April 16, 1993
Washington, DC

COMPUTER PROFESSIONALS CALL FOR PUBLIC
DEBATE ON NEW GOVERNMENT ENCRYPTION INITIATIVE

Computer Professionals for Social Responsibility (CPSR) today called for the public disclosure of technical data underlying the government's newly-announced "Public Encryption Management" initiative. The new cryptography scheme was announced today by the White House and the National Institute for Standards and Technology (NIST), which will implement the technical specifications of the plan. A NIST spokesman acknowledged that the National Security Agency (NSA), the super-secret military intelligence agency, had actually developed the encryption technology around which the new initiative is built.

According to NIST, the technical specifications and the Presidential directive establishing the plan are classified. To open the initiative to public review and debate, CPSR today filed a series of Freedom of Information Act (FOIA) requests with key agencies, including NSA, NIST, the National Security Council and the FBI for information relating to the encryption plan. The CPSR requests are in keeping with the spirit of the Computer Security Act, which Congress passed in 1987 in order to open the development of non-military computer security standards to public scrutiny and to limit NSA's role in the creation of such standards.

CPSR previously has questioned the role of NSA in developing the so-called "digital signature standard" (DSS), a communications authentication technology that NIST proposed for government-wide use in 1991. After CPSR sued NIST in a FOIA lawsuit last year, the civilian agency disclosed for the first time that NSA had, in fact, developed that security standard. NSA is due to file papers in federal court next week justifying the classification of records concerning its creation of the DSS.

David Sobel, CPSR Legal Counsel, called the administration's apparent commitment to the privacy of electronic communications, as reflected in today's official statement, "a step in the right direction." But he questioned the propriety of NSA's role in the process and the apparent secrecy that has thus far shielded the development process from public scrutiny. "At a time when we are moving towards the development of a new information infrastructure, it is vital that standards designed to protect personal privacy be established openly and with full public participation. It is not appropriate for NSA -- an agency with a long tradition of secrecy and opposition to effective civilian cryptography -- to play a leading role in the development process."

CPSR is a national public-interest alliance of computer industry professionals dedicated to examining the impact of technology on society. CPSR has 21 chapters in the U.S. and maintains offices in Palo Alto, California, Cambridge, Massachusetts and Washington, DC. For additional information on CPSR, call (415) 322-3778 or e-mail <cpsr@csli.stanford.edu>.

Article: 15318 of sci.crypt
Newsgroups: sci.crypt,alt.privacy,comp.org.eff.talk,alt.security,alt.dcom.telecom
Path:
agate!usenet.ins.cwru.edu!gatech!emory!sol.ctr.columbia.edu!eff!coolidge.eff.org!Banisar
From: Dave Banisar <Banisar@washofc.cpsr.org>

Subject: CPSR Statement on White House Crypto Plan
Message-ID: <1993Apr16.214751.28995@eff.org>
X-Xxmessage-Id: <A7F4A1214F01AC81@coolidge.eff.org>
X-Xxdate: Fri, 16 Apr 93 17:45:05 GMT
Sender: usenet@eff.org (NNTP News Poster)
Nntp-Posting-Host: coolidge.eff.org
Organization: CPSR, Civil Liberties and Computing Project
X-Useragent: Nuntius v1.1.1d17
Date: Fri, 16 Apr 1993 21:47:51 GMT
Lines: 60
Xref: agate sci.crypt:15318 alt.privacy:6288 comp.org.eff.talk:16996
alt.security:10210 alt.dcom.telecom:1781

April 16, 1993
Washington, DC

COMPUTER PROFESSIONALS CALL FOR PUBLIC
DEBATE ON NEW GOVERNMENT ENCRYPTION INITIATIVE

Computer Professionals for Social Responsibility (CPSR) today called for the public disclosure of technical data underlying the government's newly-announced "Public Encryption Management" initiative. The new cryptography scheme was announced today by the White House and the National Institute for Standards and Technology (NIST), which will implement the technical specifications of the plan. A NIST spokesman acknowledged that the National Security Agency (NSA), the super-secret military intelligence agency, had actually developed the encryption technology around which the new initiative is built.

According to NIST, the technical specifications and the Presidential directive establishing the plan are classified. To open the initiative to public review and debate, CPSR today filed a series of Freedom of Information Act (FOIA) requests with key agencies, including NSA, NIST, the National Security Council and the FBI for information relating to the encryption plan. The CPSR requests are in keeping with the spirit of the Computer Security Act, which Congress passed in 1987 in order to open the development of non-military computer security standards to public scrutiny and to limit NSA's role in the creation of such standards.

CPSR previously has questioned the role of NSA in developing the so-called "digital signature standard" (DSS), a communications authentication technology that NIST proposed for government-wide use in 1991. After CPSR sued NIST in a FOIA lawsuit last year, the civilian agency disclosed for the first time that NSA had, in fact, developed that security standard. NSA is due to file papers in federal court next week justifying the classification of records concerning its creation of the DSS.

David Sobel, CPSR Legal Counsel, called the administration's apparent commitment to the privacy of electronic communications, as reflected in today's official statement, "a step in the right direction." But he questioned the propriety of NSA's role in the process and the apparent secrecy that has thus far shielded the development process from public scrutiny. "At a time when we are moving towards the development of a new information infrastructure, it is vital that standards designed to protect personal privacy be established openly and with full public participation. It is not appropriate for NSA -- an agency with a long tradition of secrecy and opposition to effective civilian cryptography -- to play a leading role in the development process."

CPSR is a national public-interest alliance of computer industry professionals dedicated to examining the impact of technology on society. CPSR has 21 chapters in the U.S. and maintains offices in Palo Alto, California, Cambridge, Massachusetts and Washington, DC. For additional information on CPSR, call (415) 322-3778 or e-mail <cpsr@csli.stanford.edu>.