Federal Policy-Making and National Security Controls on Information

SANDRA N. MILEVSKI

ABSTRACT

[*Author's Note:* The views expressed in this article are those of the author and do not necessarily reflect those of the U.S. National Commission on Libraries and Information Science.]

THIS ARTICLE REVIEWS the roles of the three branches of government in making policy for national security controls on information. It reviews legislative actions (statutes, appropriations, hearings) and executive actions (executive orders, regulations, contract provisions) in the post-war era with a focus on developments during the Carter, Reagan, and Bush presidencies.

INTRODUCTION

All three branches of the federal government—legislative, executive, and judicial—have a role in making information policy and, more specifically, in making policies governing national security controls over information. Such controls are most frequently exercised over technological data, data of a sensitive military nature, or information critical for trade considerations. In providing the various controls in effect today, the three branches have acted within the broad operational bounds provided by the Constitution—i.e., the legislature makes laws which are then interpreted and enforced by the executive with the judiciary having powers of final oversight.

HISTORY

A brief review of major national security actions since World

Sandra N. Milevski, U.S. National Commission on Libraries and Information Science, 1111 18th Street, NW, Suite 310, Washington, DC 20036
LIBRARY TRENDS, Vol. 39, Nos. 1 & 2, Summer/Fall 1990, pp. 132-44

War II traces the development and expansion of the concept. In the period immediately preceding and including the war, national security considerations were strictly limited to military affairs. The year 1940 marked the first in a series of Executive Orders (E.O.) issued by the president to establish policies and procedures for classifying information; E.O. 8381 (Roosevelt) served as the basis for all later executive revisions of the national security information classification system. In 1946, Congress took a more extreme stance than the president with enactment of the Atomic Energy Act, which was born of the secretive wartime Manhattan Project. This law provided that, unlike other military information which was to be reviewed and then classified, all nuclear-related information was automatically classified from its creation, regardless of its ownership and whether it was created in the public or private sectors. The 1950 Espionage Act provided for communications secrecy, including cryptography, and certain patent applications were to be delayed to protect them from public disclosure under the Invention Secrecy Act.

In 1947 the omnibus National Security Act revamped the organization of the entire defense establishment. It established the National Security Council (NSC) and the Central Intelligence Agency (CIA) and gave the latter responsibility for intelligence operations. In 1951 President Truman issued E.O. 10290 which stirred some controversy because it included in the national security classification system, for the first time, nonmilitary as well as military agencies. The emphasis was slowly changing from a wartime to a post-war mentality, and by 1954 the Atomic Energy Act was revised to meet the needs and concerns of private enterprises involved in the nuclear industry.

Over the next two decades, four Executive Orders refined the classification system: E.O. 10104 and 10501 (Eisenhower, 1953); E.O. 11652 (Nixon, 1972); and E.O. 12065 (Carter, 1978). The Nixon E.O. marked an expansion of the concept of national security by adding "foreign relations" (a vague term exceeding policy considerations to include diplomacy and operations) to the national defense formula to comprise national security. The Carter E.O. limited the extent of classification by introducing two new criteria for classification: (1) damage to national security had to be identifiable and not just potential, and (2) when deciding whether to declassify a previously classified document, officials were to apply a "balancing test" of whether the value of the information to the public exceeded the threat to national security.

The executive has perhaps more leeway in establishing national security controls than the other two branches of government because

of its dominance in the foreign relations domain, its many agencies writing regulations that interpret the laws of Congress, and its ability to act quickly and seize the initiative when compared with the legislature and the judiciary. Harold C. Relyea (1987) has said that "national security remains a largely ambiguous concept often appearing but otherwise undefined in Federal statutes, given considerable deference and latitude by the judiciary, and affording the executive enormous power and broad discretion regarding its application" (p. 22).

The federal agencies most frequently involved in national security controls include the Departments of Commerce (export controls), Defense (contract provisions), Energy (nuclear information), and State (immigration). National security considerations have prompted these agencies, as well as components of the Executive Office of the president such as the National Security Council, the Central Intelligence Agency, and the Office of Management and Budget, to classify information and impose other secrecy restrictions, limit the export of goods and information, delay or prevent the issuance of patents, and attempt to censor the communications of certain classes of citizens, such as scientists and federal employees and contractors.

Over the past decade in particular, the content and manner of implementation by the executive branch of various national security controls over information have engendered controversy because of their circumscription of national traditions of intellectual freedom and international traditions of open scientific communication. This trend began in the late 1970s during the Carter Administration when various scientific, educational, and other types of exchanges between the Soviet Union and the United States were curtailed; when the administration sought to forestall publication of the (unclassified) memoirs of a former CIA operative and of information on assembling a hydrogen bomb, and when the unprovoked Soviet invasion of Afghanistan in December 1979 brought detente to a crashing halt. A series of "spy scandals," unfolding over several years, followed. During this time the first attempts by the government to limit scientific communication were begun, and the Supreme Court in *Snepp v. United States* (1980) decided that secrecy agreements imposed upon the intelligence community are constitutional.

Concern over the outflow of U.S. technological information was genuine and widespread among those knowledgeable in the area; it was not a creation of overzealous government censors. In the late 1970s commercial competitors and hostile military parties stepped up their efforts to acquire such data. The Soviet Union in particular shifted from an exclusively military focus to an all-inclusive one,

targeting the civilian sector and universities as well. These efforts prompted Admiral Bobby R. Inman (1982) to utter his famous remark about the "hemorrhage of the country's technology." Various professional societies reviewed the situation, and the American Council on Education recommended voluntary prepublication review for sensitive manuscripts in the field of cryptography. A 1976 Department of Defense task force chaired by J. Fred Bucy, president of Texas Instruments, had already emphasized the need to hold back the technology but not the basic science. It was the Bucy Report (Dept. of Defense, 1976) which introduced the concept of "critical technologies" which was the basis of the 1979 Export Administration Act. Thus controversy surrounding national security controls stems not from their need, but from the degree and methods of implementation.

The federal government's statutory authority to impose national security controls is elaborated by executive branch administrative regulations, contract provisions stemming from them, and presidential directives. Pertinent statutes include the aforementioned Atomic Energy Act, the Invention Secrecy Act, the Arms Export Control Act, the Export Administration Act, the Immigration and Nationality Act (McCarran Act), plus the federal agency-generated regulations governing their implementation. The well-known Freedom of Information Act does not apply to national security considerations as explained later.

Statutes and Companion Regulations

Enacted in 1946 and amended in 1954, the Atomic Energy Act establishes a category of data—"restricted data"—dealing with atomic weapons and nuclear materials over which the federal government has exclusive jurisdiction, regardless of the creator of the data. Private individuals or enterprises creating such data with private funds as well as federally funded contractors and federal employees are equally liable under this law, which was the authority cited in 1979 when the Carter Administration opposed *The Progressive,* which published directions for assembling a hydrogen bomb. In 1981 Congress further amended this act to allow the Secretary of Energy to halt the dissemination of unclassified information if it could have a negative effect on the common defense or on public health and safety. In April 1985, the Department of Energy completed work on and issued the final regulations accompanying this amendment which prohibits the unauthorized disclosure of "Unclassified Controlled Nuclear Information" (UCNI).

The Invention Secrecy Act (1951) is designed to allow the federal government to control private technological data revealed in patent

applications if it might harm national security. Developed for wartime situations and made permanent in 1952, it charges the Patent Commissioner with reviewing patent applications and if, in his opinion, their disclosure might be detrimental, passing them on to the defense agencies for review. The agencies may decide for secrecy, in which case the Patent Office may withhold any given patent for one year. This period of time may be extended, but the applicant may also appeal to the Secretary of Commerce and make claims for damages and compensation through the court system.

The Arms Export Control Act (1976) controls the export of goods and materials from the United States and the access which foreign citizens may have to the same within this country. Such controls have been in place for over fifty years, first under a joint resolution of Congress (1935), then under the Neutrality Act (1937-39) and the Mutual Security Act (1954). The International Traffic in Arms Regulations (ITAR) that accompany the act include certain scientific information—"technical data"—as a category of exportable (or nonexportable) good, and, in addition, define the term "export" so broadly as to encompass release of the information within the United States. The Department of State, with the assistance of the Department of Defense, maintains the companion list of embargoed goods—the U.S. Munitions List. The term "list" is a misnomer since its size approximates that of the Manhattan telephone directory.

The more recent Export Administration Act (1979, as amended in 1981, 1985, and 1988) has a similar function and is implemented through the Export Administration Regulations. The Department of Commerce maintains the accompanying Commodity Control List for dual use items, while Commerce along with Defense and Energy compile the Militarily Critical Technologies List. The latter list, over 700 pages long, is itself a classified document.

The original Export Administration Act was due to expire automatically during the 98th Congress. As the Congress progressed and lawmakers realized that they would not be able to complete a full reauthorization before the act lapsed, they twice passed legislation temporarily extending it from September 30, 1983 to October 14, 1983 (PL 98-108) and again from February 29, 1984 to March 30, 1984 (PL 98-222). However, Congress failed to pass a permanent law before its expiration on March 30 and before the conclusion of the 98th Congress, and President Reagan issued an Executive Order (E.O. 12470) on that same day, just as he had in the interim period between October and February. Both Executive Orders declared a state of national emergency and invoked the International Emergency Economic Powers Act to continue the export controls. When the 99th Congress finally passed the Export Administration Amendments

Act of 1985 (PL 99-64), the president revoked the state of emergency with another E.O. (12525). This seesaw serves to illustrate the superior speed and flexibility which the executive enjoys over the relatively lumbering pace of Congress.

As of this writing, the most recent revisions to the rules governing the Commodity Control List were published by Commerce's Bureau of Export Administration in the February 28, 1989 *Federal Register.* Amendments made to the Export Administration Act by the 1988 Omnibus Trade and Competitiveness Act (PL 100-418) called for changes that include enhancing multilateral controls over technology exports, easing exports to the People's Republic of China, simplifying licensing requirements, reducing processing times, reducing the size of the list, and defining the roles of the various agencies involved (the act also provided penalties for Toshiba Machine Company and Kongsberg Vaapenfabrik, which sold controlled technology to the USSR). Other changes in the regulations stemmed from recommendations of the Secretaries of State and Energy and from multilateral strategic controls reviews held by the United States and allied countries through the coordinating committee (COCOM).

A recently enacted law expands the two export control acts explained earlier. The Department of Defense Authorization Act for fiscal year 1984 (PL 98-94) allows DoD to withhold technical data under its control from domestic public disclosure if those data fall under nonexportable categories on any of the lists or if they require a license or approval for export. Two DoD directives issued in November 1984 elaborate on the law. This provision reinforces the earlier regulations' broad interpretation of the definition of "export," which includes the domestic dissemination of information to be kept from foreign nationals. The key terms within the context of these three statutes are "technical data" and "export"; any data or information falling under these terms need not undergo the classification process for dissemination to be prohibited. The 1985 regulations provide for a system of seven levels of markings (unclassified/unlimited; DoD; DoD and contractors; federal government; federal government and contractors; special class; subject to export control) on documents to identify the type of source and to expedite release of the information without the need to trace the originating organization (Young, 1985).

A final statute providing authority for the application of national security controls within the United States is the Immigration and Nationality Act ("McCarran Act," 1952) which allows the Department of State to deny entry to this country to foreign nationals because of their political and ideological beliefs. Upheld by the Supreme Court in *Kleindienst v. Mandel* (1972), this act serves as the basis

for actions started in the late 1970s by the Department of State, sometimes in conjunction with Commerce in its export control capacity, to prevent foreign scientists, students, and others from acquiring sensitive information through participation in conferences, attending classes in certain subjects, or performing laboratory research.

The first well-known incident occurred in February 1980 when the American Vacuum Society was forced to rescind invitations to its international meeting. Early in 1981 the State Department informed Cornell University that certain East European foreign visitors would be limited to classroom activities. In the fall of that year, the State Department advised university administrators to exclude students from the People's Republic of China from studies and/or research in certain fields.

The limitations on scientific communication and academic freedom which these visa conditioning and campus policing requirements represented mobilized the science and academic communities, which have released a series of reports on the matter. Early examples are the landmark September 1982 National Academy of Sciences (1982) report "Scientific Communication and National Security," based on findings of a panel chaired by Dale R. Corson and the April 1984 American Association for the Advancement of Science compilation of all visa and import control incidents affecting professional societies and their meetings. In September 1985, the presidents of twelve scientific and engineering societies sent a letter to the Secretary of Defense to state that their organizations would no longer allow restricted meeting sessions. The government has responded to these concerns through a number of mechanisms—such as a 1982 Defense Science Board Task Force on University Responsiveness to National Security Requirements report, a 1983 statement by the State Department on applying appropriate McCarran Act restrictions when denying or restricting visas, an ad hoc DoD-University Forum chartered in 1984 as a permanent advisory committee to the DoD. Later presidential directives do not indicate a change of direction.

Although this listing indicates major laws from which the executive agencies derive authority to promulgate national security controls regulations, it is not exhaustive. Some narrower statutes, in turn, elaborate on actions derived from the president's authority. One example is the Classified Information Procedures Act which governs the introduction of classified information in open court and was recently an issue in the Oliver North trial (Lardner, 1989).

Although the Freedom of Information Act (1966) is the best known vehicle for obtaining from the federal government what

otherwise might be closely held information, it does not apply in cases with national security considerations. Thus national security information is excluded from FOIA requests as a category. The FOIA codifies the citizens' right to know as based in the First Amendment right to petition; previously, the release of federal information was at the agencies' discretion, which frequently operated on a need-to-know basis. However, the law specifies nine categories of information which may be (but do not necessarily have to be) protected from disclosure. These include categories: (1) information already properly classified as secret under an executive order; (3) information excepted from disclosure by a statute which specifies withholding in either a nondiscretionary manner, or according to particular criteria, or by broader categories or types; and (4) trade secrets or privileged or confidential commercial or financial information (most FOIA requests are from commercial enterprises seeking information about their competitors). Thus national security information is excluded from FOIA requests as a category.

The FOIA was amended and strengthened in 1975 to provide the same kind of court review for national security information as for other information, but in the 98th Congress an exemption from FOIA requests was granted for certain CIA operational files. Because the FOIA applies exclusively to the executive branch of the government (Congress having exempted itself from FOIA requirements, as it frequently does with other legislation), it sets up a situation of ongoing tension between the people's right to know and the exercise of the chief executive's executive privilege, a doctrine of refusal to divulge state secrets practiced by every president since George Washington.

Contract Provisions

A third source of authority within the federal government for instituting national security controls stems from its power of the purse. The ultimate power to allocate funds lies with Congress, which can, however, authorize a program but in effect kill it by not providing an appropriation of funds for its operation. For national security applications, however, this power is most often exercised on a daily basis by the Department of Defense through its spending in support of research and development and on various commercial contracts. Thus the department may impose secrecy requirements on the results of research conducted not only by federal employees but also by private parties in industry or academe whose projects are even partially federally funded. According to experts at the American Physical Society, some 75 percent of all federally funded research and development performed in this country is DoD-sponsored, and the

DoD share of basic research and academic science, where it is not dominant, is steadily increasing (R. L. Park, Director, Office of Public Affairs, American Physical Society, to author, personal communication, November 1987). Even when the agency does not impose its own restrictions through contract provisions or cannot invoke the export licensing requirements or security classification, a contractor who fails to comply with agency wishes in such matters decreases his chances of being awarded subsequent contracts.

Presidential Directives

The series of executive orders mentioned earlier established and developed the classification system and identified seven categories of information which could be classified. These are listed in E.O. 12065 (1978) as: (a) military plans, weapons, or operations; (b) foreign government information; (c) intelligence activities, sources, or methods; (d) foreign relations or foreign activities of the United States; (e) scientific, technological, or economic matters relating to national security; (f) U.S. government programs for safeguarding nuclear materials or facilities; or (g) other categories of information which are related to national security and which require protection against unauthorized disclosure.

In April 1982, the Reagan Administration issued the latest presidential revision of the classification system as E.O. 12356 to take effect that August. This executive order reversed the previous trend toward greater openness by introducing a number of changes. The executive order:

—removed the presumption in favor of a less restrictive classification or no classification in cases of "reasonable doubt";
—removed the "identifiable damage" criterion and replaced it with a reasonable expectation of damage;
—cancelled the automatic declassification of documents after six years and provided for classification as long as required by national security considerations;
—removed the requirement to balance public interest with the need to protect national security ("balancing test");
—provided new authority for officials to reclassify after a document had been declassified or was already in the public domain;
—added the option, at agency discretion, of classifying privately funded basic research, which was previously excluded.

Developed without the opportunity for public comment and the object of extensive Congressional criticism in oversight hearings (U.S. Congress, 1982), this E.O. now defines the classification process and serves as a basis for further executive branch agency actions.

In December 1982, the administration extended its nondisclosure efforts from classified to unclassified information by establishing an interagency task force to review the vulnerability of sensitive information which did not meet classification guidelines. The following March, the administration issued National Security Decision Directive (NSDD) 84, which targeted federal employees as potential sources of sensitive information but also included federal contractors in its scope. In its original form, NSDD 84 mandated lifelong nondisclosure agreements for federal employees with security clearances, prepublication reviews of works written by employees with the highest security clearances (i.e., access to "Sensitive Compartmented Information" [SCI]), polygraph examinations in the course of investigations, and strictures on contacts between employees and the media.

That same fall, Congress placed over a dozen limitations on NSDD 84 including prohibition of polygraph examinations and limitations on several SCI provisions. Undaunted, the administration tried again in November 1985 with NSDD 196, itself a classified document. This directive, administered by the CIA, required all agency personnel with access to SCI (estimated at over 182,000 federal employees and contractors) (ALA, 1986) to submit to polygraph examinations. The controversy aroused was sufficient to prompt the administration to rescind the directive in September 1986. (Congress followed up by passing PL 100-347 which the president signed into law in June 1988. The law restricts the use of polygraph examinations by private sector employers, but federal and state governments as well as national security agencies and their contractors are among the exemptions.)

In the meantime, Standard Form 4193, a lifelong prepublication agreement for those with access to SCI, had been introduced to supplement the much more common Standard Form 189, the result of NSDD 84. This pledge not to reveal classified or *classifiable* information applies to all federal employees with security clearances and introduced the concept of "sensitive but not classified information." The definition of classifiable information provided in the *Federal Register* (1987a) elicited sufficient negative comment to be later revised (1987b) to eliminate currently unclassified information which might, at some future time, become classified. By December 1987, Congress had taken temporary action to bar the use of both of these standard forms (language in 1987 and 1988 appropriations bills prohibiting the use of appropriated funds to produce or disseminate SF-189), but many previously signed pledges are still extant.

Under President Bush, SF-312, developed in 1988 to succeed SF-189, defines classified information as including written and *oral* communications that, if they were written, would be classified or in the process of being classified. It provided for punishment of federal employees who divulge information that they know or *should know* is classified or is in the process of being classified. In the 1990 Treasury, Post Office, and General Government Appropriations bill, Congress again prohibited the use of federal funds to print or disseminate SF-312; President Bush protested that language but signed the bill into law nevertheless.

Another presidential directive of September 1984, NSDD 145, dealt only with information in electronic format and focused on security safeguards for telecommunications, computer systems, and other automated information systems handling sensitive but unclassified government information. It promoted a comprehensive, coordinated approach on the assumption that isolated items of unclassified information, when aggregated with other such items, could, in sum, reveal sensitive matters. However, the directive did not define what such sensitive but unclassified information is.

An October 1986 memorandum signed by then-National Security Adviser John M. Poindexter (NTISSP #2 "National Policy on Protection of Sensitive but Unclassified Information in Federal Government Telecommunications and Automated Information Systems") implemented NSDD 145 and "defined" sensitive but not classified information by leaving what was deemed sensitive to the discretion of each federal department and agency. This Poindexter memorandum also gave the National Security Agency the preeminent role in federal computer/communications security matters.

Government agency representatives soon started acting on NSDD 145 and NTISSP #2 provisions. In 1986, Mead Data Central and other database creators and vendors were reporting visits by DoD, FBI, and CIA representatives seeking to limit foreign access, through legal and technological means, to databases which might contain easily aggregated sensitive information. Widespread protests against this practice and the Poindexter memorandum resulted in the rescission of NTISSP #2 by Poindexter's successor, Frank Carlucci, in March 1987 (it is commonly believed that the rescission was largely decided by a desire to disassociate the Poindexter name from further controversy in the wake of the Iran-Contra scandal). Congress also responded definitively with the Computer Security Act of 1987 which limits the National Security Agency's role in federal computer security to military agencies and assigns the National Bureau of Standards

(now National Institute of Standards and Technology) responsibility for computer security in all civilian agencies. However, NSDD 145 still remains in effect.

Future Prospects

The administration's continuing concern with national security and its increasing control over related and potentially related information during the past decade appear to be continuing from the Carter to the Reagan and now into the Bush presidencies. Two days before his departure from office, President Reagan signed E.O. 12267 which establishes "policies and procedures governing the assertion of Executive privilege by incumbent and former Presidents in connection with the release of Presidential records..." (U.S. Office of the President, 1989, p. 1). The order sets up procedures to review records of the present and former presidents and to invoke the executive privilege of secrecy by either if "disclosure...might impair the national security (including the conduct of foreign relations), law enforcement, or the deliberative processes of the Executive branch" (p. 1). According to this E.O., only a final court order can override an incumbent president's claim of privilege.

Press reports early in the Bush presidency state that the administration is circulating a draft executive order on classified information which would establish uniform standards for granting security clearances throughout the executive branch. It would also eliminate the requirement that agencies provide a reason for denial and the chance to respond for those federal employees and government contractors who are denied such clearances. This would remove all rights of due process in such instances.

Congressional reaction to the draft proposal has been negative. Representative Don Edwards, chair of the House Judiciary Subcommittee on Civil and Constitutional Rights, urged Bush not to sign the draft version: "a person denied a clearance on the basis of erroneous information...would never have an opportunity to correct it (Marcus, 1989, p. A4). The chairmen of six major House committees wrote to Bush to express their concern over the potential violation of civil rights and promised legislative action to counter that threat. Subsequently, in a March 24 memorandum, Bush authorized a complete review of the proposal by an interagency working group of lawyers who had not previously worked on the issue (Devroy & Marcus, 1989, p. A13). However, the final word on this question may be spoken by the judiciary. In *Department of the Navy v. Egan,* the Supreme Court decided that no one has the "right" to a security clearance and therefore "procedural safeguards derived from the common law may not be appropriate in security-clearance cases."

However the saga of national security controls over information continues to unfold, the mechanisms for policy-making in this field at the federal level remain unchanged: Congressional statutory authority and supplemental "pressure" through oversight hearings, appropriations, and histories of legislative intent; executive initiatives such as presidential directives, executive agency development of regulations to accompany statutes, and contract provisions; and the relatively rarely applied powers of review of the judiciary. It remains for the interested citizen, both proponent and opponent of the many forms of control now in existence, to monitor the actions of government and lobby in appropriate places to effect an optimal balance of needed security controls with freedom of information.

References

American Library Association. (1986). *Less access to less information by and about the U.S. government: 2: A 1985-86 chronology: January 1985-December 1986.* Washington, DC: American Library Association.

Department of Defense. Office of the Director of Defense Research and Engineering. (1976). *An analysis of export controls of U.S. technology—a DoD perspective: A report of the defense science board task force on export of U.S. technology.* Washington, DC: Department of Defense

Devroy, A., & Marcus, R. (1989). President to take a 'fresh look' at proposed security clearance order. *Washington Post,* April 20, Sec. A, p. A13.

Inman, B. R. (1982). Address at the American Association for the Advancement of Science Annual Meeting, Washington, DC, January 3-8.

Lardner, G., Jr. (1989). U.S. joins North case abruptly. *Washington Post,* February 9, Sec. A, pp. A1, A23.

Marcus, R. (1989). Plan to deny clearances without explanation eyed. *Washington Post,* February 10, Sec. A, p. A4.

National Academy of Sciences. Panel on Scientific Communication and National Security Committee on Science, Engineering, and Public Policy. (1982). *Scientific communication and national security.* Washington, DC: National Academy Press.

Relyea, H. C. (1987). National security and information. *Government Information Quarterly, 4*(1), 11-28.

U.S. *Federal Register* (1987a). February 21, p. 48367.

U.S. *Federal Register* (1987b). August 11, p. 29793.

U.S., Congress, House, Committee on Government Operations. (1982). *Security classification policy and executive order 12356.* Washington, DC: USGPO.

U.S., Office of the President. (1989). Executive order 12267. *Weekly compilation of presidential documents, 25*(1), 82-83.

Willard, R. K. (1989). "No one has a 'right' to a security clearance. *Washington Post,* March 25, Sec. A, p. A13.

Young, L. (1985). DoD publication policy. In B. J. Meredith (Ed.), *The international flow of scientific and technical information* (Presented at the FLICC Forum on Federal Information Policies, 27 February 1985) (pp. 5-7). Washington, DC: Library of Congress.