DOCUMENT RESUME

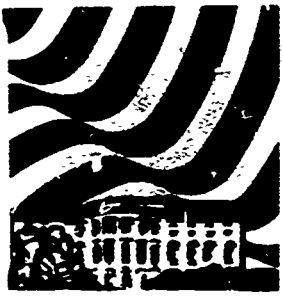
ED 324 022 IR 053 300

AUTHOR Shattuck, John; Spence, Muriel Morisey
TITLE A Presidential Initiative on Information Policy. Number 7.
INSTITUTION Benton Foundation, Washington, DC.
PUB DATE 89
NOTE 46p.; Project on Communications & Information Policy Options. For related reports, see IR 053 286-288.
AVAILABLE FROM Policy Options Project, Benton Foundation, 1776 K Street NW, Washington, DC 20006 ($6.50 per single copy, $33.00 for a boxed set of eight papers).
PUB TYPE Legal/Legislative/Regulatory Materials (090) -- Viewpoints (120)

EDRS PRICE MF01/PC02 Plus Postage.
DESCRIPTORS Access to Information; Data Collection; Federal Government; *Freedom of Information; Information Dissemination; *Information Needs; Information Utilization; International Trade; *National Security; *Policy Formation; Privacy; *Scientific and Technical Information
IDENTIFIERS *Information Policy; *Office of Management and Budget

ABSTRACT

Two trends have inhibited the development of information and ideas, which are vital resources in a modern technological society. First, the Federal Government is engaged in efforts to control the flow of scientific and technical information (STI) to make it less accessible to foreign competitors and hostile nations. Second, the role of government in collecting, maintaining, and publishing information has been curtailed because of reduced federal spending on information resources. The President's policy agendas should include an initiative on information policy with special programs focusing on science, the economy, and national security. The following elements would be included in such an initiative: (1) a review of the system for classifying information; (2) a review of export controls and related restrictions on the communication of unclassified STI; (3) steps to give Congress and the public time to comment on proposed executive orders and national security directives; (4) interagency deliberations to develop guidelines that protect against undue government control over the content and conclusions of federally sponsored research; (5) actions to limit the role of the Office of Management and Budget; (6) revisions in the Freedom of Information Act to facilitate access to government information; and (7) authorization for the Secretary of Defense to curb inappropriate secrecy in agency budgets. (SD)



7 A Presidential Initiative on Information Policy

John Shattuck & Muriel Morisey Spence

Benton Foundation
Project on Communications &
Information Policy Options

The Benton Foundation

The Benton Foundation, based in Washington, D.C., is a private grantmaking foundation committed to improving the democratic process through increased public understanding and use of communications and information technologies. A legacy of Senator William Benton, the foundation supports projects in the fields of communications policy, public affairs and the media, and communications education.

Benton Foundation Project on Communications & Information Policy Options

In early 1988, the Benton Foundation commissioned a series of eight papers to explore future options for public policy in the communications and information arenas. Written by recognized authorities in their respective fields, the papers identify critical issues and options confronting policymakers at the federal level.

Through the publication of this series, the foundation seeks to stimulate public awareness and discussion of the communications and information issues that will affect our society in the coming decade. Two broad themes are addressed in the papers: the role of policy in the rapidly changing mass media marketplace; and the ethical, constitutional, and regulatory challenges that arise from the increasing use of computers in our society.

The views in this paper are those of the author(s), and do not necessarily represent those of the Benton Foundation, its directors, or its staff.

A Presidential Initiative on Information Policy

John Shattuck & Muriel Morisey Spence

About the Authors

John Shattuck is Vice President of Harvard University (government, community, and public affairs). He also holds appointments as Lecturer at the Harvard Law School and Senior Associate in the Program on Science, Technology, and Public Policy at Harvard's John F. Kennedy School of Government. Mr. Shattuck served for eight years as Washington Director of the American Civil Liberties Union before going to Harvard in 1984. He has also taught at the Woodrow Wilson School of Politics at Princeton University, and has authored, edited, or contributed to *Freedom at Risk* (1988), *Privacy. Cases, Materials and Questions* (1988), *Endangered Rights* (1984), *Constitutional Government in America* (1980), *Rights of Privacy* (1977), and *Government Secrecy in America* (1975). In 1988, Mr. Shattuck received the Public Interest Law Award from the Yale Law School, and in 1984 was awarded the Roger Baldwin Medal for outstanding national contribution to civil liberties.

Muriel Morisey Spence is Director of Policy Analysis at Harvard University's Office of Government, Community, and Public Affairs. She is also Lecturer on Education and Acting Director of the Field Experience Program at Harvard's Graduate School of Education. Her previous positions include legislative counsel to the American Civil Liberties Union, legislative counsel to the U.S. Department of Justice, Civil Rights Division, and senior legislative assistant to Representative Shirley Chisholm.

Executive Summary

Information and ideas are vital resources in a modern technological society. In recent years, two trends have inhibited the development of these resources in the United States. First, the federal government has engaged in extensive efforts to control the dissemination of scientific and technological information so that it is less accessible to foreign competitors and hostile nations. Second, the role of the government in collecting, maintaining, and publishing information has been curtailed because of reduced federal spending on information resources.

The short-term benefits of these policies are outweighed by substantial long-term costs to the economy, the national defense, and the democratic tradition of open government.

The new President's domestic and foreign policy agendas should include a Presidential Initiative on Information Policy, with special attention to programs on science, the economy, and national security. The initiative should include the following elements.

(1) A thorough review of the classification system should be conducted with the goal of drafting a new executive order based on the principle that the need to protect national security information must be balanced against equally important public interest in informing the public about government activities.

(2) The current system of export controls and related restrictions on the communication of unclassified scientific and technical data should be reviewed. In initiating this policy review, the President should call for responsible agencies to protect military security and promote national economic interests by substantially reducing areas of control, thus enhancing the ability of U.S. scientists and businesses to benefit from the increased availability of scientific and technical data.

(3) Steps should be taken to give both Congress and the public time to comment on proposed executive orders and national security directives before their promulgation, with appropriate procedures for the protection of classified information.

(4) Inter-agency deliberations should be conducted to develop guidelines that protect against undue governmental control over the content and conclusions of federally sponsored basic research and the writings of present and former federal employees.

(5) The President should propose legislative and Executive branch actions to limit the role of the Office of Management and Budget in conducting regulatory review, influencing substantive agency decisions, and relying on the private sector for the dissemination of information generated with federal funds.

(6) Executive branch guidelines implementing the Freedom of Information Act should be revised to facilitate access to government information

(7) The Secretary of Defense should be authorized to continue efforts by DoD to curb inappropriate secrecy in agency budgets while cooperating fully with congressional oversight of federal defense spending

INTRODUCTION

Information and knowledge are vital resources in a modern technological society. The economic and military strength of the United States is increasingly based on our capacity to translate an expanding information and knowledge base into products and processes that contribute to prosperity and national defense. In addition, our democratic system is rooted in a belief that the free flow of information and ideas is vital to the fabric of our national life.

In recent years, two trends have inhibited the development of information resources in the United States. First, increased efforts have been made by the federal government to control the dissemination of scientific and technological information so that it is less accessible to foreign competitors and hostile nations. Second, the role of the government in collecting, maintaining, and publishing information has been curtailed because of reduced federal spending on information resources.

The elements of these trends are clear. A broad system of national security controls has curtailed the ability of American scientists to communicate technical data and collaborate freely with their foreign counterparts. The capacity of the United States to innovate and compete in a world economy driven by technology has been diminished in subtle but important ways by an export control system that restricts scientific communication. Governmental processes have been negatively affected by a broadened classification system that has increased the need for compartmentalized decision-making in the federal bureaucracy. Curtailment of the government's traditional role as a source of statistical and technical data about the economy and the work force has impeded the study and development of economic and social policy. Restrictions on the publication of federally funded research have deprived the public of information for which it has paid with its tax dollars.

Any short-term benefits of these policies are outweighed by substantial long-term costs to the economy, the national defense, and the democratic tradition of open government. These costs are

particularly great in the areas of science and technology. Reports by the National Academy of Sciences in 1982 and 1987 have warned of a growing threat to U.S. economic and military security of broad controls on scientific communication.[1] "With respect to U.S. military and economic progress," the 1982 report concluded, "controls may slow the rate of scientific advance and thus reduce the rate of technological innovation. Controls also may impose economic costs for U.S. high technology firms, which offset both their prices and their market share in international commerce. Controls may also limit university research and teaching in areas of technology. A national policy of security by accomplishment has much to recommend it over a policy of security by secrecy." The 1987 NAS report indicated that the cost to the U.S. economy of the current regime of export controls, including controls over technical and scientific data, is 188,000 jobs and $9 billion per year. According to the report, 52 percent of U.S. high-technology companies experienced lost sales in 1986 primarily as a consequence of export controls.

In addition to the economic and military costs of broad information controls, there are considerable costs to the U.S. political system and culture. The United States has a tradition of open communication and public access to information. Our Constitution was adopted two centuries ago after agreement was reached on the inclusion of two essential features designed to foster open communication. The first was the imposition of an affirmative obligation on the federal government to publish regular information about its taxing and spending activities. The second was a commitment to have a Bill of Rights, with the First Amendment as its cornerstone, guaranteeing freedom of speech, thought, and religion, and freedom of the press. Now here is our national commitment to the free flow of information and ideas more important than on issues involving science, technology, and economic growth. From this perspective, the recent trends in federal information policy are adversely affecting important values of free speech, academic inquiry, and democratic participation.

The discussion that follows summarizes key information policy trends and events of recent years, describes some of their implications, and offers recommendations for policy actions by the new Administration.[2]

THE NEED FOR A PRESIDENTIAL INITIATIVE ON INFORMATION POLICY

Reversal of the trend toward restricting the free flow of information in the United States should be a central feature of the new President's domestic and foreign policy agendas, with special attention to programs on science, the economy, and national security.

While Congress necessarily plays an important role in shaping such policies, there are several reasons why changes are most likely to occur if the President takes early advantage of the unique leadership opportunity that comes at a time of presidential transition. First, a new President has maximum influence on the terms of public debate. Second, appointments of Cabinet members, such as the Secretaries of Defense and State, and other principal policy advisors, such as the Director of Central Intelligence, the National Security Advisor, and the President's Science Advisor, provide an opportunity to create new leadership of key executive agencies. Third, the Senate confirmation hearings necessary for many appointments present an early opportunity for the incoming Administration to establish working relationships with key congressional offices. Fourth, career officials in executive agencies need an early indication of the new Administration's policy perspectives in order to function most efficiently. Finally, Congress must be able to anticipate the legislative recommendations that will be of primary interest to the new Administration.

Two procedural objectives should guide the formulation of a Presidential Initiative on Information Policy. The first is to allow ample opportunity for public and congressional notice and comment on planned Executive branch actions. The second is to maintain a cooperative relationship with Congress in the development of legislation and during the congressional oversight process. Because a wide range of issues and practices are implicated in information

policy, no one document or statement is likely to be sufficient. The priorities for action should be (1) an early presidential statement identifying information policy as an issue of significant concern, (2) inter-agency deliberations to identify specific areas for action, and, at the same time, (3) the initiation of consultations with Congress.

ISSUES TO BE ADDRESSED IN THE INITIATIVE

The ultimate goals of an information policy initiative by the new Administration should be to improve U.S. competitiveness, strengthen the national defense, and enhance democratic decision-making by reversing the recent trend toward excessive governmental control of the flow of information.

Two themes should dominate the early presidential messages on information policy. The first is that free and open communication of information should occur except in instances of demonstrable and substantial public necessity. The second is that changes in federal information policy should be developed and implemented cooperatively between the Executive branch and the Congress.

A Presidential Initiative on Information Policy should address at least seven important areas (1) the classification system, (2) export controls and related restrictions on the communication of unclassified scientific and technical data, (3) national security decision directives, (4) prepublication review and censorship, (5) management of federal information resources, (6) the Freedom of Information Act; and (7) secrecy in agency budgets.

1. The Classification System

A major information policy development in the last six years has been the unprecedented expansion of the security classification system.[1] Executive Order 12356, issued by President Reagan in 1982, reverses a trend during the previous four administrations toward increasing emphasis on the free circulation of knowledge and information — a trend marked by limiting classification, defining the

purposes of classification, and providing procedures for declassification. This trend is reflected in Executive Order 12065, promulgated in 1978, and its predecessor orders extending back to the Eisenhower Administration.

E.O. 12356 modifies the classification system in major ways that limit the availability of information. It establishes a presumption in favor of classification in all cases where officials are in doubt whether secrecy is necessary, it eliminates the previous Order's requirements of automatic declassification of information within a prescribed length of time, and it extends new authority to officials to reclassify information that is already in the public domain. Executive Order 12356 also abolishes a requirement in the previous Order that federal officials "balance the public's interest in access to government information with the need to protect certain national security information from disclosure." In addition, the threshold standard for classification is reduced, giving classifying officials considerably greater discretion. Instead of having to demonstrate "identifiable damage" to the national security, the classifier must show only that "disclosure reasonably could be expected to cause damage to the national security."

The present Order also revises other significant features of the classification system. The previous Order expressly precluded the use of federal classification authority over non-governmentally sponsored basic research, while the present Order leaves the matter to agency discretion. The present Order also permits the reclassification of information if "the information requires protection in the interest of national security and the information may reasonably be recovered," even after an agency has received a request for it under the Freedom of Information Act or the Privacy Act. By contrast, the earlier Order provided that "[c]lassification may not be restored to documents already declassified and released to the public. . ." and that "no document originated on or after the effective date of this Order may be classified after an agency has received a request for the document under the Freedom of Information Act. . ."

The present classification system allows government officials to impose classification restrictions over federally funded research projects even after research contracts have been signed and work has begun. The Order allows classification to occur at any stage of a project and to be maintained indefinitely. Some scholars fear that under the new classification order, "[a]cademic research not born classified may die classified." The net effect is to inhibit researchers who are unwilling to do classified research from making long-term intellectual investments in non-classified projects in such fields as cryptography or laser science, which have features that make them likely subjects for classification at a later date. The long-term cost may be the loss of important scientific contributions that such scholars might make in these fields.

The publication of federally funded research also is affected by the recent expansion of the classification system. Publication decisions are governed by National Security Decision Directive (NSDD) 189,[4] promulgated in response to concerns that unclassified research sponsored by the federal government might be restricted. The Directive provides that restrictions on publication can only result from classification, but Executive Order 12356 gives officials authority to reclassify information already in the public domain. Thus, NSDD 189 does not adequately address the concern already noted that research that is not classified when begun may become classified while it is underway.

The President should order a thorough review of the classification system with the goal of drafting a new executive order aimed at restructuring the system. The text of this draft should be made available for review and comment by congressional offices with oversight responsibility over the agencies involved, as well as the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence.

The new executive order should be based on the principle that the need to protect national security information must be balanced

against an equally important public interest in disclosure of information gained through government-funded research or in informing the public about government activities.

The new order should:

- reverse the current presumption in favor of classification in all cases where officials are in doubt about whether secrecy is necessary;

- raise the threshold standard for classification,

- require automatic declassification within a prescribed period of time,

- eliminate the authority of officials to reclassify information already in the public domain; and

- lift restrictions on the communication of unclassified information between Americans and foreigners

2 Export Controls and Related Restrictions on the Communication of Unclassified Scientific and Technical Data

The classification system reaches information collected by or under the sponsorship of government Current efforts to control the dissemination of technical data, however, have extended beyond classification into a growing number of civilian scientific and technological fields

Until recently, as a general rule only two types of limitations have been allowed on the communication of scientific and technical data In the case of information controlled by the government, the classification system has been the means of protecting national security interests In the case of information not controlled by the

government, restrictions on communication have been limited to rare circumstances involving a clear and present danger to the national security.

Advocates of broader restriction on scientific and technical data assert that such data are different from other kinds of freely communicated information for two reasons. First, technical data can be used to create things that are intrinsically dangerous, such as weapons systems. Second, technical data can have an immediate economic utility and are thus often more like commodities than information. These characteristics have been regarded as warranting an extensive system of export controls over categories of technical data, new controls over the kinds of communication scientists can have among themselves, and limitations on the communication of "sensitive" unclassified information.

There are many practical difficulties in enforcing broad controls over the communication of unclassified technical information, as well as significant costs to the economy, to scientific research, and ultimately to the national defense itself.

The export control laws were originally enacted primarily to regulate the overseas export of tangible goods.[5] Over the last decade, however, they have been used increasingly to restrict the communication of technical information and ideas within the United States. The Departments of Defense and Commerce, for example, have sought to require scientific and engineering societies to limit access to professional conferences at which unclassified technical papers are to be presented. According to the American Association for the Advancement of Science, there have been more than a dozen incidents in the past eight years of restrictions on the communication of unclassified technical data at scientific conferences. Such restrictions can also be made conditions of research contracts. Furthermore, the Department of Defense has recently required universities engaged in unclassified DoD-sponsored research in artificial intelligence to certify that persons who receive technical data generated by the research are U.S. or Canadian citizens.

Beyond the restrictions on contact between U.S. and foreign scientists, general categories of scientific and technical research have been designated as inherently sensitive and therefore subject to generic information controls For example, in 1981, at the request of the Reagan Administration, Congress amended the Atomic Energy Act to authorize the Secretary of Energy to regulate "the unauthorized dissemination of unclassified nuclear information "[6]

A final area of scientific and technical information targeted for control in recent years is information in electronic data bases. This is by far the largest category of potentially restricted information, because it can be found in any academic, commercial, or governmental computerized information system. National Security Decision Directive 145, issued by President Reagan in 1984, calls for "a comprehensive and coordinated approach" to all telecommunications and automated information systems, under the theory that "information, even if unclassified in isolation, often can reveal sensitive information when taken in the aggregate "[7]

In the wake of NSDD 145, President Reagan's former National Security Advisor, John Poindexter, promulgated a directive that sought to restrict not only unclassified information affecting national security interests, but also any computerized information that could adversely affect "other government interests," including "government or government-derived economic, human, financial, industrial, agricultural, technological, and law enforcement information."[8] This White House directive raised the specter of U.S intelligence agencies monitoring and regulating virtually all academic and commercial computerized data bases and information exchanges in the United States. The directive was withdrawn in March 1987 under congressional pressure, but the underlying policy, set out in NSDD 145, remains in place

In order to address this set of information policy problems, the new President should direct the National Security Council and the Departments of Defense and Commerce to conduct a thorough

review of the current system of export controls and related restrictions on the communication of unclassified scientific and technical data. In initiating this policy review, the President should require the NSC to provide regular, affirmative policy direction to the responsible line agencies to protect military security and promote national economic interests by substantially reducing the areas of control, thus enhancing the ability of U.S. scientists and businesses to benefit from the increased availability of scientific and technical data. As the National Academy of Sciences recommended in its 1987 report, "the preparation of control lists must be a dynamic process that is both informed by advice from technical advisory groups and constrained by the need to be clear, to focus control efforts more narrowly on fewer items, and to coordinate U.S. actions more clearly with that of the Coordinating Committee on Multilateral Export Controls (COCOM) of our allies."

The President should also direct the NSC and the relevant line agencies to work with the Congress to eliminate the use of restrictions on unclassified fundamental research. Specifically, two sources of authority should be amended or repealed.

First, the Department of Defense Authorization Act of 1984[9] now contains an exemption to the Freedom of Information Act (FOIA) which permits DoD to "withhold from public disclosure any technical data with military or space application in the possession of, or under the control of, the Department of Defense," whose export would otherwise require a validated export license. The effect of this provision has been to bar the publication of certain unclassified technical research conducted under government contract. A particularly dramatic example of this provision's effect occurred in March 1985 when the DoD notified the organizers of the international symposium of photo-optical instrumentation engineers that nearly two-thirds of the scheduled papers could not be publicly presented because they contained information falling within the new FOIA exemption. This restraint on the communication of unclassified research should be repealed.

Second, National Security Decision Directive 189[10], signed by President Reagan in 1985, states that "[n]o restrictions may be placed upon the conduct or reporting of federally-funded fundamental research that has not received security classification, *except as provided in applicable U.S. statutes.*" Since the applicable statutes include the export control laws, the qualifying phrase offers no protection for the open communication of basic research and thus should be deleted.

3. National Security Decision Directives

Presidential directives, such as proclamations and executive orders, have been used since the earliest days of the federal government to express Executive branch policie and implementation guidelines. A numerical system for these directives was begun in 1907. The Federal Register Act of 1935[11] requires that presidential directives be published in the *Federal Register* and reproduced in the annual and cumulative volumes of the *Code of Federal Regulations.*

For approximately 70 years some of these directives have been confidential or security classified. Since 1947, the National Security Council has produced directives which have set forth the U.S. position on a wide variety of national security issues. Most are classified and thus unavailable for congressional or public scrutiny. According to the General Accounting Office,[12] at least 1,042 have been issued since 1961. Of these, only 247 have been publicly released, while the rest have remained secret.

In 1976, the Senate's Special Committee on National Emergency and Delegated Emergency Powers concluded that such secret presidential directives lack prescribed formats or procedures and are not systematically revealed to the Congress or the public.[13] These directives have been used to advance some of the most troubling presidential policies. For example, President Johnson used directives to authorize the production of secret weapons systems. President Nixon issued a number of such directives relating to United States involvement in Southeast Asia

The Reagan Administration designated these instruments "National Security Decision Directives." By some estimates, approximately 200 NSDDs have been issued since 1981, but fewer than ten have been publicly disclosed in whole or in part. During the Reagan presidency, NSDDs were the principal means of initiating a variety of domestic and foreign policy actions. For example, President Reagan issued a NSDD to authorize agencies other than the Central Intelligence Agency to conduct covert operations. Similarly, NSDD 84, issued in March 1983, imposed long-term controls over all federal employees and contractors with authorized access to certain categories of classified information, requiring them to sign lifetime prepublication review agreements as a condition of access. This directive was later withdrawn under congressional pressure.

A long-standing interest in presidential proclamations and executive orders led the House Committee on Government Operations in 1982 to issue a Committee report on "Security Classification Policy and Executive Order 12356."[14] The Committee recommended that the Executive branch give both Congress and the public time to comment on proposed executive orders before their promulgation, and provide written findings detailing the policy problems each proposed order is intended to solve. In August 1988, the Government Operations Subcommittee on Legislation and National Security held hearings on legislation to require that presidential directives be shared with Congress and in compliance with statutory rules of accountability, publication, and record-keeping. The legislation provides for the protection of classified directives.

The new President should take steps to implement these congressional committee recommendations with respect to both executive orders and national security decision directives. The Government Operations Committee Report called for giving congressional committees classified versions of the findings and explanations, while making unclassified versions available to the public. At the same time, the President should cooperate with Congress in developing legislation to establish guidelines for the use and disclosure of presidential directives. An important step towards effective cooperation with Congress in this area should be the release to relevant

congressional committees of a list of the known directives from recent years.

4. Prepublication Review and Censorship

As sponsor of a wide range of information-producing activities, the federal government is uniquely positioned to influence, and sometimes control, the content of information that is publicly disseminated. Such influence can rise to the level of official censorship if it unduly prevents present or former government employees from writing or publishing freely · undermines the objectivity of research or other data-gathering activities. The use of prepublication review to screen the writings of government employees or the results of research conducted under government contract can create a climate of censorship. The effect of this climate is to deprive the public of the benefits of scientific research and information about the workings of government, undermining principles of openness and freedom of inquiry.

Since 1981, all government employees with high-level security clearances have been required to sign Form 4193, which contains a lifetime promise to submit for prepublication review virtually all writings, including works of fiction. A 1986 General Accounting Office report on the impact of Form 4193 concluded that in 1984, 21,718 books, articles, speeches, and other materials were reviewed under agency prepublication review processes. In 1985, this number grew to 22,820. The GAO determined that as of December 31, 1985, at least 240,776 individuals had signed Form 4193. During the same two-year period, there were only 15 unauthorized disclosures of information through the writings or speeches of current or former employees. The purported benefits to national security appear to be far outweighed by the risk of undue censorship.

In the area of federally funded research, agency contracts with scholars have in recent years created a tension between the funding agency's interest in getting a prescribed research product and the scholar's interest in remaining free to conduct research without inappropriate constraints. This tension has been heightened by

governmental efforts to modify funded research and limit the scholar's ability to publish or release research results, documents, or computer software. Prepublication review provisions in research contracts have been important tools to exert such influence over the research. For example, researchers at Harvard University objected in 1984 to attempts by the Department of Housing and Urban Development to retain the right to require "changes" in the data, methodology, or analysis of their funded research. In declining the contract, the University's Office of Sponsored Research asked how it was possible to require "changes in data, methodology, or analyses without attacking the very foundations upon which resulting reviews, opinions, and conclusions are based?"

Restrictions on publication are a source of frequent conflict between the Central Intelligence Agency and its civilian contract researchers and consultants, many of whom are academic scholars. Until recently, most CIA contracts required consultants and researchers for the agency to submit all their writings for prepublication review. The censorship permitted by this restriction made such contracts unacceptable to many universities. In 1986, the CIA revised its rule on prepublication review, narrowing the restriction for outside scholars to "the specific subject area in which a scholar had access to classified information." As a practical matter, however, the new rule continues to present problems for contract researchers and consultants. Civilian experts who use classified information in consulting with the CIA tend to conduct research only in their fields of specialization, and any subsequent writing they do in that field will still presumably be subject to prior CIA review under the new rule. Thus, the danger of broad censorship remains.

Prepublication review policies should be the subject of interagency deliberations designed to develop guidelines that protect against undue governmental control over the content and conclusions of federally sponsored basic research and the writings of federal employees. To be effective, prepublication review guidelines must direct agencies to draft research contracts that are consistent with both the agency's interest in the research to be funded and the need to protect the researcher's intellectual independence and

integrity. For example, there should be constraints on the scope of an agency's prepublication review authority to prevent censorship stemming from the agency's disagreement with the policy implications of the writing or research in question. Sharp limits on how long an agency can conduct its review prior to publication would prevent delays that rob the research of timeliness. It may be necessary to develop separate prepublication review policies for at least three categories of research and publications that have varying levels of national security relevance. classified research, unclassified research with national security implications, and research with no discernible national security implications. Without separate guidelines, the second two categories are likely to be subject to restrictions on publication that would be suitable only for classified research

5 Management of Federal Information Resources

A pivotal point in the recent evolution of government information policy occurred in 1980 when Congress enacted the Paperwork Reduction Act (PRA).[15] The purpose of the Act was to "minimize the Federal paperwork burden." The new statute replaced the Federal Reports Act of 1942,[16] which had long provided the basic statutory framework for the record-keeping and reporting requirements imposed by the federal government on private businesses and nonfederal government entities.

Earlier, in 1974, Congress had responded to growing public concern about the burden of federal demands for information by establishing a Commission on Federal Paperwork.[17] The Commission's final report, issued in October 1977, estimated that the combined cost to the government and the public of federal paperwork requirements amounted to $100 billion a year. These requirements included the preparation of tax and health care forms, loan applications, and compliance reports affecting most segments of the population. The Commission's recommendations complemented Congress' review of possible amendments to the laws governing the management of information requests directed to the public. That review culminated in passage of the Paperwork Reduction Act in 1980

The legislative history of the PRA makes clear that Congress was concerned with both the "excessive" cumulative impact on the public of federal paperwork requirements and the potential for abuse of the authority set out in the Act. Accordingly, the Act mandated the elimination of unnecessary and wasteful paperwork requirements, but provided that this stipulation must not interfere with "the substantive policies and programs of departments, agencies and offices."[18]

The PRA created an Office of Information and Regulatory Affairs (OIRA) within the Office of Management and Budget (OMB), and charged it with developing comprehensive information policies for the entire federal government.[19] The OIRA Administrator is obligated to determine whether the collection of information by an agency is "necessary for the proper performance of its functions," including "whether the information will have practical utility for the agency." A key element of this effort is the concept of "information resources management"—the coordinated planning and management of all information activities, including creation, collection, use, and dissemination.

Through its implementation of the PRA, OMB has become increasingly involved not only in information resources management, but also in regulatory review and substantive policymaking. Congressional review of OMB's implementation of the PRA in 1982 and 1983 established that a significant portion of OIRA's resources had been devoted to regulatory review activities rather than information resources management.

In 1985, OMB consolidated its control of federal information activities by means of Circular A-130, "Management of Federal Information Resources," which set forth criteria for the collection and dissemination of information by federal agencies. Major changes in information policy have resulted from OMB implementation of the two principal statutory criteria, (1) "necessary for the proper performance of agency functions" and (2) "practical utility," as well as a criterion added by Circular A-130, but not found in the PRA, that dissemination of information be conducted (3) in "the most cost

effective manner" with "maximum feasible reliance on the private sector."

Through Circular A-130, OMB has intruded in agency judgments about research and publication and thus has limited the availability of information. For example, a 1986 congressionally requested study of 51 proposed research projects submitted to OMB by the Centers for Disease Control found OMB was more likely to reject research projects with an environmental or occupational health focus than projects involving infectious diseases or other conventional illnesses. The study also cited OMB decisions to block proposed research projects on the basis that they lacked "practical utility." These included, for example, proposed research on the effects of worker exposure to dioxin.[20] A cost-benefit analysis led OMB to block a proposed Environmental Protection Agency regulation designed to protect consumers and workers from asbestos. The requirement that information dissemination be conducted in the most cost effective manner has also led to increased reliance on the private sector for information services traditionally provided by government agencies, often at increased cost to the information consumer.

In a related development, OMB has conducted a systematic reduction in federal publications. An early example was an OMB directive (Bulletin 81-16) to review publications and costs arising from the printing and production of written or audio-visual materials. In response, the Department of Education created the Publication and Audio-Visual Advisory Council (PAVAC). The Council rejected so many requests from Department-funded projects to publish materials they had developed that the House Committee on Government Operations concluded that the process amounted to censorship.[21]

The 1986 reauthorization of the PRA is a partial response to growing criticism of the information policy directives of the OMB. The reauthorization law includes provisions to make the OIRA publicly accountable for its decisions. The new law requires that any "written communication" between the OIRA and an agency must be

available for public examination. The reauthorization also requires fuller disclosure in the *Federal Register* whenever an agency submits to the OIRA an information collection proposal. However, the new statute does not require that the substance of the proposal be included and does not require a public comment period. As for constraints on regulatory review by OMB, although the Act now expressly forbids the OIRA from using funds appropriated under the PRA to conduct regulatory review, OMB effectively retains that authority because the amended Act includes regulatory paperwork in the provision that limits paperwork approval to three years. Thus, OMB will review all information collections required by regulation at least once every three years.

The Reauthorization Act also addresses perceived deficiencies in OIRA's handling of statistics programs. During the first three years of the Reagan Administration, the OMB eliminated the agency's statistical policy branch, cut substantially the number of OMB statistical personnel, and minimized the significance of statistical policy to government planning. For example, a study presented in a March 1986 Joint Economic Committee hearing on the status of the nation's economic statistics concluded that "planning and research for new and better ways to meet changing needs and take advantage of new technology have suffered. Ultimately this neglect is likely to add to the cost of statistical programs as well as weaken their quality."[22] The Reauthorization Act strengthens OIRA's statistical responsibilities and requires the OIRA to appoint a professional statistician as the U.S. chief statistician.

Three principles should guide the new Administration's review of information management issues. First, OMB's information management activities should be kept separate from regulatory review. Second, OMB must not be permitted to use its paperwork clearance authority to interfere with substantive agency decisions. Third, information collection and dissemination should be designated as essential federal agency functions, and involvement of the private sector in these activities should not interfere with the availability of information generated with federal funds.

In addition, the new Administration should support stronger statutory limits on OMB's regulatory review and substantive decision-making, and limitations on the broad discretion granted to OMB in the Paperwork Reduction Act's "practical utility" criterion for the review of proposed paperwork. These needed constraints on OMB can be accomplished through cooperation between Congress and the Executive branch.

6. Freedom of Information Act

For more than two decades, public access to government information has been firmly established in the United States as a matter of law. The Freedom of Information Act, passed by the Congress in 1966 and amended four times since,[23] authorizes private individuals and organizations to obtain information collected and maintained by the federal government which has not otherwise been made available through government publications. It amended Section 3 of the Administrative Procedure Act of 1946 which stated that only "persons properly and directly concerned" could have access to official records. Under the FOIA "any person" can have access to identifiable agency records unless the information falls under one of the specified exemptions. In a period when federal information policies have reduced the amount of information collected and published by the government, the FOIA has become increasingly important as a vehicle for public access.

The 1986 amendments to the FOIA (Freedom of Information Reform Act, Subtitle N of H.R. 5484, The Anti-Drug Abuse Act of 1986) increased law enforcement agencies' rights to withhold certain records and gave the Office of Management and Budget the authority to set guidelines for agency rules concerning fees that agencies can charge for searching and processing requested records. In doing so, Congress recognized that exorbitant fees can be a significant barrier to public access, and that it is often in the public interest for agencies to waive fees for academic researchers and other nonprofit requesters.

Under the amendments, each agency must promulgate regulations specifying its schedule of fees for responses to FOIA requests and procedures for determining when fees should be waived or reduced. Fees chargeable to any requester may be waived or reduced "if disclosure of the information is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester." The legislative history makes clear that this waiver provision is not limited to situations where the requester intends to disseminate the requested information widely to the public, including journalists.

Despite congressional intent to enhance the utility of the FOIA, OMB has taken steps to limit public access by narrowly construing the fee waiver amendments in several respects and applying the management principles that it is using to limit the amount of information collected and published by federal agencies. The final Uniform Fee Schedule and Guidelines issued by OMB in March 1987[24] affect each agency's fee schedules and thus have the potential for placing limits on access to a wide range of information for researchers, libraries, and other nonprofit entities. For example, the guidelines permit "educational institution(s)" to obtain documents for the cost of reproduction alone, excluding the first 100 pages. However, OMB's definition limits "educational institutions" to entities "which operate a program or programs of scholarly research," thus excluding public libraries, vocational schools, instruction centers, and a wide variety of other entities that provide educational instruction and materials but may not employ scholars engaged in research

The OMB guidelines relating to requests for "commercial use" expressly reject the presumption that a request "on the letterhead of a nonprofit organization [is] for a non-commercial request." Critics of this OMB decision point out that the congressional floor managers of the 1986 amendments made clear they favored fee waivers for nonprofit organizations Reps Glenn English (D-Okla.) and Thomas Kindness (R-Ohio) stated that "a request from a public interest group, nonprofit organization, labor union, library or similar or-

ganization, or a request from an individual may not be presumed to be for commercial use unless the nature of the request suggests that the information is being sought solely for a private, profit-making pose."[25]

An important element of the new President's information policy initiative should be to direct the development of revised guidelines on FOIA implementation that reflect a principal legislative purpose of the 1986 amendments. eased access to information through appropriate use of fee schedules. These new guidelines should be drafted with adequate opportunity for public and congressional notice and comment A key principle in the guidelines should be that access to information should not be unduly limited through the imposition of exorbitant fees or excessively narrow interpretations of the statute.

7 Secrecy in Agency Budgets

Democratic decision-making depends on the ability of an informed Congress to make judgments about the spending of federal tax dollars In recent years, it has been increasingly difficult for Congress or the public to know how billions of dollars spent by the Department of Defense are being used. The reason is that a growing amount of such expenditures is included in so-called "black" budgets This phrase has come to include both "special access programs," which are subject to secrecy controls beyond the regular classification system, and other programs for which unclassified funding data are not available from the DoD. When DoD officials use the term 'black budget," they are referring to programs whose existence and purpose may be classified.[26]

The asserted authority for special access programs is Executive Order 12356, which provides that agency heads "may create special access programs to control access, distribution, and protection of particularly sensitive information."[27] Access is thereby limited to categories of officials, such as agency heads and congressional committee chairmen DoD officials say that aggregate budget data are sensitive because they may reveal to adversaries in what fields

the United States has chosen to concentrate time and resources and whether we have achieved significant breakthroughs.

Estimates of the amount of money involved in secret budgets vary between $22 billion and $35 billion, depending on whether the count includes only weapons research and development and acquisition, or intelligence spending as well. So long as large and expanding amounts of defense spending are not subject to informed oversight by Congress, democratic decision-making about defense policy is severely impeded

Congressional oversight of special access programs is particularly difficult for three reasons. First, congressional offices have insufficient bases on which to make independent evaluations of program rationales, design, and performance. Second, with little information, Congress has a reduced capacity to detect fraud, waste, and mismanagement. Third, there is inadequate information on which to base evaluations of the level of budget growth.

Executive branch oversight of secret budgets also has been limited. A May 1988 General Accounting Office report found that the Secretary of Defense has no centralized office with cognizance of all special access programs because of the difficulties of compiling program information. The GAO also found that the DoD was not following its own criteria for placing programs in the "black budget." The GAO observed that special access program sponsors often consider the sensitivity of a proposed program or technology sufficient justification for the "special access" designation without demonstrating, as regulations require, that normal security procedures are inadequate. The regulations also require a showing that the number of persons with access to a special access program will be small and commensurate with the goal of providing extra protection for information. The GAO found, however, that in Air Force special access programs, for example, the number of accesses granted was in the tens of thousands.[28] This suggests strongly that special access status is insufficient reason to deny access to Members of Congress and their staffs

There is reason to doubt whether the growing use of special access programs (SAPs) is achieving its goal of improving security protection of particularly sensitive information. A 1987 Defense Investigative Service (DIS) field review report indicated that many programs that are designated SAP receive less stringent security protection than programs subject to normal classification. In June 1987, the DoD established a Special Access Program Review Panel to examine the results of the DIS field review and evaluate the security administration of DoD special access programs. The Special Access Program Review Panel presented its report in August 1987 to the Deputy Undersecretary of Defense for Policy. The panel's recommendations included proposed improvements in regulatory definitions of special access programs and the implementation of previous recommendations concerning oversight, rationale for establishment and maintenance of SAPs, and personnel security.[29]

Congress has already begun to take steps to address the need for more effective legislative oversight of "black budget" programs. An amendment to the FY 1988 Defense appropriations bill requires the Secretary of Defense to report to congressional defense committees on

- the total amount requested for special access programs in a particular year,

- the total amount spent on special access programs in the last five years,

- the cost of individual "black budget" programs and their projected future costs, and

- a brief description of each program

The amendment permits the Pentagon to withhold information from the "black budget" reports for national security reasons.

Recent efforts by DoD and the Congress to curb inappropriate secrecy in agency budgets are important first steps toward improved oversight and monitoring of federal defense spending. The President should give the Secretary of Defense a mandate to continue this progress within DoD while cooperating fully with congressional oversight efforts.

CONCLUSION

These changes in federal information policy should be an essential part of the agenda of the new Administration. The free flow of information and ideas is vital to the fabric of our national life. The engines of innovation that drive our economy and guarantee our security are powered by open and unfettered communication. Government policies aimed at broadly controlling the communication of information and ideas are ultimately self-defeating and may soon become irreparably damaging to our democratic principles unless the new President seizes the initiative and changes the course that these policies have taken over the last decade.

Notes

1. Academy of Sciences, "Scientific Communications and National Security" (National Academy Press, Washington, D.C., 1982); National Academy of Sciences, "Balancing the National Interest: U.S. National Security, Export Controls and Global Economic Competition" (National Academy Press, Washington, D.C., 1987).

2. *See* generally Shattuck and Spence, *Government Information Controls: Implications for Scholarship, Science and Technology* (Association of American Universities, March 1988).

3. *See* Appendix A.

4 "National Policy on the Transfer of Scientific, Technical and Engineering Information," September 21, 1985. *See* Appendix C.

5. *See* Appendix B.

6. 42 U.S.C 2168(a)(1)

7 NSDD 145, "National Policy on Telecommunications and Automated Information Systems Security," September 17, 1984.

8 NTISSI No 2, "National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Information Systems," October 29, 1986.

9. P.L 98-94

10 "National Policy on the Transfer of Scientific, Technical and Engineering Information".

11. 44 U.S.C 1505(a).

12. *See* Appendix C.

13. S. Rept. 94-922, 94th Congress, 2nd Session.

14. H. Rept. 97-731, 97th Congress, 2nd Session.

15. P.L. 96-511.

16. 56 Stat. 1078.

17. P.L. 93-556.

18. 44 U.S.C. 3518(e).

19. *See* Shattuck and Spence, *Government Information Controls*, pp. 49-54. A more detailed discussion of the issues in this section is presented in another paper in this series, "Strengthening Federal Information Policy. Opportunities and Realities at OMB," by Gary Bass and David Plocher.

20 "OMB Review of CDC Research. Impact of the Paperwork Reduction Act," House Subcommittee on Oversight and Investigations, 98th Congress, 2nd Session (October 1986).

21. H. Rept. 99-978, 99th Congress, 2nd Session (1985).

22 "The Quality of the Nation's Economic Statistics." Hearings Before the Joint Economic Committee, 99th Congress, 2nd Session, March 17 and April 17, 1986, p. 41.

23. In 1974, 1976, 1983, and 1986. *See* Appendix D.

24. 52 Federal Register 10012.

25. *Congressional Record*, October 8, 1986, P.H9464.

26 *See* "Special Access Programs and the Defense Budget. Understanding the 'Black Budget'," Alice C. Maroni, Foreign Affairs and National Defense Division, Congressional Research Service, December 2, 1987.

27. E.O. 12356, Sec 4.2.

28. "Special Access Programs, DOD Criteria and Procedures for Creating Them Need Improvement," Unclassified Summary to Congressional Committees, May 1988.

29. "Report of the Department of Defense Special Access Program Review Panel," 31 August 1987.

Appendix A

Classification System

I. History

The current classification system was established by Executive Order (E.O.) 12356, National Security Information, 47 Fed. Reg. 14874 (April 2, 1982), reprinted in Codification of Presidential Proclamations and Executive Orders 1961-1985 at 587.

E.O. 12356 is the latest in a long series of executive classification directives that began in 1940 when President Franklin Roosevelt issued E.O. 8381, Defining Certain Vital Military and Naval Installations and Equipment, 5 Fed. Reg. 1145 *et seq.* (March 26, 1940), reprinted in 3 C.F.R. 1938-1943 Compilation at 634. President Roosevelt acted under the authority of a 1938 statute expressly delegating to the President the authority to create a classification system "in the interests of national defense." (52 Stat. 3 (1938)). The 1940 Order applied to military and naval installations and equipment, including private companies engaged in the defense industry. Equipment was expressly defined to include "books, pamphlets, reports, maps, charts, plans, designs, models, drawing, photographs, contracts, or specifications."

The classification system has continued to be defined through a series of executive orders. These include E.O. 10104, issued by President Truman in 1950, E.O. 10290, issued by President Truman in 1951, E.O. 10501, issued by President Eisenhower in 1953, E.O. 10964, issued by President Kennedy in 1961, E.O. 11652, issued by President Nixon in 1972; and E.O. 12065, issued by President Carter in 1978. There is widespread agreement among legal scholars that these orders, while not subject to the congressional approval process, have the force of law.

Significant points in the evolution of the classification system include:

- the expansion of the justification of the classification system to "protect the national security" rather than the narrower concept of national defense (E.O. 10290),

• resting the authority for the classification system on the broad executive power of Article II of the Constitution rather than on statutory grounds;

• extending the reach of the classification system beyond defense installations and equipment to the "Executive branch" in general,

• restoration of "national" defense as the operative term in E.O. 10501 (1961) while placing increased priority on the interest in public disclosure. The Order's opening paragraph provided that "it is essential that the citizens of the United States be informed concerning the activities of their government."

• a trend toward increasing emphasis on balancing the need for classification against the value of public disclosure. E.O. 11652 (1972), for example, began with the statement that "The interests of the United States and its citizens are best served by making information regarding the affairs of government readily available to the public ."

• a shift back towards classification in E.O. 12356 (1982), which states in its opening paragraph, "[I]t is essential that the public be informed concerning the activities of its Government, but... the interests of the United States and its citizens require that certain information concerning national defense and foreign relations be protected against unauthorized disclosure."

II Classification Structure

E O 10501 (1953) substituted for the existing four-level classification structure a three-level structure that has remained largely intact since then, although there have been changes in the definitions of classification categories The current categories are.

• *Top Secret* "Information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security" (Sec 1.1(1)(1)) Authority to classify is vested in the President, agency heads, and officials designated by one of the above,

• *Secret* "Information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security." (Sec 1.2(a)) Authority is vested in a slightly larger group of officials; and

• *Confidential.* "Information the unauthorized disclosure of which reasonably could be expected to cause damage to the national security." (Sec. 1.1 (a0(3)). Authority to classify is even wider. E.O. 12356 deleted the word "identifiable" before "damage" in the Confidential category.

III Administration

The National Security Council (NSC) has responsibility for the overall administration of the classification system. This responsibility was originally assigned to the NSC by E.O. 10501 (1953). The NSC was created by the National Security Act of 1947, 61 Stat. 495, July 26, 1947. Since 1978, the system has been administered by the Information Security Oversight Office (ISOO), a unit of the General Services Administration (GSA) that operates under the direction of the NSC. ISOO coordinates classification policy with the various executive agencies that have original classification authority as well as other agencies requesting classification authority (32 C.F.R. Secs. 2001-2003)

IV Information Categories

Since 1978, specific categories of information have been expressly designated in the executive orders on classification. The system now applies to the following:

(1) military plans, weapons, or operations;

(2) the vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security,

(3) foreign government information,

(4) intelligence activities (including special activities), or intelligence sources or methods;

(5) foreign relations or foreign activities of the United States,

(6) scientific, technological, or economic matters relating to the national security;

(7) United States Government programs for safeguarding nuclear materials or facilities;

(8) cryptology;

(9) a confidential source; or

(10) other categories of information that are related to the national security and that require protection against unauthorized disclosure as determined by the President or by agency heads or other officials who have been delegated original classification authority by the President."

Categories (2), (8) and (9) were added by E.O. 12356 (1982), although the information in these categories had previously been subject to classification under the catch-all "other categories of information" (E.O. 12065 (1978), Sec 1-3012(g)).

V. Enforcement

The unauthorized disclosure of classified information with intent to damage the national defense is subject to criminal prosecution. (18 U.S.C. 795, 797, 798) In addition, government employees with high-level security clearances must sign a lifetime promise to submit their writings for for prepublication review

Appendix B

Export Controls Pertaining to Technical Data

The current system of export controls reflects foreign policy, national security, and domestic economic considerations. The system is implemented through a variety of statutory authorities and administrative structures. Export controls may be directed at the commodity to be exported, at countries of designation, or at both.

Presidential authority to regulate exports derives from the broad grant of power to the executive to conduct foreign relations under Article II of the Constitution and from certain specific statutes. Those that affect directly the exporting of technical data are summarized below.

Export Administration Act of 1979, P.L. 96-72, September 29, 1979, 93 Stat. 503 (codified at 50 U.S.C. app. Sec. 2401), the principal foreign trade statute is administered by the Department of Commerce through the International Trade Administration in accordance with the Export Administration Regulations (EAR), 15 C.F.R. Parts 368-399.

The EAR applies to the exporting of unclassified data. (Exports of classified data are covered by the Arms Export Control Act, summarized below.) Enforcement of the EAR provisions is primarily the responsibility of the United States Customs Service, particularly the Technology Investigations Section within the Strategic Investigations Division.

The Commerce Department works with the Defense Department (through the Technology Security Administration) and other agencies to prepare the Militarily Critical Technologies List (MCTL) which supplements the Commerce Department's own Commodity Control List (CCL) (see 50 U.S.C. 2404(d)). Both lists designate sensitive applied technologies that the Defense Department wants to control. The MCTL itself is classified, but reportedly covers all newly created technical documents generated by DoD-funded research, development, test, and evaluation programs.

Controls are also assigned on the basis of the country of destination. (15 C.F.R. Secs. 370.2, 370.11(b), Supplement to Part 370, Part 385). The Coordination Committee for Multilateral Export Controls (COCOM) coordinates the efforts of the NATO member countries (except Iceland) and

Japan to control the export of sensitive technologies to communist countries. This also is administered through the Export Administration Act. (See 50 U.S.C 2416(e), 15 C.F.R. Sec. 370.11(c)).

Under EAR, "export" means "(i) an actual shipment or transmission of technical data out of the United States, or (ii) any release of technical data in the United States with the knowledge or intent that the data will be shipped or transmitted from the United States..." Data may be released for export through "(i) visual inspection by foreign national..., [or](ii) oral exchanges of information in the United States or abroad of personal knowledge or technical experience acquired in the United States." (15 C.F.R. Sec. 379.1(b)(1)(2))

"Technical data" means "information of any kind that can be used, or adapted for use, in the design, production, manufacture, utilization, or reconstruction of articles or materials. The data may take a tangible form, such as a model, prototype, blueprint, or an operating manual. The tangible form may be stored on recording media, or the data may take an intangible form such as technical service. All software is technical data." (15 C.F.R. Sec. 379.1)

A license from the Department of Commerce is required for lawful exporting. A general license is general authorization to export certain commodities, while a validated license governs particular exports to particular countries. For technical data, the relevant licenses are the GTDA (General License Technical Data Available to All Locations) and the Validated License (Technical Data).

Arms Export Control Act (22 U.S.C. 2751 *et seq.*, October 1', 1968). This Act regulates trade in armaments. Imports are administered by the Department of the Treasury. Exports are administered by the Department of State, Bureau of Politico-Military Affairs, Office of Munitions Control, in accordance with the International Traffic in Arms Regulations (ITAR) (22 C.F.R. Secs. 121-130). ITAR creates the U.S. Munitions List (22 C.F.R. Sec. 121.01) listing products that are subject to export control and for which export licenses are required. Enforcement and counterintelligence with regard to exports is primarily the responsibility of the Federal Bureau of Investigation. Like EAR, ITAR defines export to include the disclosure or transfer of technical data to a foreign person, whether in the United States or abroad.

Trading with the Enemy Act (50 U.S.C. Sec. 5) This statute regulates the export of goods to countries that are deemed to be hostile to the United States Presidential exercise of the authority to regulate under this Act is restricted to wartime, but the statute permits the President to retain continuing authority to regulate trade on an annual basis by issuing a proclamation declaring the need for such authority. (Memorandum of the President of the United States Extension of International Emergency Powers, 52 Fed. Reg. 33397 (August 27, 1987))

Patents The Patent and Trademark Office in the Department of Commerce is authorized to order "that the invention be kept secret and .. the grant of a patent [be withheld] whenever publication or disclosure by the grant of a patent might, in the opinion of the interested Government agency, be detrimental to the national security" if the government has a property interest in the invention (35 U S C. 181, based on c. 950, 66 Stat 805 (1952), Secrecy of Certain Inventions and Licenses to Export and File Applications in Foreign Countries, 37 C.F R. Secs 5 1-5.33). When the government does not have a property interest in the invention but the Commissioner of Patents and Trademarks determines that publication or disclosure by the granting of a patent might be detrimental to the national security, the Commissioner is directed to allow the appropriate agencies to inspect the applications, and the invention shall be kept secret and the grant of a patent withheld if the agency(ies) so finds The relevant agencies in this regard are the Departments of Defense and Energy, the National Aeronautics and Space Administration, and any other defense agency designated by the President (37 C F R Secs 5 1-5 33)

In addition to provisions that apply to all patent applications with a bearing on national security, applications for foreign patents are subject to additional procedures to prevent unauthorized disclosure to foreign countries

Atomic Weapons and Nuclear Materials The Atomic Energy Act of 1954 as amended by the Nuclear Non-Proliferation Act of 1978 (68 Stat 932 (1954), 92 Stat 126 (1978), 42 U S C 2011-2296) bars the export of "restricted data" in the absence of an agreement with the importing country governing the safekeeping, usage, and report of the data in the interests of nuclear nonproliferation and national security Exports may be restricted by type of data, by country of destination, or both Violations are punishable by injunctions, restraining orders, fines, or imprisonment

Appendix C

Presidential National Security Directives

National security directives are unpublished policy statements promulgated by the Executive branch without public disclosure or opportunity for public or congressional comment or oversight. Most legal commentators view them as legally binding within the Executive branch. These directives apparently date from the creation of the National Security Council in 1947. They were known as National Security Council Presidential ("P") and "Mill" Papers under Presidents Truman and Eisenhower. Presidents Kennedy and Johnson called them "National Security Action Memorandums" (NSAMs), Presidents Nixon and Ford had "National Security Decision Memorandums." A category known as National Security Council Intelligence Directives (NSCIDs) was apparently used by Presidents Truman through Nixon. President Carter issued "Presidential Directives," and President Reagan chose the name "National Security Decision Directives" (NSDDs).

In issuing national security directives, the President acts as legislator, chief executive, diplomat, and commander-in-chief of the armed forces. The directives' scope includes covert military and other security operations, access to computerized data bases (e.g., NSDD 145) and the transfer of technical data (e.g., NSDD 189).

Appendix D

Freedom of Information Act

The Freedom of Information Act (FOIA) (P.L. 89-487, 5 U.S.C. Sec. 552) was enacted on July 4, 1966, after a decade of congressional review of the availability of information in the hands of the Executive branch. It amended Section 3 of the Administrative Procedure Act of 1946 (APA), which stated that only "persons properly and directly concerned" could have access to official records.

The FOIA reversed the APA's underlying presumptions against public access to government records and set in place procedural and administrative mechanisms to protect the public's right to know. Under the FOIA "any person" can have access to identifiable agency records unless the information requested falls under one of nine specified exemptions. Properly withheld information includes records covered by executive orders on foreign or defense policies, trade secrets, personal and medical records, certain law enforcement records, regulatory records of financial institutions, and geological information concerning wells.

Unlike the APA, which provided no appeals mechanism for rejected requests, the FOIA allows someone denied access to information to appeal the denial to the head of the agency. If the administrative appeal is also denied, the requestor may then sue the agency in federal district court. In the judicial proceedings, the government bears the burden of justifying its withholding of the information and proving that the records fall under one of the nine exemptions.

In 1974, Congress amended the FOIA after identifying six major problem areas with compliance. Without deadlines for replies or penalties for violations, agencies were slow to respond and in many instances misused the statutory exemptions to keep information from the public. The 1974 amendments strengthened the FOIA by setting a thirty-day initial response time, allowing courts to conduct *in camera* reviews of materials to determine if they were properly withheld, establishing fee waiver and reduction guidelines, and requiring that documents containing segregable portions of sensitive information be released in expurgated form.

Two years later, Congress again amended the FOIA by passing the Government in the Sunshine Act (P.L. 94-409, September 13, 1976, 90 Stat. 1241, 5 U S.C Secs. 551, 552b, 557; Title 5 App., Sec. 10; Title 39, Sec. 410), which requires most agency meetings to be open to the public.

The 1986 amendments to the FOIA (Freedom of Information Reform Act of 1986, Subtitle N of H.R. 5484, The Anti-Drug Abuse Act of 1986) increased law enforcement agencies' rights to withhold certain records, and gave the Office of Management and Budget the authority to set fee schedules.

The 1984 Defense Department Authorization Act (P.L. 98-94, 97 Stat. 614, September 24, 1983) also contained a FOIA amendment. Section 1217 permits the Defense Department to "withhold from public disclosure any technical data with military or space application in the possession of, or under the control of, the Department of Defense, if such data may not be exported lawfully outside the United States without an approval, authorization, or license under the Export Administration Act of 1979. . or the Arms Export Control Act "

Access to information through the FOIA is also significantly affected by the classification guidelines set out in executive orders (see Appendix A), since classified documents are among those covered by FOIA exemptions

About This Series

This publication is one of eight papers that comprise the Benton Foundation Project on Communications & Information Policy Options. Papers may be ordered individually, or as a boxed set, by contacting the foundation at the address below.

Papers in this series include:

1 *The Role of Public Policy in the New Television Marketplace*
Jay G. Blumler
University of Leeds and University of Maryland

2 *Public Broadcasting*
Harry M. Shooshan III and Louise Arnheim
Shooshan & Jackson Inc.

3 *Charging for Spectrum Use*
Henry Geller and Donna Lampert
Washington Center for Public Policy Research
Duke University

4 *A Federal Right of Information Privacy: The Need for Reform*
Jerry Berman and Janlori Goldman
American Civil Liberties Union

5 *Watching the Watchers. The Coordination of Federal Privacy Policy*
George Trubow
The John Marshall Law School

6 *Strengthening Federal Information Policy Opportunities and Realities at OMB*
Gary Bass and David Plocher
OMB Watch

7 *A Presidential Initiative on Information Policy*
John Shattuck and Muriel Morisey Spence
Harvard University

8 *The Federal Structure for Telecommunications Policy*
Henry Geller
Washington Center for Public Policy Research
Duke University

Individual copies are $6.50 each, including postage and handling. The boxed set of eight papers is available for $33.00, including postage and handling. A bulk discount of 10% is available for orders of 10 or more copies of the same paper. Checks or money orders should be made payable to the Benton Foundation and mailed to:

Policy Options Project
Benton Foundation
1776 K Street, N.W.
Washington, D.C. 20006

BENTON FOUNDATION

1776 K Street, N.W.
Washington, D.C. 20006