforcement officials acting under proper authority.

The temporary relaxation of controls is part of a broader encryption initiative designed to promote electronic information security and key recovery. Export control jurisdiction for commercial encryption products will be transferred from the State Department to the Commerce Department. The Administration also will seek legislation to facilitate the development of a market for key recovery. As announced by the Vice President in July, the government will continue to expand the purchase of key recovery products for U.S. government use, promote key recovery in international discussions, and stimulate the development of innovative key recovery products.

Under the relaxation, export licenses will be issued contingent on commitments from exporters to explicit milestones for developing and incorporating key recovery features into their products and building the supporting infrastructure internationally. The government will monitor progress closely, using licensing regulations and a special government-industry commission. It will suspend licenses if milestones are not met. Once key recovery is globally viable, only such products will be licensed for export.

Specifically, firms wishing to export 56-bit DES products will be required to provide a data recovery product development plan during the licensing process. The plan will:

- address such elements as research and development, testing, production, and marketing;
- include an assessment of the overall market potential for data recovery products and services;
- be updated with a semi-annual progress report; and,
- not be publicly releasable to protect business confidentiality.

In addition, industry representatives will be invited to participate in a joint public-private Data Recovery Infrastructure Commission. The functions of the Commission will include:

- developing alternative approaches for a global data recovery architecture;
- advising the Secretary of Commerce on licensing policy based on progress towards building a global infrastrucuire and lessons-learned from key recovery implementation;
- advising the Attorney General on technical confidence issues vis-a-vis access to escrowed keys.
- identifying other technical, policy, and program issues for governmental action.

The government will reevaluate the relaxation policy at the end of the two year period.

o o o o o .

Questions and Answers about the Encryption Liberalization Initiative

1. Will the US stop the exports of non-key-recovery encryption products at the end of two years?

A: Yes. The plan is to stop exports of any product that does not support key recovery unless unavoidable circumstances delay the creation of the key recovery infrastructure so that it is impractical to sell such products internationally. The government will be advised on this matter by the Data Recovery Infrastructure Commission.

2. Does the two years begin from the date of the new regulation or from the date of the approved export?

A: The two years begins 60[?] days after the effective date of the final regulation. The delay will permit exporters to file applications before the beginning of the two year period.

3. What does it mean to "develop" a key recovery product? Is it sufficient to make the product but not spend funds advertising and marketing the program?

A: Data recovery product development plans will address such elements as research and development, testing, production, and marketing. We are looking for genuine commitments, commensurate with the size of the market involved. The government will suspend licenses if milestones are not met.

4. After two years, will the commitment require that a firm stop domestic sales of products that do not support key recovery?

A: The government has no plans to control the domestic sale of encryption products.

5. If a producer makes a business decision that it cannot afford to enter the market for products that support key recovery, is it fair to stop them from competing for exports on a level playing field with a larger competitor exporting the same encryption product after the larger competitor has given the US a commitment to develop a product?

A: We will require all firms to provide a key recovery product development plan during the export licensing process. While we will take into account the business situation of the individual firms, we believe they will need to incorporate key recovery into their business plans in order to remain competitive.

6. If a reseller or end-user is the exporter, how will the process provide for an opportunity for the product producer to give the necessary commitment? If the software producer does give such a commitment, may other parties export non-escrow products?

A: All exporters will provide a key recovery product development plan as a part of the export licensing process. If the firm is not a product producer, the proposal should either reflect the use of products that are already approved for export, or address plans for marketing and distribution related to products that support key recovery.

ATTACHMENT B

Executive Order No. XXXXX

Administration of Export Controls on Encryption Products

By the authority vested in me as President by the Constitution and the laws of the United States of America, including but not limited to the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.), in order to take additional steps with respect to the national emergency described and declared in Executive Order No. 12924 of August 19, 1994, and continued on August 15, 1995 and on August 14, 1996, I, WILLIAM J. CLINTON, President of the United States of America, find that it is necessary that the provisions set forth below shall apply to administration of the export control system maintained by the Export Administration Regulations, 15 CFR Part 730 et seq. ("the EAR"). Accordingly, it is hereby ordered as follows:

Section 1. Treatment of Encryption Products. In order to provide for appropriate controls on the export and foreign dissemination of encryption products, export controls of encryption products that are or would be, on this date, designated as defense articles designated in Category XIII of the United States Munitions List and regulated by the United States Department of State pursuant to the Arms Export Control Act, 22 U.S.C. 2778 et seq. ("the AECA"), but that subsequently are placed on the Commerce Control List in the EAR, shall be subject to the following conditions:

(a) I have determined that the export of encryption products described in this section may harm national security and foreign policy interests even where comparable products are or appear to be available from sources outside the United States, and that facts and questions concerning the foreign availability of such encryption products cannot be subject to public disclosure or judicial review without revealing or implicating classified information that could harm United States national security and foreign policy interests. Accordingly, sections 4(c) and 6(h)(2)-(4) of the Export Administration Act of 1979 ("the EAA"), 50 App. U.S.C. 2403(c) and 2405(h)(2)-(4), as amended and as continued in effect by Executive Order No. 12924 of August 19, 1994, and by Notices of August 15, 1995 and August 14, 1996, all other analogous provisions of the EAA relating to foreign availability, and the regulations in the EAR relating to such EAA provisions, shall not be applicable with respect to export controls on such encryption products. Notwithstanding this, the Secretary may, in his discretion, consider the foreign availability of comparable encryption products in determining whether to issue a license in a particular case or to remove controls on particular products, but is not required to issue licenses in particular cases or to remove controls on particular products based on such consideration;

(b) In conducting the license review described in section 1 of Executive Order No. 12981 of December 5, 1995, with respect to export controls of encryption products described in this section, the Departments of State, Defense, Energy and Justice and the Arms Control and Disarmament Agency each shall have the opportunity to review any export license application submitted to the Department of Commerce. The Department of Justice shall, with respect to such products, be a voting member of the Export Administration Review Board established in

section 5(a) of Executive Order No. 12981 of December 5, 1995, and of the Advisory Committee on Export Policy established in section 5(b) of that order, and shall be a full member of the Operating Committee established in section 5(c) of that order, and of any other committees and consultation groups reviewing such export controls;

(c) Because the export of encryption software, like the export of other encryption products described in this section, must be controlled because of such software's functional capacity, rather than because of any possible informational value of such software, such software shall not be considered or treated as "technology," as that term is defined in section 16 of the EAA (50 App. U.S.C. § 2415), and in the EAR;

(d) With respect to encryption products described in this section, the Secretary of Commerce shall take such actions, including the promulgation of rules, regulations, and amendments thereto, as may be necessary to control the export of assistance (including training) to foreign persons in the same manner and to the same extent as the export of such assistance is controlled under the AECA (as amended by section 151 of Public Law 104-164); and

(e) Regulation of encryption products described in this section shall be subject to such further conditions as the President may direct.

Sec. 2. Effective Date. The provisions described in section 1 shall take effect as soon as any encryption products described in section 1 are placed on the Commerce Control List in the EAR.

Sec. 3. Judicial Review. This order is intended only to improve the internal management of the executive branch and to ensure the implementation of appropriate controls on the export and foreign dissemination of encryption products. It is not intended to, and does not, create any rights to administrative or judicial review, or any other right or benefit or trust responsibility, substantive or procedural, enforceable by a party against the United States, its agencies or instrumentalities, its officers or employees, or any other person.

THE WHITE HOUSE

William J. Clinton

September , 1996

ATTACHMENT C

Presidential Decision Directive

Encryption products, when used outside the United States, can jeopardize our foreign policy and national security interests. Moreover, such products, when used by international criminal organizations, can threaten the safety of citizens of the United States here and abroad, as well as the safety of the citizens of other countries. The exportation of encryption products accordingly must be controlled to further United States foreign policy objectives, and promote our national security, including the protection of the safety of United States citizens abroad. Nonetheless, because of the increasingly widespread use of encryption products for the legitimate protection of the privacy of data and communications in nonmilitary contexts; because of the importance to United States economic interests of the market for encryption products; and because, pursuant to the terms set forth in Executive Order No. XXXXX of September __, 1996, Commerce Department controls of the export of such dual-use encryption products can be accomplished without compromising United States foreign policy objectives and national security interests, I have determined at this time not to continue to designate such encryption products as defense articles on the United States Munitions List.

Accordingly, under the powers vested in me by the Constitution and the laws of the United States, I direct that:

1. Encryption products that presently are or would be designated in Category XIII of the United States Munitions List and regulated by the United States Department of State pursuant to the Arms Export Control Act (22 U.S.C. 2778 et seq.) shall be transferred to the Commerce Control List, and regulated by the Department of Commerce under the authority conferred in Executive Order No. 12924 of August 19, 1994 (as continued on August 14, 1996), Executive Order No. 12981 of December 5, 1995, and Executive Order No. XXXXX, of September __, 1996; except that encryption products specifically designed, developed, configured, adapted or modified for military applications (including command, control and intelligence applications), shall continue to be designated as defense articles, shall remain on the United States Munitions List, and shall continue to be controlled under the Arms Export Control Act. The transfer described in this paragraph shall be effective upon the issuance of final regulations (the "Final Regulations") implementing the safeguards specified in this Directive and in Executive Order No. XXXXX.

2. The Final Regulations shall specify that the encryption products specified in section 1 shall be placed on the Commerce Control List administered by the Department of Commerce. The Department of Commerce shall, to the extent permitted by law, administer the export of such encryption products, including encryption software, pursuant to the requirements of sections 5 and 6 of the former EAA (50 App. U.S.C. §§ 2405 and 2406), and the regulations thereunder, as continued in effect by Executive Order No. 12924 of August 19, 1994 (continued on August 15, 1995 and on August 14, 1996), except as otherwise indicated in or modified by Executive Order No. XXXXX of September __, 1996, Executive Order No. 12981 of December 5, 1995, and any executive orders and laws cited therein.

3. The Final Regulations shall provide that encryption products described in section 1 can be licensed for export only if the requirements of the controls of both sections 5 and 6 of the former EAA (50 App. U.S.C. §§ 2405 and 2406), and the regulations thereunder, as modified by Executive Order No. XXXXX of September __, 1996, Executive Order No. 12981 of December 5, 1995, and any executive orders and laws cited therein, are satisfied. Consistent with § 742.1(f) of the current Export Administration Regulations, the Final Regulations shall ensure that a license for such a product will be issued only if an application can be and is approved under both section 5 and section 6. The controls on such products will apply to all destinations. Except for those products transferred to the Commerce Control List prior to the effective date of the Final Regulations, exports and reexports of encryption products shall initially be subject to case-by-case review to ensure that export thereof would be consistent with United States foreign policy objectives and national security interests, including the safety of United States citizens. Consideration shall be given to more liberalized licensing treatment for each such individual product after interagency review is completed. The Final Regulations shall also effectuate all other specific objectives and directives set forth in this Directive.

4. Because encryption source code can easily and mechanically be transformed into object code, and because export of such source code is controlled because of the code's functional capacity, rather than because of any "information" such code might convey, the Final Regulations shall specify that encryption source code shall be treated as an encryption product, and not as technical data or technology, for export licensing purposes.

5. All provisions in the Final Regulations regarding "de minimis" domestic content of items shall not apply with respect to the encryption products described in paragraph 1.

6. The Final Regulations shall, in a manner consistent with section 16(5)(C) of the EAA, 50 App. U.S.C. 2415(5)(C), provide that it will constitute an export of encryption source code or object code software for a person to make such software available for transfer outside the United States, over radio, electromagnetic, photooptical, or photoelectric communications facilities accessible to persons outside the United States, including transfer from electronic bulletin boards and Internet file transfer protocol sites, unless the party making the software available takes precautions adequate to prevent the unauthorized transfer of such code outside the United States.

7. Until the Final Regulations are issued, the Department of State shall continue to have authority to administer the export of encryption products described in section 1 as defense articles designated in Category XIII of the United States Munitions List, pursuant to the Arms Export Control Act.

8. Upon enactment of any legislation reauthorizing the administration of export controls, the Secretary of Defense, the Secretary of State, and the Attorney General shall reexamine whether adequate controls on encryption products can be maintained under the provisions of the new statute, and advise the Secretary of Commerce of their conclusions as well as any recommendations for action. If adequate controls on encryption products cannot be maintained under a new statute, then such products shall, where consistent with law, be

designated or redesignated as defense articles under 22 U.S.C. 2778(a)(1), to be placed on the United States Munitions List and controlled pursuant to the terms of the Arms Export Control Act and the International Traffic in Arms Regulations. Any disputes regarding the decision to so designate or redesignate shall be resolved by the President.