PREPARED TESTIMONY

AND

STATEMENT FOR THE RECORD

OF

MARC ROTENBERG

DIRECTOR, WASHINGTON OFFICE

COMPUTER PROFESSIONALS FOR

SOCIAL RESPONSIBILITY (CPSR)

ON

THE COMPUTER SECURITY ACT OF 1987 (P.L. 100-235) AND THE MEMORANDUM OF UNDERSTANDING BETWEEN THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) AND THE NATIONAL SECURITY AGENCY (NSA)

BEFORE

THE SUBCOMMITTEE ON LEGISLATION AND NATIONAL SECURITY,

COMMITTEE ON GOVERNMENT OPERATIONS

U.S. HOUSE OF REPRESENTATIVES

MAY 4, 1989

Mr. Chairman, members of the Committee, thank you for the opportunity to testify today on the implementation of the Computer Security Act. I am testifying on behalf of Computer Professionals for Social Responsibility (CPSR), a national membership organization of computer scientists. CPSR has reviewed a number of federal computing proposals, including a detailed assessment of the proposed expansion of the FBI's record system for Congressman Don Edwards.

I would like to thank you for convening this hearing. In our letter to the Committee earlier this month, we emphasized that vigorous oversight would be necessary for successful implementation of the Computer Security Act. We are very pleased that you have undertaken this hearing.

You have asked me to review the Memorandum of Understanding between NIST and NSA and to determine whether it complies with the spirit and intent of the Computer Security Act.[1] To answer that question it is necessary to look at the history of the Act and the record established by this Committee.

THE IMPORTANCE OF THE COMPUTER SECURITY ACT

The central computer security question in the last two Congresses was whether responsibility for the security and privacy

[1] "Memorandum of Understanding Between the Director of the National Institute of Standards and Technology and the Director of the National Security Agency Concerning the Implementation of Public Law 100-235" (signed March 23, 1989); Public Law No. 100-235, 1988 U.S. Code Congressional and Administrative News (100 Stat.) 1724.

of information stored in government computer systems should be entrusted to a civilian agency or an intelligence agency.

In 1984, the President had issued a National Security Decision Directive, NSDD-145, which gave the intelligence agencies broad authority to peruse computer databases, for so-called "sensitive but unclassified information."2 A subsequent memorandum from John Poindexter, expanded this authority still further to include "all computer and communications security for the Federal Government and private industry."3 As the government's authority to control access to computerized information for the purpose of protecting national security expanded, the free of flow of information diminished.4 Stories of agents visiting private information vendors and public libraries soon followed.5 At the same time, a wide range of other

---

2 "National Policy on Telecommunications and Automated Information Systems Security" (September 17, 1984).

3 The memorandum, NTISSP No. 2 "Policy for Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Systems," was eventually rescinded. David Sanger, "Rise and Fall of U.S. Data Directive," The New York Times, March 19, 1987.

4 See generally Jerry J. Berman, "National Security vs. Access to Computer Databases: A New Threat to Freedom of Information," 2 Software Law Journal 1 (1987).

5 Bob Davis, "Federal Agencies Press Data-Base Firms to Curb Access to 'Sensitive' Information," The Wall Street Journal, January 28, 1987, Judith Axler Turner, "Pentagon Planning to Restrict Access to Public Data Bases," The Chronicle of Higher Education, January 21, 1987; Connie Oswald Stofko, "Inquiry by FBI Causes Libraries to Assess Records, SUNY Reporter, February 12, 1987. The NSA also approached election officials and investigated computerized vote-counting software. Burnham, "US Examines if

activities by the government further threatened to restrict access to information.6

Many organizations opposed these efforts. Mead Data Central warned that such "restrictive and unwarranted policies" threatened not only the information industry, but many sectors of the economy, "including legal, financial, government, medical, and the scientific and technological community."[7] The IEEE stated that the "unabridged dissemination of unclassified scientific and technical information is crucial for the continued advancement of US industry."[8] The American Bankers Association expressed concern that NSA encryption technologies would be ill-suited for the private sector and criticized the failure of NSA to recertify the

---

Computer Used in '84 Elections is Open to Fraud," The New York Times, September 24, 1985, at A17.

6 See American Library Association, Less Access to Less Information by and about the U.S. Government (1988); Steven L. Katz, "National Security Controls, Information, and Communications in the United States," 4 Government Information Quarterly 63 (1987); People For the American Way, Government Secrecy: Decisions without Democracy (1987); John Shattuck & Muriel Morisey Spence, Government Information Controls: Implications for Scholarship, Science and Technology, excerpted in "When Government Controls Information," 91 Technology Review 62 (April 1988).

7 House Committee on Science, Space, and Technology, H.R. Rep. No. 153, pt. 1, 100th Cong., 1st Sess. 18 (1987) [the "Science Committee Report"], reprinted in 1988 U.S. Code Congressional and Administrative News 3133 ["1988 U.S.C.A.N."] (Statement of Jack W. Simpson, President, Mead Data Central).

8 Science Committee Report at 19, reprinted in 1988 U.S.C.A.N. 3134 (statement of John M. Richardson, Chairman, Committee on Communications and Information Policy, Institute of Electrical and Electronic Engineering).

public key cryptography standard DES.[9] The American Library Association identified a threat to intellectual freedom and adopted a resolution calling for the repeal of the new security directive.[10] And Jerry Berman, with the ACLU, in testimony before this Committee, warned of the dangers of unleashing the NSA to patrol computers. He said:

> There are good reasons for current limitations and why we should worry about whether they are being eroded by NSDD-145. NSA operates outside the normal accountability channels which control other agencies of government. It has no legislated charter. Its existence was not acknowledged until 1962.[11]

This Committee, already in the process of reviewing federal computer standards, made clear its opposition to the NSA's activities, through letters, statements, and a comprehensive hearing record. Chairman Brooks said that NSDD-145 was "one of the most ill-advised and potentially troublesome directives ever issued by a President" and warned that a new form of government censorship would result if a secret intelligence agency was responsible for computer security throughout the federal

---

[9] Computer Security Act of 1987: Hearings on H.R. 145 Before a Subcommittee of the Committee on Government Operations, House of Representatives, 100th Cong., 1st Sess. 113-14 (the "Hearings") (statement of Cheryl W. Helsing), Science Committee Report at 19, reprinted in 1988 U.S.C.A.N. 3133.

[10] Id. at 550-51.

[11] Hearings at 104. See generally U.S. Senate, Select Committee to Study Governmental Operations with Respect to Intelligence Agencies (1976), James Bamford, The Puzzle Palace (1983), David Burnham, The Rise of the Computer State 118-44 (1983), Morton H. Halperin, Jerry J. Berman, et al., The Lawless State 171-86 (1976)

government.[12] Congressman Glickman, the sponsor of the bill which became the Computer Security Act, stated that there was a fundamental problem with "any directive that affected virtually all civil agencies of government and that had been issued without any public comment."[13] Congressman English stressed that the "insatiable desire of the military for controlling information" was the most convincing argument for legislation.[14]

In short, there was a widely shared belief, based on experience and public policy considerations, that the National Security Agency was the wrong agency to set computer security standards for the federal government.

In passing the Computer Security Act, Congress decided that a civilian agency, the National Institute of Standards and Technology, would be responsible for computer security. NIST was already authorized under the Brooks Act to set standards for computer systems, and had been working on computer standards since the early 1960s when it helped develop the widely used encryption program, DES. And, unlike the NSA, NIST had a good reputation with the private sector.[15]

Congress recognized that there were computer systems operated

---

12 Hearings at 525, 526.

13 Id. at 456.

14 Id. at 23.

15 Id. at 320, reprinted in Government Operations Committee Report at 12, reprinted in 1988 U.S.C.A.N. 3164 (statement of Robert H. Courtney).

in military and intelligence agencies that may pose special or unique problems, requiring NSA technical guidelines. But Congress went to great lengths to spell out these systems, citing statutes, detailing procedures, and avoiding such phrase as "sensitive but unclassified," or "national security," that were overly broad or easily misconstrued.

Thus, on the central question of which agency was responsible for computer security in the federal government, the intent of Congress is unambiguous; the Act stated that "the National Bureau of Standards shall have the mission of developing standards, guidelines, and associated methods and techniques for computers systems."[16]

Since the passage of the Act, NIST has been working to implement the requirements of the Act, reviewing agency security plans, conducting open meetings, and initiating research on computer standards.[17] About a month ago, NIST and NSA signed a Memorandum of Understanding. The central question before the Committee now is whether the M.O.U. is consistent with the Act passed by Congress and signed by the President.

INCONSISTENCIES BETWEEN THE M.O.U. AND THE COMPUTER SECURITY ACT

A Memorandum of Understanding between two agencies should

---

16 § 3, 15 U.S.C. § 278g-3(a)(1).

17 Kevin Power, "NIST Sets Security Review Deadline," Government Computer News, November 21, 1988, at 97; Kevin Power, "Analysts Prepare to Review Agency Security Plans," Government Computer News, January 9, 1989, at 81.

clarify the responsibilities of each agency, the methods in which each agency will undertake its assignments, in a manner that is consistent with the authorizing legislation. The M.O.U. fails this threshold test.

- It transfers the authority to establish and review computer standards from the NIST to the NSA;
- It undermines the authority of the Advisory Board, established by the Act;
- It creates a new layer of national security review;
- It invites the NSA to enter the offices of private information companies and government contractors;
- It revives many of the problems arising from the phrase "sensitive but unclassified";
- It grants NSA the opportunity to review all matters of cryptography undertaken by NIST.

Instead of resolving issues left open by the Act, such as the status of NSDD-145, it undermines the Act, transferring authority that Congress intended to remain at the Commerce Department to Fort Meade.

Under the Act, Congress made clear that NIST would be responsible for federal computer security. The language is straightforward and consistent. The preamble states: "To provide for a computer standards program within the National Bureau of

Standards."[18] The amendments to the NIST organic act say: "The National Bureau of Standards shall have the mission of developing standards, guidelines and associated methods and techniques for computer systems;"[19] the NIST has "the responsibility within the Federal Government for developing . . . standards and guidelines for the cost effective security and privacy of sensitive information in Federal computer systems." [20] The amendments to the Brooks Act state that:

> The Secretary of Commerce shall, on the basis of Standards and guidelines developed by that National Bureau of Standards . . . promulgate standards and guidelines pertaining to federal computer systems, making such standards compulsory and binding to the extent to which the Secretary determines necessary to improve th efficiency of operation or security and privacy of Federal computer systems.[21]

NSA was given an advisory role, to offer "technical advice and assistance," where appropriate.[22] NSA retained authority only over those computer systems that were exempted under the statute. These systems were indicated explicitly by reference to statute or

---

18 The Computer Security Act, preamble, 101 Stat. 1724 (1988).

19 Id. § 3, 15 U.S.C. § 278g-3(a)(1).

20 Id. § 3, 15 U.S.C. § 278g-3(a)(3).

21 Id. § 4, 40 U.S.C. § 759 note.

22 Id. § 4, 40 U.S.C. § 759 note. See id. § 3, 15 USC § 278g-3(c)(2).

to established procedures specifically authorized under criteria established by Executive order or an act of Congress.[23]

In passing the Computer Security Act, Congress did not create a joint venture. The NSA is one of many agencies that is expected to work with NIST to help implement the Act. Under the Act, NIST is authorized to coordinate closely with other agencies, including the Departments of Defense and Energy, the General Accounting Office, the Office of Technology Assessment, and the Office of Management and Budget.[24] The Office of Personnel Management is also required to issue regulations prescribing the procedures for computer system security training, based on guidelines developed by NIST.[25]

The Administration, in endorsing passage of the Computer Security Act, also made clear that it expected NIST to be responsible for computer standards and for NSA to provide assistance, as NIST saw fit. A letter from OMB Director Jim Miller stated that:

---

23 See id. § 3, 15 U.S.C. 278g-3(a)(3)

24 Id. § 3.

25 Id. § 6, 40 U.S.C. 759 note.

> Computer security standards, like other computer standards, will be developed in accordance with established NBS procedures. In this regard the technical security guidelines provided by NSA to NBS will be treated as advisory and subject to appropriate NBS review.[26]

But the M.O.U. cedes NIST standard-setting authority to the NSA. Instead of providing technical advice and assistance, as required by the Act, NSA is now setting the rules. The M.O.U. requires NIST to recognize "the NSA-certified rating of evaluated trusted systems under the Trusted Computer Security Evaluation Criteria without requiring additional evaluation."[27] This is the so-called Orange Book, developed by the NSA, that sets out the different levels of security for computer systems.

This Committee and witnesses who testified at the hearings raised serious doubts about the Orange Book.[28] The Office of Technology Assessment also questioned whether the Orange Book standards would be appropriate for the diverse needs of the federal government.[29] In fact, these guidelines could be fundamentally at odds with our system of open government.

---

26 Government Operations Committee Report at 37, reprinted in 1988 U.S.C.A.N. 3189 (letter to Congressman Brooks); Science Committee Report at 41, reprinted in 1988 U.S.C.A.N. 3156 (letter to Congressman Roe).

27 The M.O.U. at 2.

28 Government Operations Committee Report at 26, reprinted in 1988 U.S.C.A.N. 3178. "Their guidance is not even accepted by the major data processing operations within NSA," Hearings at 313-21 (statement of Robert Courtney).

29 Office of Technology Assessment, Defending Secrets, Sharing Data 117-127 (1987) (Charles K. Wilk, Project Director) [the "OTA Report"].

According to a paper titled "A Comparison of Commercial and Military Computer Security Policy," cited in the OTA Report, "military security policy is really a set of policies designed to control classified information from unauthorized disclosure or disclassification."[30]

Have those concerns been answered? Has NIST made a determination that the Orange book standards are consistent with the needs of civilian agencies? Is there a publicly reviewable record that explains the basis for this decision? Does the Advisory Board endorse this outcome?

More surprising is that the M.O.U. restricts the NIST from any prospective review of computer security standards. This provision is not only at odds with the intent of the Act, but will undermine efforts to enhance computer security. Innovation is critical for the development of new information security technologies.[31]

There is a legitimate concern about the development of different computer standards for federal computer systems. Congress recognized that it could be inefficient and costly. Computer manufacturers also did not want to develop computer

---

30 OTA Report at 117, citing David D. Clark, MIT Laboratory for Computer Science, and David R. Wilson, Ernst & Whinney.

31 OTA Report at 6. This provision also suggests the cost that secrecy imposes on scientific innovation. See, e.g., Robert L. Park, "Science and Secrecy," Bulletin of Atomic Scientists, March, 1985, at 22. See Harold Willenbock, "Information Controls and Technological Progress," Issues in Science and Technology, Fall 1986, at 88. See generally National Academy of Sciences, Scientific Communications and National Security (1982)

systems for the federal government with two different sets of standards. For this reason the Act required that standards NIST developed be "consistent and compatible" with existing standards for the protection of properly classified systems.[32] But Congress considered and explicitly rejected the proposition that NSA should have authority for developing technical guidelines:

> Since work on technical security standards represents virtually all of the research effort being done today, NSA would take over virtually the entire computer standards from the National Bureau of Standards. By putting NSA in charge of developing technical security guidelines (software, hardware, communications), NBS would be left with the responsibility for only administrative and physical security measures -- which have generally been done years ago. NBS, in effect, would on the surface be given the responsibility for the computer standards program with little to say about the most important part of the program -- the technical guidelines developed by NSA.[33]

It was clearly not the intent of Congress that NIST should become a clearinghouse for NSA's technical standards.

Second, the M.O.U. will undermine the Computer System Security and Privacy Advisory Board established by the Act. This Advisory Board is responsible for identifying emerging issues, advising NIST and the Secretary of Commerce, and reportings its findings to Commerce, OMB, NSA, and the Oversight Committees.[34]

---

[32] § 3, 15 U.S.C. § 278g-3(b)(6)(B).

[33] Government Operations Committee Report at 25-26, reprinted in 1988 U.S.C.A.N. 3177-78. See also Science Committee Report at 27, reprinted in 1988 U.S.C.A.N. 3142.

[34] § 3, 15 U.S.C. § 278g-4(b) (duties).

Under the Act, the Board is made up of leading representatives from the computer and telecommunications industry, the federal government and independent contractors; the Secretary of Commerce selects the Chair of the Board.[35] The purpose of the Board is to ensure that NIST "receives qualified input from those likely to be affected by its standards and guidelines, both in government and the private sector."[36] The American Bankers Association testified that "one of the most important aspects" of the bill "is the establishment of a formal mechanism for private sector communication and cooperation with the Federal Government."[37]

The M.O.U. sets forth a different mechanism. It is a Technical Working Group that will review computer security issues.[38] It is headed by the NSA Deputy Director for Information Security and the NIST Deputy Director. Nowhere, in the M.O.U., is the relationship between the Working Group and the Advisory Board described.

There are three potential problems with this procedure. First, it is likely to divert issues to the Technical Working Group that should properly be considered by the Advisory Group. Second, creating a joint NSA-NIST committee for matters involving

---

35 § 3, 15 U.S.C. § 278g-4(a).

36 Science Committee Report at 27, reprinted in 1988 U.S.C.A.N. 3142. See also Government Operations Committee Report at 40, reprinted in 1988 U.S.C.A.N. 3192.

37 Hearings at 114 (statement of Cheryl W. Helsing).

38 The M.O.U. at 3-4.

unclassified computer systems is inconsistent with the roles assigned NIST and NSA under the Act. Third, because of the authority granted to the NSA Deputy Director under the M.O.U., the NSA could easily control the agenda of this working group. In effect, the M.O.U. allows NSA to refer any issue at any time to the working group for resolution within 14 days. This is simply not a sensible ways to ensure NIST authority when the resources of NSA far exceed NIST.

Third, the M.O.U. creates a new layer of national security review. Under the M.O.U., "all matters regarding technical systems security techniques" must be reviewed, prior to public disclosure, to ensure that they are consistent with "national security."[39] In the words of Chairman Brooks, this procedure will shift decisions about computer security standards to "the basement of the White House and the back rooms of the Pentagon."[40]

The framers of the Act provided a mechanism for review, but after the rules had been made public. This was purposeful. It was intended to avoid pre-publication review, and to strengthen the wall protecting the decision-making authority of the Commerce Department so as to prevent the national security administration from crawling in over the top. The procedure in the M.O.U. for National Security Council review effectively dismantles this safeguard.

---

39 Id.

40 Hearings at 2.

Fourth, the M.O.U. breathes new life into NSDD-145. According to the M.O.U., the NSA will:

> Upon request by Federal agencies, their contractors and other government-sponsored entities, conduct assessments of the hostile intelligence threat to federal information systems, and provide technical assistance and recommend endorsed products for application to secure systems against the threat.[41]

This is NSDD-145, part two. Will it have Congressional blessing? This language invites the National Security Agency back into the offices of information vendors to provide government security systems or to restrict access to electronic information. This was one of the key concerns that led to adoption of the Computer Security Act.[42] Recall the statement of Assistant Secretary of Defense Donald Latham, chairman of NTISSC, who said:

> I'm very concerned about what people are doing--and not just the Soviets. If that means putting a monitor on NEXIS type systems, I'm for it. The question is, how do you do that technically without interference?[43]

The private sector responded that it was not the Kremlin they worried about, but their business competitors. But the M.O.U. resurrects the "hostile intelligence threat"[44] and leaves open the possibility that the government may very well put monitors on

---

41 The M.O.U. at 3.

42 See, e.g., "Are Data Bases a Threat to National Security?" BusinessWeek, December 1, 1986, at 39.

43 The Washington Post, May 27, 1986.

44 The M.O.U. at 3.

computer systems.

There is another aspect of this clause that is troubling. While it seems to restrict the ability for the NSA to visit purely "private" companies, it leaves open the possibility that any federal agency could request that the NSA undertake an assessment of any information system maintained by a federal contractor. Such a procedure will undercut NIST's authority for computer security and could be an open license for government surveillance of computer systems throughout the country.

The Act created a mechanism for the NSA to raise national security concerns. An NSA representative serves as a member of the Advisory Board. That is the appropriate place to discuss these questions.

Fifth, the efforts that Congress made to delineate the computer systems covered under the Act are largely swept aside by the language of the M.O.U.. In drafting the Act, Congress purposefully rejected the phrase "sensitive, but unclassified" and avoided the term "national security," fearing that this term would confuse the responsibilities of the NIST and the NSA. It used the term "public interest" to describe the President's authority to reject standards. It exempted from the Act those systems where information must be kept secret in the interest of "national defense" or "foreign policy." In part, and in whole, these choices show the determination of Congress to avoid the open-ended

trap of national security designations.[45] However, the M.O.U. ignores these decisions by Congress and says flatly that all systems must be reviewed to "ensure they are consistent with the national security of the United States."[46]

It is also important to understand how the critical term "sensitive" is used in the Act. It does not create another category of restricted information.[47] It is used to underscore the importance of the information, and the risks that might result, such as loss of life or violation of personal privacy, if the information were modified, destroyed or disclosed.[48] In effect, it was to operate as a triggering mechanism, to help agency administrators distinguish between systems that might contain records on individuals and systems that were designed to be widely accessible, such as computerized bulletin boards.

The M.O.U. distorts this view of information protection and returns to the "sensitive but unclassified" approach of NSDD-145 and the Poindexter memorandum. It treats sensitive information as information that must be controlled, for which access may be restricted. This is how information security is viewed by

---

45 See Harold C. Relyea, "National Security and Information," 4 Government Information Quarterly 11 (1987).

46 The M.O.U. at 3-4.

47 Government Operations Committee Report at 24, 31, reprinted in 1988 U.S.C.A.N. 3176, 3183.

48 Science Committee Report at 21, reprinted in 1988 U.S.C.A.N. 3136.

intelligence agencies.[49] This approach to computer security could drape the entire federal government under a veil of national security review.

This is not simply at odds with the Computer Security Act, but also with the Freedom of Information Act, the law which establishes a fundamental right for citizens in the United States to have access to the records of government. It is the statute that preserves our open system of government and prevents the government from erecting barriers against its citizens. Congress anticipated this problem and added a section to the bill to make sure that computer security legislation would not erode the principles underlying the Freedom of Information Act.[50]

A final question Mr. Chairman, what exactly did NIST and the NSA intend to accomplish by adoption of this M.O.U.? Presumably, it was to ensure the faithful compliance with Act. But even this is not clear. The M.O.U. states that NIST and the NSA will:

> Work together to achieve the purposes of the memorandum with the greatest efficiency possible, avoiding unnecessary duplication of effort.[51]

If this M.O.U. is the basis for NIST-NSA cooperation for computer security, then the starting point must be a commitment to work

---

49 See OTA Report at 117.

50 § 8. See also statement of the President, 24 Weekly Compilation of Presidential Documents 10, January 11, 1988, reprinted in 1988 U.S.C.A.N. 3197-1 (January 8, 1988).

51 The M.O.U. at 3 [emphasis added].

together to achieve the purposes of the Act, as passed by Congress.

As it currently stands, the M.O.U. is directly at odds with the plain language of the Computer Security Act. Is this significant? Could the Committee simply say: that's not really what we intended, but, in comparison to NSDD-145, "sensitive but unclassified," and some of the other problems that led to passage of the Act, this may not be so pressing. The answer to that question is no. If it was important to pass the legislation, then it is important to see that it is implemented as Congress intended.

THE CONSEQUENCES OF IMPLEMENTING THE M.O.U.

The Memorandum of Understanding will have significant consequences for both the free flow of information and the type of security protection established by the federal government.

A. Impact on Access to Information

Less than three years ago, the Director for Information Systems for the Department of Defense, said:

> I don't believe that the issue is whether or not we're going to protect information, I believe that the issue is what information we're going to protect both within the Federal Government, both within DOD and also within industry.[52]

I believe, after reviewing the M.O.U., that NSA intends to make good on its promise. If left in place, this M.O.U. will restrict access to information for Congress, for information vendors and government contractors, and for the general public.

1. The Congress

Congress will require access to particular information about the conduct of the agencies to assess the program, and to determine when changes are necessary, and to appropriate adequate funds to get the job done. Without adequate oversight, there can be no assurance that the goals of the act will be achieved.

But if the Technical Working Group is left in place, then Congress may be denied access to information necessary to assess the progress of computer security. Under the M.O.U., the NSA will be able to appeal any proposed standards to the National Security Council, prior to publication. What happens when the NSC rules that certain standards may not be adopted? How will Congress find out? Under the Act, there is a clear mechanism for notifying the oversight committees if the President rejects a standard.[53]

---

52 Government Operations Committee Report at 15, reprinted in 1988 U.S.C.A.N. 3167. "Are Data Bases a Threat to National Security?" BusinessWeek, December 1, 1986, at 39.

53 § 4, 40 U.S.C. § 759(d)(1).

Absent a similar procedure for the Technical Working Group, this preliminary review may place the whole process of developing computer standards for the federal government behind the drawn curtain of national security.

2. Impact on Information Vendors and Government Contractors

Mead Data Central is one of the largest vendors of computer-based information in the world. It has over 200,000 customers and maintains more than 47 million full-text documents. Yet, in 1987, Mead Data Central reported to this Committee that it had removed the National Technical Institute Service (NTIS) file from its system. Although it cited economic and policy reasons for the decision, it is hard to escape the conclusion that, but for the pressure brought to bear by NSDD-145, that service would be available today.

What will happen when a smaller information vendor, a government contractor, or a government-sponsored organization, is approached by officials from Ft. Meade, notified of a potential hostile intelligence threat, and asked whether it would like NSA's assistance in improving computer security? What databases will then be removed? And how will Congress or anyone else know about actions taken by intelligence agencies under the banner of "national security"?

3. Impact on the public

The impact on the public of government restrictions on access to information has been widely documented.[54] Efforts to expand national security authority chill speech, restrict intellectual inquiry, hinder economic trade, constrain scientific innovation, and undermine open government.

If, under the M.O.U., the Congress is not able to obtain the information necessary to oversee the Act and information companies face possible new restrictions, what is the likely impact on the free flow of information for the general public? That is, of course, the central test for the implementation of the Act.

B. Impact on Protection of Information

Considering the history of NSDD-145 and the Poindexter memo,[55] the potential impact of the M.O.U. on the free flow of information is one way to assess whether the M.O.U. should be left unchanged; the other is whether the M.O.U. will establish security and privacy practices consistent with the Act.

The security goals of a civilian agency are often different than those of a military agency.[56] Emphasizing the computer security interest, as defined by the National Security Agency, could, in fact, undermine both the management goals and the privacy interests the Act seeks to protect.

---

54 See note 6 and accompanying text.

55 See notes 2-14 and accompanying text.

56 See notes 29-31 and accompanying text.

Effective computer security plans should be built around solid-management practices, not gold-plated technologies. In a report for Congressman Don Edwards on the proposed expansion of the FBI's record system, CPSR members wrote:

> Advances in computer technology can be used to improve security, accountability, and data quality. But system administrators and managers carry the ultimate responsibility to ensure that the system is well designed and properly maintained.[57]

Technical guidelines should follow from organizational requirements. But shifting authority from NIST to NSA may undermine this fundamental goal of information security.

One of the primary reasons for concern about the security of federal computer systems is the large amount of personal information held by the federal government. We need assurance from the government that information will be properly maintained, that it will not be used a reason other than for which it was collected. As the Supreme Court stated recently in the Reporter's Committee case "a centralized computer file pose[s] a 'threat to privacy'."[58] The misuse of personal information contained in government computer systems will have harmful consequences.[59]

---

57 Horning, Neumann, Redell, Goldman & Gordon, "A Review of NCIC 2000" (1989).

58 Department of Justice v. Reporters Committee for Freedom of the Press, No, 87-1379, slip. op. at 20 (decided March 22, 1989).

59 See generally David Burnham, The Rise of the Computer State (1983), Kenneth C. Laudon, The Dossier Society (1986), David F.

As used in the Act, the term "sensitive" information must be understood to emphasize the importance of protecting the privacy interests of all Americans whose medical, employment, tax, and a host of other records are maintained by the federal government.

I would draw the Committee's attention to an important principle discussed in David Linowes's recent book, Privacy in America.[60] Mr. Linowes was the chair of the U.S. Privacy Protection Study Commission from 1977 to 1979. His book discusses the problem of the rapid accumulation of personal information in large organizations. He urges organizations to adopt Fair Information Practices, including the requirement of information "minimization" to insure that privacy is protected.[61] According to that principle, only necessary information should be collected.

Now this principle could be at odds with fundamental security practices. For example, audit trails, which enhance system security, may also undercut privacy safeguards. On the one hand an audit trail satisfies an important security goal: it creates a record of all the transactions on a system to determine what changes where made, at what point, and by whom. At the same time, an audit trail generates an activity log of individuals who are using the system: when they worked with the system, and what they

---

Linowes, Privacy in America (1989), Robert Ellis Smith, Privacy (1980), Alan F. Westin, Privacy and Freedom (1967).

60 David F. Linowes, Privacy in America (1989).

61 Id. at 175. A related principle is that information should only be used for the purpose for which it was collected. Id. at 176.

did. If the system contains an electronic mail capability, then an audit trail might also record the times when messages were sent, the address of the messages, as well as the content.

To the extent that agencies seek to improve system security through the incorporation of audit trails, they will generate an extraordinary amount of transactional information about the activities of people inside and outside of federal government. This information, already in computer form, might then become grist for the mill of employee reviews, censorship, and workplace monitoring.

There is no simple solution to this problem.[62] Computer security, in the narrow sense, will require audit trails. But privacy protection and the principle of information minimization might argue against excessive use of audit trails. Where will the NSA strike that balance?

A chilling description from Aleksander Solzhenitsyn describes the risk of gathering excessive information:

---

62 A group of CPSR members examined the privacy and security trade-offs of audit trails at a recent meeting. They suggested that the problem might be addressed by: (1) stating clearly the purpose of the audit trail in the system specifications; (2) developing a record destruction procedure for audit trails; (3) limiting the circumstances when an audit trail may be accessed, e.g. when actual data misuse, alteration, or destruction is shown; and (4) isolating audit trails so as to avoid the consolidation of "event" histories. Meeting of Computer Professionals for Social Responsibility, DC Chapter, May 2, 1989. (Summary available from CPSR).

> As every person goes through life he fills in a number of forms for the record, each containing a number of questions . . . There are thus hundreds of little threads radiating from every person, millions of threads in all. If these threads were suddenly to become visible, the whole sky would look like a spider's web, and if they materialized like rubber bands, buses and trams and even people would lose the ability to move and the wind would be unable to carry torn-up newspapers or autumn leaves along the streets of the city.[63]

REMEDIAL OR LEGISLATIVE ACTION

What can be done to get the legislation back on track?

First, the President should rescind NSDD-145. This Decision Directive is responsible for much of the confusion about the roles of the NSA and the NIST. It is doing little to strengthen national security; it may do much to weaken economic competitiveness, restrict scientific inquiry, and undermine open government.

In its place the President should issue a new executive order, revising the federal standard for information classification, and reversing the trend toward secrecy that is threatening our system of open government. As John Shattuck and Muriel Morisey Spence have stated:

---

63 Quoted in David Burnham, The Rise of the Computer State 47-48 (1983).

> The engines of innovation that drive our economy and guarantee our security are powered by open and unfettered communication. Government policy aimed at broadly controlling the communications of information and ideas may soon become irreparably damaging unless it is substantially reversed.[64]

Second, Congress should increase funding for the NIST, contingent on its withdrawal from the M.O.U., so that it has the resources to fulfill the responsibilities it has been assigned under the Act. Without sufficient funding, NIST will continue to go, hat in hand, to the NSA for technical assistance.

Third, this Committee must make clear to the Director of the NSA, the Director of NIST, and the Secretary of Commerce, that the M.O.U. is not in accord with the Computer Security Act, and that, for this reason, neither party can be bound by the agreement. This is a matter of Congressional authority that goes far beyond this specific agreement.

Fourth, the NIST staff responsible for implementing the Act, and those at NSA who are working to assist NIST, must go back to the privacy statutes governing record-keeping practices in the federal agencies. Without a clear understanding of the importance of the Privacy Act and the related statutes, NIST will fail to address a central concern of the Act: the protection of personal privacy.

Fifth, Congress must begin public hearings on the role of encryption technology. For too long data encryption has been left

---

64 "Essay: Needed A Free Flow of Information and Idea," Scientific American, January 1989, at 114.

to the intelligence agencies. Now, it is clear that encryption is the most important technical safeguard for ensuring the privacy and authenticity of all messages that travel along computer networks.[65]

Discussions about government cryptography must become public discussions, regardless of the agencies involved.[66] We also need to know, in particular and on the record, whether the NSA is engaged in routine monitoring of communications within the United States. And, according to Federal Computer Week, DARPA's Information Science and Technology Office is developing an expert system that can "examine millions of telephone calls a day and discern subtle and complex patterns for follow-up by law enforcement officials."[67] Has the NSA participated in this work?

Mr. Chairman, fifteen years ago, the Senate Intelligence Committee warned that the NSA's "potential to violate the privacy of Americans is unmatched by any other intelligence agency."[68]

---

65 McLellan, "Internet Computer Network to Use Code to Ensure Privacy," The New York Times, March 21, 1989.

66 The NSA has repeatedly tried to restrict the publication of cryptography research. See, e.g., David Burnham, The Rise of the Computer State 139-40 (1983), Kolata, "NSA Asks to Review Papers Before Publication," 215 Science 1485 (March 19, 1982), "Prior Restraints on Cryptography Considered," 208 Science 1442-43 (June 27, 1980).

67 Anthes, "DARPA Program to Battle War on Drugs, Terrorism," April 24, 1989, at 1, 53.

68 U.S. Senate, Select Committee on Intelligence, Intelligence Activities and the Rights of Americans, Final Report 201 (1976), reprinted in S. Bamford, The Puzzle Palace 473 (1983)

The Chairman of that Committee, Senator Frank Church, said that NSA intelligence-gathering capabilities were essential to the security of the United States. But he also warned that the massive eavesdropping devices and computers of the NSA create a "tremendous potential for abuse."[69] If ever turned against the communications system of the United States,

> no American would have any privacy left . . . There would be no place to hide.
>
> We must see to it that this agency and all agencies that possess this technology operate within the law and under proper supervision, so that we never cross over that abyss. That is an abyss from which there is no return.[70]

Mr. Chairman, twelve years ago I was in Washington and had the opportunity to meet with Senator Church after a hearing. I asked him about the role of Congressional oversight in intelligence activities. He left no doubt about its importance. Neither can this Committee.

---

69 National Broadcasting Company, Meet the Press 6 (1975) (NBC television broadcast, August 17, 1975)

70 Id.