BNA, INC.

MEDICAL RESEARCH LAW & POLICY

BNA Employee-Owned Since 1947

REPORT



# Publication Restrictions in Federal Research Contracts: *Recent Developments Invite Clarification of Government Policy*

BY ALEXANDER E. DREIER, ESQ.

University administrators report a recent increase in the number of federal research agreements that contain provisions restricting the publication and dissemination of information that is not classified.[1] It is clear that the government may prohibit publication or release of classified material. But federal agencies are now more apt to place restrictions on research results that are unclassified yet still deemed ''sensitive,'' usually on the ground that the information may implicate national security interests. This development not only has implications for research, it also raises broader questions concerning the proper scope of government controls on unclassified information.

Reports issued this year by the Congressional Research Service highlight these questions and note they are attracting increased attention from Congress, other policymakers, and the academic community.[2] Controversy surrounds the issue. In February 2002, for example, the U.S. Department of Defense (''DoD'') issued a draft report that would have required researchers to obtain DoD approval before discussing or publishing findings of all military-sponsored unclassified research. Critics, including many academics, objected, and the report was withdrawn.[3]

Publication restrictions strain many universities' ability to accept a federal grant or contract. Agreeing to the limitations may violate institutional policies or at least conflict with a culture of free inquiry and academic freedom. Many universities' policies expressly prohibit giving a research sponsor the right to censor or veto publication of research results.[4] Some universities have turned down research funds because the sponsoring agency would not agree to remove a publication restriction provision from the funding agreement.[5] More broadly, many fear that limitations on dissemination of research may slow scientific progress in areas, such as understanding biological agents usable as weapons, where progress is needed most.

In some circumstances, publication restrictions also may result in research becoming subject to export controls. These can complicate university research, particularly where the research team includes non-U.S. citizens. In this context, two export regulations may come into play. The International Traffic in Arms Regulations (ITAR) require a license to export ''defense articles''

[1] *See* Genevieve J. Knezo, '' 'Sensitive But Unclassified' and Other Federal Security Controls on Scientific and Technical Information: History and Current Controversy,'' Congressional Research Service (April 2, 2003) at 1; Anne Marie Borrego, ''Colleges See More Limits on Research,'' *The Chronicle of Higher Education*, Nov. 1, 2002, at A24.

[2] Knezo, *supra*; Dana A. Shea, ''Balancing Scientific Publication and National Security Concerns: Issues for Congress,'' Congressional Research Service (Jan. 10, 2003).

*Alexander E. Dreier is an attorney with Hogan & Hartson LLP in Washington, D.C.*

[3] *See* Ron Southwick, ''Pentagon Backs Away from Strict Controls on Basic Research,'' *The Chronicle of Higher Education*, May 31, 2002, at A21.

[4] *See, e.g.*, the report of the Massachusetts Institute of Technology *ad hoc* faculty group, *In the Public Interest*, *available at:* http://web.mit.edu/newsoffice/nr/2002/publicinterest.html.

[5] *Id.*

 ISSN 1539-1035

and related technical data, a category that includes materials that may be present in university laboratories.[6] The Export Administration Regulations (EAR) require a license to export specified ''dual-use'' items, *i.e.*, those that have potential military and civilian application, as well as related technical data.[7] Both sets of regulations treat release of covered technical data to foreign nationals as ''exports,'' even if the data never leave the United States.[8] However, they often do not apply to universities because fundamental research is exempt from the requirements. But when the research sponsor attaches publication restrictions to funding, a university may find that the ''fundamental research'' exemption is no longer available under the regulations.[9]

In addition to their impact on universities, publication restrictions also can implicate a policy issue of broader national concern: How should results of basic scientific research that include sensitive information that could aid terrorism or pose other national security threats be protected? One possibility is for the government to expand authority to classify information. After Sept. 11, 2001, the heads of several agencies responsible for a great deal of research—the Department of Health and Human Services, the Department of Agriculture, and the Environmental Protection Agency—were given new classification authority.[10] This development suggests the possibility that more research will become classified. An alternative approach is government controls, short of classification, on unclassified information that an agency deems to be sensitive. That seems to be the method adopted by several agencies in restricting publication of research findings. Either method, though, when applied to basic research at universities, creates friction with established federal policies, which presume that results of basic research should be unclassified and unclassified basic research should be subject to no government controls.

## *Federal policy concerning ''sensitive but unclassified'' information*

Long-standing federal policy permits classification of federal information as ''top secret,'' ''secret,'' or ''confidential.'' Since before World War II, the government generally has declined to classify basic scientific research,[11] and to impose publication restrictions on nonclassified basic research.[12] During the 1980s, concern about access of foreign scientists and students to information subject to export controls prompted DoD to restrict presentation of such information at conferences and in classrooms.[13] A 1984 National Security Defense Directive ordered that ''sensitive, but unclassified, government or government-derived information, the loss of which could adversely affect the national security interest'' should be ''protected in proportion to the [national security] threat.'' As recounted in a recent Congressional Research Service report, the General Accounting Office and others criticized the absence in the directive of a precise definition of ''sensitive, but unclassified'' and voiced concern that this category might be interpreted so broadly as to cover a wide range of government-generated information.[14]

The ensuing controversy led the Reagan administration in 1985 to issue a directive, known as NSDD-189, to clarify federal policy.[15] It affirmed that ''to the maximum extent possible, the products of fundamental research remain unrestricted.'' Specifically, the directive said that ''[n]o restrictions may be placed upon the conduct or reporting of federally-funded fundamental research that has not received national security classification, except as provided in applicable U.S. statutes.''[16] NSDD-189 thus reflects a national policy to curtail restrictions on fundamental university research, and to ensure that the primary mechanism for controlling such research is classification.

The Bush administration has reaffirmed the continuing validity of that policy since the Sept. 11, 2001, attacks and the subsequent anthrax attacks. National Security Advisor Condoleezza Rice specifically confirmed in November 2001 that NSDD-189 remains the policy of the government.[17] The State Department also separately stated that NSDD-189 remains in effect and that the State Department has no intent to regulate fundamental research.[18] In October 2002 testimony before a House committee, the director of the White House Office of Science and Technology Policy (''OSTP'') acknowledged there was an ''impression that the administration is considering a policy of prepublication review of sensitive federally funded research. This is incorrect,'' he said. In an interview, he added: ''There has been no general change, either in the presidential directive or the policies within Department of Defense research.''[19]

Other federal policy statements seem to confirm this. A 1995 directive—Executive Order 12958—affirmed that the government may classify ''scientific, technological, or economic matters relating to the national security'' but prohibited classification of ''basic scientific research information not related to the national security.''[20] Although President Bush in March 2003 amended that order by explaining that matters relating

---

[6] 22 C.F.R. Part 121.

[7] 15 C.F.R. § 774.

[8] *See* 22 C.F.R. § 120.17(4); 15 C.F.R. § 734.2(b).

[9] *See* 22 C.F.R. § 120.11(8) (exempting information made available to the public ''through fundamental research in science and engineering at accredited institutions of higher learning in the United States where the resulting information is ordinarily published and shared broadly in the scientific community''); 15 C.F.R. § 734.8.

[10] *See* Knezo, *supra*, at 39.

[11] Basic research has been defined as ''experimental or theoretical work undertaken primarily to acquire new knowledge of the underlying foundation of phenomena and observable facts, without any particular application or use in view.'' Shea, *supra*, at 1 n.3 (quoting Organisation for Economic Cooperation and Development, *Frascati Manual* 30 (2002)).

[12] A notable exception is certain nuclear fission research, which is ''born classified'' under the Atomic Energy Act. *See* Shea, *supra*, at 6.

[13] *See* Knezo, *supra*, at 11.

[14] *See id*.

[15] National Security Decision Directive 189, ''National Policy on the Transfer of Scientific Technical and Engineering Information'' (Sept. 21, 1985), *available at:* http://www.fas.org/irp/offdocs/nsdd/nsdd-189.htm.

[16] *Id*.

[17] *See* Letter from C. Rice to H. Brown, Nov. 11, 2001, *available at:* http://www.fas.org/sgp/bush/cr110101.html.

[18] International Traffic in Arms Control Regulations; Exemptions for U.S. Institutions of Higher Learning, 67 Fed. Reg. 15,099 (March 29, 2002).

[19] Borrego, *supra*.

[20] Executive Order 12958, Classified National Security Information, 60 Fed. Reg. 19,825, 19,827, 19,829 (April 17, 1995).

  MRLR ISSN 1539-1035

to ''defense against transnational terrorism'' are among those eligible for classification, he retained the bar on classification of basic scientific research not related to the national security.[21]

These general pronouncements imply that government policy on publication of unclassified university research has not changed fundamentally since the 1980s. But universities' experience in individual cases suggests that some federal agencies are taking a different approach. To illustrate, it is useful to consider one contractual provision that one agency—DoD—has included in some research contracts.

## *Case study: Restrictions in Department of Defense research agreements*

Some DoD research contracts include a clause (''the DFARS Disclosure Clause''), found in the DoD Federal Acquisition Regulations Supplement, which provides that the ''Contractor'' may not release to anyone outside the Contractor's organization ''any unclassified information . . . pertaining to any part of this contract'' without the agency's written approval.[22] If a university is the Contractor, then the DFARS Disclosure Clause would appear to require the university to obtain advance approval before publishing any research results pertaining to the university's work under the contract. Such a restriction would be unacceptable to many universities because it is contrary to university policy, as noted above.

There are two obvious solutions to this problem. First, the university could seek to have the disclosure clause removed from the contract. Alternatively, the university could ask that the responsible contracting officer give advance written approval to the university's publication of any and all research results pertaining to the university's fundamental research under the contract.

Another possible resolution exists if the university is a subcontractor. Although the prime contractor generally would be required to ''flow down'' the Disclosure Clause to subcontractors, it may have some latitude to frame any flow-down clause to accommodate the circumstances of each subcontract. For example, the DFARS Disclosure Clause obligates the prime contractor to flow down a requirement that is ''similar'' to the requirement imposed on the prime contractor itself.[23] In these circumstances, a prime contractor might be able to take the position that the Disclosure Clause should not literally apply to a university subcontractor because it would violate policies of the university as well as policies of the federal government.

Some universities confronted with the DFARS Disclosure Clause in a proposed contract have noted that it seems to conflict with other DoD policies concerning restrictions on fundamental research results. Specifically, one DoD directive provides that ''[t]echnical documents resulting from contracted fundamental research efforts will normally be assigned Distribution Statement A''—*i.e.*, ''Approved for public release; distribution is unlimited''—''except for those rare and exceptional circumstances where there is a high likelihood of disclosing performance characteristics of military systems, or of manufacturing technologies that are unique and critical to defense . . . .''[24] Thus, where university research does not fall within the ''rare and exceptional circumstances'' in which dissemination of research results may be restricted, this directive would seem to indicate that no restrictions should be placed on distribution or publication of any technical documents resulting from the research.

Another DoD policy provision holds that security classification is the only permissible mechanism for controlling information generated by DoD grants and contracts, unless another means is authorized by law. It states DoD policy to ''[a]llow the publication and public presentation of unclassified contracted fundamental research results. The mechanism for control of information generated by DoD-funded contracted fundamental research in science, technology, and engineering performed under contract or grant at colleges, universities, and nongovernmental laboratories is security classification. No other type of control is authorized unless required by law.''[25] DoD also sets out ''criteria for identifying fundamental research activities performed under contract or grant that are excluded from [prepublication] review requirements.'' The criteria provide that research funded by budget Category 6.1 (''research'') or 6.2 (''exploratory development'') and performed on-campus at a university is ''fundamental'' except in ''rare and exceptional circumstances where the [research] presents a high likelihood of disclosing performance characteristics of military systems or manufacturing technologies that are unique and critical to defense.''[26] This provision seems to create a strong presumption against publication restrictions for unclassified research.

DoD so far has not amended any of these policy statements in a way that would seem to permit a more restrictive approach to university research. A recent proposal would have amended DoD Directive 5200.39, which currently protects critical acquisition program information, technology, and systems, by extending it to include basic scientific research funded by DoD. Among other things, the amendment would have required agency approval before public release of technical data deemed to be critical research.[27] However, the proposed amendment was withdrawn because of concern in the research community about the publication restriction.[28]

Another complicating factor is inconsistent use of these provisions in apparently similar circumstances. Universities have reported a number of instances in which agencies, including those within DoD, initially have proposed, but then agreed to delete or moderate, the Disclosure Clause language in negotiations with universities. In one such instance, the agency originally proposed to include the Disclosure Clause, but, after

[21] Executive Order 13292, Further Amendment to Executive Order 12958, as Amended, Classified National Security Information, 68 Fed. Reg. 15,315 (March. 25, 2003).

[22] 48 C.F.R. § 252.204-7000.

[23] *Id*.

[24] DoD Directive 5230.24, E3.1.1.1.1 (March 18, 1987).

[25] DoD Instruction No. 5230.27 (Oct. 6, 1987).

[26] DoD Directive 5230.24, E3.1.1.1.1.

[27] *Cf*. DoD Directive 5200.39 (Sept. 10, 1997).

[28] The withdrawal of the proposed policy is described in a Congressional Research Service Issue Brief, *available at:* http://www.cnsr.org/CRSs_t.pdf. *See also,* Don J. DeYoung, ''Federation of American Scientists White Paper: Proposed Security Controls on Defense Research'' (2002), *available at:* http://www.fas.org/sgp/othergov/deyoung.html.

the university pointed out that the provision conflicted with national policy, offered to substitute an alternative that allowed the university to publish or otherwise distribute the research results, on the condition that they be submitted to the agency ''for review and comment at least thirty (30) days prior to any such release.'' In another subcontract involving a university, which contained similar language, a program director agreed that the provision need not be included and agreed that ''[p]apers resulting from unclassified contracted fundamental research are exempt from prepublication controls.''[29]

## *The broader context: What information is ''sensitive''?*

These experiences highlight that it may be useful for the government to clarify on a federal-governmentwide level the types of information dissemination that may be restricted in research agreements. The lack of consistent policy in this area appears to be one aspect of broader inconsistency in the different definitions and standards federal agencies employ for sensitive but unclassified information. According to a 1997 congressional report, for example, ''at least 52 protective markings [are] being used on unclassified information,'' with such various names as ''sensitive but unclassified,'' ''limited official use,'' and ''official use only.''[30]

The statement of federal policy in NSDD-189 (''No restrictions may be placed upon the conduct or reporting of federally-funded fundamental research that has not received national security classification, except as provided in applicable U.S. statutes.'') itself seems to have signaled an effort—not entirely successful—to prescribe a consistent governmentwide approach following attempts within the executive branch to restrict dissemination of a broader category of information. A Congressional Research Service report describes how, in 1986, President Reagan's National Security Advisor, John Poindexter, issued a policy document, applicable to electronic information handled by any federal agency or contractor, that defined ''sensitive'' information as not only that which ''could affect national security'' interests, but also that which could effect ''other Federal Government interests.''[31] Although criticism from Congress and others led to withdrawal of the policy document in 1987, the Department of Energy continues to use an identical definition of ''sensitive but unclassified'' information.[32] Other agencies, too, continue to have in place broad definitions of sensitive information. The Department of the Navy, for example, issued guidance in 1995 stating that ''all unclassified information processed by'' the Department of the Navy is ''sensitive,'' and ''essentially all business conducted within the government'' should be considered ''sensitive but unclassified.''[33] The Department of Interior has taken a similar position.[34]

After Sept. 11, 2001, and the anthrax attacks, the government seemed to strengthen federal agencies' ability not only to classify information, but also to place controls on unclassified material. The White House issued a memorandum calling for federal agencies to reconsider measures for safeguarding information regarding weapons of mass destruction and other sensitive documents related to homeland security. Agencies were directed to reconsider whether documents should be classified and to report progress to the White House. An accompanying memorandum issued by the National Archives and Records Administration (''NARA'') mandated that agencies safeguard ''sensitive information related to America's homeland security.''[35] NARA instructed agencies to consider on a case-by-case basis whether information might be protected from disclosure under the Freedom of Information Act (''FOIA''). It cited exceptions for information relating to an agency's ''internal personnel rules and practices,'' trade secrets, and certain privileged or confidential commercial or financial information.[36]

The NARA memorandum relied on October 2001 guidance issued by Attorney General John Ashcroft, which encouraged agencies to interpret certain FOIA exemptions more broadly than under previous guidance. While earlier guidance issued by former Attorney General Janet Reno urged agencies to release information, even if the law provided a basis to withhold it, if no ''foreseeable harm'' would result, the new Department of Justice interpretation encouraged them to withhold information if there was a ''sound legal basis'' for doing so. [37] The Attorney General's memorandum also broadly interpreted FOIA's exemptions in relation to ''the need to protect critical systems, facilities, stockpiles, and other assets from security breaches and harm'' and potential use as weapons of mass destruction. It said agency assessments and statements regarding the vulnerability of these assets should be exempt from FOIA requests under the exception for an agency's ''internal personnel rules and practices.'' The memorandum encouraged agencies to ''avail themselves of the full measure'' of this FOIA exemption, which it said protects ''a wide range of information'' related to critical assets.[38]

Members of Congress have opposed the more restrictive approach to disclosure of sensitive information that these directives reflect. The House committee that oversees FOIA criticized the Attorney General's October 2001 memorandum, rejected the ''sound legal basis'' standard it adopted for withholding FOIA information, and ordered agencies to continue to release information unless they reasonably foresaw that disclosure would be harmful to an interest protected by a FOIA exemp-

[29] Examples such as these have been cited by university counsel at professional conferences.

[30] *Report of the Commission on Protecting and Reducing Government Secrecy*, Senate Document 105-2 (1997).

[31] *See* Knezo, *supra*, at 13 (citing ''National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Information Systems,'' NTISSP No. 2).

[32] *Id.* at 13, 20.

[33] *See id.* at 22 n.71.

[34] Dep't of Interior, Departmental Manual, 375 DM § 19.3 (April 15, 2002).

[35] *See* Knezo, *supra*, at 24 (citing White House memorandum and NARA memorandum, both *available at:* http://www.usdoj.gov/oip/foiapost/2002foiapost10.htm).

[36] *Id.*

[37] A copy of the Ashcroft guidance is *available at:* http://www.usdoj.gov/oip/foiapost/2001foiapost19.htm.

[38] *Id.*

   ISSN 1539-1035

tion.[39] The Homeland Security Act, which addressed disclosure under FOIA of ''critical infrastructure information,'' imposes further requirements in this area. It requires that research conducted by the Department of Homeland Security ''shall be unclassified'' to the ''greatest extent possible.''[40]

As these developments illustrate, the fact that there are varying approaches within the government to protection of sensitive information affects areas of activity that extend well beyond the research context. Larger questions loom regarding the appropriate balance between public access to government-held information and the government's ability to safeguard information that could be used to harm Americans or U.S. interests.

## *Possible future policy directions*

There is reason for some optimism that future policy will address this issue. The Homeland Security Act institutes a process that may help to provide more consistent guidance concerning the types of information agencies may control. The act requires the president to implement procedures to safeguard ''homeland security information that is sensitive but unclassified.''[41] The procedures have yet to be issued, but the Office of Management and Budget and the OSTP are developing guidelines for federal agencies that may set uniform standards for designating information as ''sensitive.'' Members of Congress, too, have weighed in on particular cases.[42] Policymakers certainly are aware of universities' concerns about agency efforts to control unclassified research results. In January 2003, higher education leaders wrote to the OSTP expressing concern over the increasing rate at which program officials were inserting pre-publication review clauses into research contracts without providing justification.[43]

Self-regulation represents another possible response to the challenge of limiting inappropriate access to sensitive information. The academic community, which long has viewed self-regulation as a more appealing alternative to government rules, has sponsored several initiatives to ensure protection of sensitive information within the scientific community. Some scientific societies, for example, have considered ways to address publication of ''sensitive'' information in scientific journals. In a well-publicized incident, the National Academy of Sciences reported that it removed from an article, and placed in an appendix available to requesters on a ''need to know'' basis, information about vulnerabilities of U.S. croplands, after review by the U.S. Department of Agriculture, which sponsored the research. The three National Academies initiated an effort to develop standards for publication that balance the need to protect sensitive information with the openness that allows scientific progress.[44] The American Society of Microbiology has asked members to exercise caution in releasing information potentially useful to terrorists and established procedures for editorial panel review of articles on ''select agents.''[45] Editors of prominent biomedical journals issued a statement in *Science* saying they would take security issues into account when reviewing articles for publication.[46]

These efforts are piecemeal and, critics say, do not lend themselves to robust enforcement. Certainly there will continue to be disagreement about where to draw the line between open scientific inquiry and secrecy necessary for national security. But regardless of how the academic community responds, federal agencies are likely to continue to set standards as well. For that reason, a clarification of federal policy in this area that applied broadly to the executive agencies likely would promote a more consistent governmental approach to research agreements.

---

[39] H.R. Rep. No. 107-371 (2002).

[40] Homeland Security Act of 2002, Pub. L. No. 107-296, § 306(a), 116 Stat. 2135 (2003).

[41] *Id*. § 892.

[42] *See* Knezo, *supra*, at 34 (citing 148 Cong. Rec. H5993-02, H5997 (daily ed. July 26, 2002) (statement of Rep. Pease)).

[43] *Id*. at 39-40.

[44] *Id*. at 32.

[45] Shea, *supra*, at 18.

[46] *See* ''Statement on Scientific Publication and Security,'' *Science*, Feb. 21, 2003, *available at:* http://www.sciencemag.org.